reference guide

hp StorageWorks SAN design

Tenth Edition (February, 2004)

Part Number: AA-RMPNL-TE

This document is a guide to designing and building HP StorageWorks Storage Area Networks (SANs). It describes how Hewlett-Packard storage systems, storage management tools, and Fibre Channel products can be used in open heterogeneous SANs. Refer to the following URL for updates to this document.
http://h18006.www1.hp.com/products/storageworks/san/documentation.html

SAN Design Reference Guide
Tenth Edition (February, 2004)
Part Number: AA-RMPNL-TE

contents

Figures

Tables

about this guide

About this Guide topics include:

Related Documentation

In addition to this guide, HP provides corresponding information:

Topic	Document Title
HP-UX	HP-UX Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide
HP-UX	HSG80 ACS Solution Software Version 8.7 for HP-UX Installation and Configuration Guide
Tru64 UNIX	Tru64 UNIX Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide
Tru64 UNIX	HSG80 ACS Solution Software Version 8.7 for Tru64 UNIX Installation and Configuration Guide
OpenVMS	OpenVMS Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide
OpenVMS	HSG80 ACS Solution Software Version 8.7 for OpenVMS Installation and Configuration Guide
Windows NT (Intel), Windows 2000	Windows NT and 2000 Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide
Windows NT (Intel), Windows 2000	HSG80 ACS Solution Software Version 8.7 for Windows NT and Windows 2000 Installation and Configuration Guide
Windows NT (Intel), Windows 2000	Enterprise/Modular Storage RAID Array Fibre Channel Cluster for Windows NT/Windows 2000 Installation Guide
Windows NT (Intel), Windows 2000	Booting Windows from a Storage Area Network Application Note
Windows NT (Intel), Windows 2000	RAID Array 4100 User Guide
Windows NT (Intel), Windows 2000	RA4100 SAN Solution User Guide
Windows NT (Intel), Windows 2000	MSA1000 User Guide
Windows NT (Intel), Windows 2000	NAS Executor E7000 Quick Start Guide
Windows NT (Intel), Windows 2000	NAS B3000 Quick Start Guide
Sun Solaris	Sun Solaris Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide

Topic	Document Title
Sun Solaris	Sun Solaris Kit V3.0 for Enterprise Virtual Array Installation and Configuration Guide
Sun Solaris	HSG80 ACS Solution Software Version 8.7 for Sun Solaris Installation and Configuration Guide
IBM AIX	HSG80 ACS Solution Software Version 8.7 for IBM AIX Installation and Configuration Guide
Linux	HSG80 ACS Solution Software Version 8.7 for Linux X86 and Alpha Installation and Configuration Guide
Linux	RA4100 SAN Solution User Guide
Novell NetWare	HSG80 ACS Solution Software Version 8.7 for Novell NetWare Installation and Configuration Guide
Novell NetWare	RAID Array 4100 User Guide
Novell NetWare	RA4100 SAN Solution User Guide
SGI IRIX	HSG80 ACS Solution Software Version 8.6 for SGI IRIX Installation and Configuration Guide
Enterprise Virtual Array	Enterprise Virtual Array HSV Controller User Guide
HSG80 Controller	HSG80 Array Controller ACS Version 8.7 CLI Reference Guide
StorageWorks Command Console	Command Console V2.5 User Guide
Enterprise Backup Solution	Enterprise Backup Solution Reference Guide
B-Series Product Line Switches	■ Core Switch 2/64 Installation Guide ■ SAN Switch 2/16 Installation Guide ■ SAN Switch 2/16 EL Installation Guide ■ SAN Switch 2/8 EL Installation Guide ■ SAN Switch 2/32 Installation Guide ■ Fibre Channel SAN Switch Management Guide ■ Fibre Channel SAN Switch Installation and Hardware Guide ■ Command Console for the SAN Switch Installation Guide ■ Combining 16-Port Switches to Construct Higher Port Count Switches Application Note
M-series Product Line Switches	■ Director 2/64 Installation Guide ■ Edge Switch 2/32 Installation Guide ■ Edge Switch 2/16 Installation Guide ■ Edge Switch 2/24 Installation Guide ■ Director 2/140 Installation Guide ■ HA-Fabric Manager User Guide ■ Product in a SAN Environment: Planning Guide for Director 2/64, Edge Switch 2/16, and Edge Switch 2/32
C-Series Product Line Switches	■ Cisco MDS Switch product documentation is available at: www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_technical_documentation.html

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

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

Text Symbols

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

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

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

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

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Getting Help

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

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

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

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://thenew.hp.com/country/us/eng/support.html.

Be sure to have the following information available before calling:

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

HP Storage Website

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

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

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

Understanding SANs

1

Storage Area Networks (SANs) provide the data communication infrastructure needed for the most advanced and most cost-efficient computer mass storage systems. SANs minimize total cost of ownership for both large and small storage systems. SAN technology supports the management features and I/O price/performance demanded in today's competitive IT environment, and offers the storage component investment protection needed to minimize capital expense.

This chapter summarizes the benefits that can be obtained by using storage area networks

Why a SAN?

SANs provide unprecedented levels of flexibility in system management and configuration. Servers can be added and removed from a SAN while their data remains in the SAN. Multiple servers can access the same storage for more consistent and rapid processing. The storage itself can be easily increased, changed, or re-assigned.

In a SAN, multiple compute servers and backup servers can access a common storage pool. The SAN offers configuration choices that emphasize connectivity, performance, resilience to outage, or all three.

SANs bring enterprise-level availability to open systems servers. Properly designed SAN storage is always available. This allows many open servers to access a common storage pool with the same degree of availability previously reserved for mainframes.

SANs improve staff efficiency by supporting a variety of operating systems, servers, and operational needs. A SAN is a robust storage infrastructure that can respond quickly to new business models, unexpected growth surges, and corporate mergers.

SANs can reduce application response time, improve processing throughput, and support high-performance backup and rapid restores. SANs enable new functionality concepts such as zero backup time, they support remote data copies at nearly unlimited distances, and they support improved business continuance scenarios involving disaster recovery planning and disaster tolerant configurations. SANs also support the latest storage security measures, and they can be managed by Web-based tools from any location.

In a well-designed SAN, these features are complementary and cumulative; that is, a SAN can incorporate all of these features, or you can start with a SAN designed for any one of them and add other features later. SANs enable economy of scale that was previously unavailable to open systems in the areas of backup, management, growth, and performance. Because of this flexibility, a SAN can grow and adapt to the changing computer storage system needs of the most challenging business environment.

HP SAN Design Philosophy

The HP SAN design philosophy is to use a mix of moderately sized components to meet a wide range of storage system requirements. This approach maximizes customer value by optimizing the use of the features and functionality provided by HP SAN products. The same set of products can be used in small office environments, large business systems, and in the most demanding enterprise-class installations. HP StorageWorks products support SAN designs that work with a heterogeneous mixture of applications, operating systems, servers, storage systems, and SAN infrastructure components.

This approach to storage system design provides the following advantages.

- Greater flexibility in SAN design, to meet the widest possible range of requirements.
- Incremental scaling over time, by the addition of capacity and features as they become required.
- Support for diverse geographic and data locality requirements.

The design of HP SAN systems is facilitated by using multiple port functionality and a simple, standardized approach to storage configuration.

Multiple Port Functionality

- **Product line components enable large SANs**.

  HP Fibre Channel switches have multiple ports, and can be interconnected across long distances to achieve large network configurations. A set of interconnected switches is called a Fibre Channel fabric. Each fabric has ports into which several computer servers, storage systems, and related components can be integrated. Multiple fabrics may be included in a single SAN if needed to meet connectivity or availability requirements.

- **HP StorageWorks RAID Array controllers enable heterogeneous SANs**.

  Each HP controller has multiple ports for connection to the SAN. In addition, each storage controller can support a heterogeneous mixture of servers. Storage controllers and servers can be added to an existing installation in an incremental fashion. This maximizes the flexibility of the configuration and supports a number of scalable growth paths from any given SAN configuration starting point.

Approaches to Simplified Design

HP provides three approaches to SAN design and implementation. You can design and implement your SAN using an HP standard design, create a variation of an HP design, or create a custom design by following the HP StorageWorks SAN design rules. These approaches are listed in order of increasing effort and experience required to implement a particular approach.

1. **HP standard design**.

   HP standard designs specify the arrangement of Fibre Channel switches within a SAN fabric and are optimized for specific Data Locality needs and typical workloads. Copying a standard design is the simplest approach to SAN design, and is recommended for anyone just starting with SAN technology.

2. **Variation of an HP design**.

   Each of the HP standard topologies is optimized for a particular data locality type and offers different levels of connectivity. Often, you can select a standard SAN design that is close to your specific needs, and then modify it to meet the data locality and connectivity

requirements. By starting from a standard design, you use the SAN experience of HP to leverage your own design efforts. This approach is recommended for anyone with an intermediate level of SAN experience.

3. **Custom design using the HP StorageWorks SAN design rules**.

   The SAN design rules specify the maximum limits and guidelines for custom-designed topologies and also allow SAN designs that can be tailored to meet unique or specific storage and access requirements. The design rules contain the essential information about HP StorageWorks SANs. This information is accessible and useful to anyone with an intermediate or advanced level of experience with SANs. For further information, refer to Chapter 3, "SAN Fabric Design Rules" and Chapter 4, "Heterogeneous SAN Platform and Storage System Rules."

Note: In this document "SAN topology" refers to the arrangement of Fibre Channel switches within a fabric.

Design Considerations

When a new SAN design is under development, or an existing SAN is to be modified, a number of design considerations must be evaluated. Such considerations include:

- Geographic Layout
- Data Locality
- Connectivity
- Storage Capacity
- Heterogeneous Platforms and Operating Systems
- Scalability and Migration
- Backup and Restore
- Data Availability
- Disaster Tolerance
- Switch and Hop Counts
- Oversubscription
- Performance and Application Workloads
- Manageability
- Fabric Zoning
- Selective Storage Presentation
- SAN Security

Each of these is discussed in additional detail below.

Geographic Layout

The geographical location of building sites, campuses, and facilities, and the location of servers and storage within individual buildings can be a major factor in determining the appropriate SAN design. Various SAN options are available to support long distance connections within a SAN, so a wide range of varying geographical needs can be met. An HP StorageWorks SAN can be implemented with multiple inter-switch cable segments. For more information on supported distances, refer to Chapter 3, "SAN Fabric Design Rules."

Support for these long distances also provides for interconnection of existing independent SAN islands into a single geographically distributed SAN. Refer to Chapter 8, "SAN Extension" and Chapter 11, "Merging SAN Fabrics" for further information.

Data Locality

A major factor in determining the optimal SAN topology design is the set of requirements associated with the data access patterns between storage and the associated servers. Storage and server deployment should be based on the specific application requirements for data locality. A high frequency of data reference and a short response time requirement implies a requirement for greater data locality—the SAN must be designed so that the servers and storage have a high capacity path between them.

In the context of SAN topology design, locality refers to the placement of storage systems in the SAN relative to the placement of the servers accessing the storage. Possible placements include:

- Local, “one-to-one”
- Centralized in a single storage pool or centralized pools, “many-to-one”
- Distributed among storage pools throughout the fabric, “many-to-many”

Local or "one-to-one" is where the primary data access is between individual servers and individual storage systems. In many cases this implies that they should both be connected to the same Fibre Channel switch. Centralized or "many-to-one" data access is where the primary access pattern is between many servers and a single centrally located storage system. Distributed or "many-to-many" is where data access occurs between many different servers and many different storage systems. Many-to-many data access is encountered in environments that use SAN-wide storage pooling and sharing.

Selection of the appropriate SAN topology design should primarily be based on the expected primary data locality need, however consideration should also be given to corporate, departmental, and organizational requirements relative to data grouping and accessibility.

Connectivity

Connectivity is the total number of Fibre Channel ports needed to connect servers and storage to the fabric. Ports available for server or storage connections are called "user ports". In multiple switch fabrics the number of user ports in a SAN will be less than the total number of ports in the SAN because of the need for inter-switch links (ISLs) to connect the multiple switches together. One ISL port is the minimum needed for connectivity, however more ISL connections may be required in order to provide the required performance.

The need for ports for Inter-Switch Link connectivity at the required performance level directly affects the total number of Fibre Channel switches required in a SAN. Data locality and geographic requirements must be taken into consideration when deciding on the number of ISL connections for the fabric. You should also consider future connectivity requirements and develop a design that can scale or that can migrate to a topology design with more capacity.

If the total number of ports required exceeds what is supported in a given topology, you must consider higher capacity topologies, or perhaps deploy multiple independent SANs.

Storage Capacity

The total storage capacity requirement, including expected future growth, should be calculated to ensure that the design is adequate to meet your needs. There are two aspects to storage capacity. The first is the total required capacity measured in GigaBytes or TeraBytes. Storage capacity can be increased by adding larger capacity disks, adding additional disks, or by deploying additional storage systems in the SAN.

A second aspect of capacity is performance. As disk drive sizes increase it is possible you will use fewer disks. This approach makes it easier to design a storage system that will have the required size but does not aid in designing for required performance. There are workloads whose performance is limited by a lower number of disk drives. Consider the performance impact of using a lower number of higher capacity disk drives versus a higher number of lower capacity disks if high application performance is a critical requirement.

Heterogeneous Platforms and Operating Systems

HP heterogeneous Open SANs support a wide range of multi-vendor hardware platforms and operating systems in a mixed environment. You can tailor your SAN for the specific platforms and operating systems you require. HP storage controllers can be shared across many different platforms and operating systems, all managed within the same SAN. Specific support limits of individual platforms and operating systems may vary and need to be understood and considered when evaluating SAN designs.

Scalability and Migration

A major benefit provided by HP standard SAN designs is the capability to grow or scale incrementally over time as storage and connectivity needs increase. For all designs, consideration should be given to choosing a design that will accommodate expected future growth and usage requirements.

HP-designed SAN topologies can address immediate needs and requirements, and accommodate future changes. There are migration paths for each of the topologies to provide for configuration flexibility, expansion, and increased capabilities. Refer to Chapter 11, "Best Practices" for information about scaling and migrating different SAN topology designs, as some transitions are easier to perform then others. All aspects of scaling and migration should be understood when choosing a topology design.

For further information, refer to Chapter 2, “SAN Topologies.”

Backup and Restore

SAN-based backup provides high bandwidth and centralized control for your backup and restore operations. This can provide significant savings in time and management complexity over individual server or network based backup and restore implementations. SAN designs should provide adequate connectivity and bandwidth for backup, to maximize the benefits of SAN based backup. If your SAN design does not consider or accommodate backup bandwidth requirements, then you may affect backup performance. Centralized backup implies lower data locality within the SAN. Backup is an operation where data is accessed infrequently and where latency is not a concern. Refer to Chapter 5, “Enterprise Backup Solution.”

Data Availability

Data availability is a broad measure of how reliable a storage system is in routine operation. Depending on the specific requirements of a given application, you can choose from a wide range of methods. In some cases, a routine tape backup on a periodic basis provides enough availability. In other cases, a SAN with multiple paths between servers and storage within a single fabric is adequate. In the most demanding environments, you can configure an HP SAN that provides No Single Point Of Failure (NSPOF) in the data access paths and in the storage systems. A mixture of different availability levels can be implemented within the same SAN, depending on the level of protection required for specific applications or data. For further information, refer to Chapter 2, “Data Availability in a SAN.”

Disaster Tolerance

Disaster tolerance is a measure of how reliably data can be accessed and restored in the event of complete failure of a facility or site.

Consideration must be given to the criticality of data in the event of unforeseen catastrophic site failures. Remote data replication requirements should be considered in the SAN design to ensure protection against site failures and full recovery of critical data. Selected data can be copied to remote storage arrays, automatically providing recovery capabilities in the case of a primary site interruption or possible loss. Using multiple storage arrays, portions of the SAN can be configured for disaster tolerance, providing a common SAN with mixed data protection levels.

Switch and Hop Counts

Data routing through the fabric is described in terms of hops, where a single hop is one or more ISLs between any two switches. The general rule is that you should minimize the number of hops between devices that will communicate regularly in a SAN.

Oversubscription

Oversubscription is a normal part of any SAN design and is essentially required to help reduce the cost of the SAN infrastructure. Oversubscription refers to the fan-out ratio of available resources such as ISL bandwidth or storage system I/O capacity, to the consumers of the resource. A general rule-of-thumb releates oversubscription to the cost of the solution such that the higher the oversubscription, the less costly the solution.

Oversubscription occurs when multiple data streams on multiple ports are funneled into a single data stream on a single port. Since all ports have equal bandwidth, there is a bandwidth mismatch when the multiple parallel data streams are directed into a single port.

Oversubscription or congestion can occur in a fabric with multiple switches when data from multiple sources must be sent to a single destination port, or when data is required to be sent across an ISL from multiple input ports. In situations where this occurs, the Fibre Channel switches utilize fairness algorithms to ensure that all devices are serviced. The switches use the fairness algorithm to interleave frames from multiple devices, thus giving fractional bandwidth to all devices. If this occurs often, then overall performance in the fabric will be reduced. Oversubscription can be minimized by ensuring that your fabric design provides for an adequate number of ISLs between all switches, and by minimizing the cases where many devices or ports are attempting to share a single switch port.

Performance and Application Workloads

Performance requirements need to be considered in any SAN fabric design. This can be difficult, because data traffic in a SAN is not always predictable. Applications can usually be classified as high bandwidth or high throughput. What is important is that the SAN provides an adequate level of performance based on the workload presented by the applications.

Other factors to consider are the locality of data in relation to the servers most likely to access the data, and the number and placement of ISLs between switches in the fabric. In general, SAN topology designs with fewer switch hops between devices provide better performance due to a lower probability of oversubscription or congestion.

Manageability

SAN management can be centralized using a dedicated Storage Management Appliance, regardless of the arrangement or location of the storage components. The Storage Management Appliance connects directly to the SAN through a Fibre Channel switch, providing it with connectivity to all devices connected to the SAN. Refer to Chapter 6, "SAN Management", for more information on SAN management.

Fabric Zoning

Zoning is a fabric management service used to define logical subsets within a SAN. Zoning enables resource partitioning for management and access control by dividing a physical SAN into multiple overlapping logical zones, where each zone is defined by the set of ports or devices that are addressable within the zone. The HP Fibre Channel switch zoning feature provides a way to control SAN access at the device or port level. This capability allows you to set up barriers between different operating environments, to deploy logical fabric subsets by creating defined server and/or storage groups, or to define temporary server and storage zones for tape backup. Zones can be configured dynamically.

Selective Storage Presentation

HP storage systems implement a LUN masking feature called Selective Storage Presentation (SSP). This feature allows you to assign or selectively present logical units on a given storage system to one or more servers in the SAN. This provides protection against unintended access of a given storageset by a given server, while allowing accesses that are needed for proper operation. This provides a level of data access security, and allows multiple operating systems to be used in a single SAN.

Utilization of both SSP and Fabric Zoning provides for the most flexible SAN node and device access management. These features should be viewed as complementary in that usage of both provides the greatest range of SAN storage access management capabilities. For more information, refer to Chapter 6, “Selective Storage Presentation.”

SAN Security

Security is provided in HP SANs and storage systems by a combination of product features and system management practices. HP StorageWorks SAN hardware and SAN management tools provide reliable access to data, robust data storage, and enforcement of data access restrictions, and careful system management ensures that proper security practices are followed. For more information, refer to Chapter 9, “SAN Security.”

Summary

SAN design requires the consideration of many factors. To successfully complete a SAN design and implementation, you provide the requirements for your SAN and HP provides the product features and capabilities needed to meet the requirements. HP offers a design philosophy and standard SAN topologies that can be used as guidance. In addition, HP provides a comprehensive set of design rules. By following these rules, you will have a SAN configuration that is supported by the HP storage engineering organization.

This guide provides the detailed information you need to design a SAN that meets your unique storage system requirements.

SAN Topologies

2

This chapter describes the HP standard SAN topologies. You should review the SAN design considerations listed in the first chapter before starting the topology selection process. The design considerations enable you to generate a list of prioritized requirements for your SAN design. This list of requirements provides a basis for selecting the optimum fabric topology.

There are three approaches that you can choose when designing your SAN. You can choose to implement an HP standard SAN topology design, a subset or variation of an HP design, or you can design a custom SAN topology. Regardless of which approach you use, the final SAN design must adhere to the SAN design rules described in Chapter 3, "SAN Fabric Design Rules" and Chapter 4, "Heterogeneous SAN Platform and Storage System Rules."

Before choosing your design, you should review the HP standard SAN topology section in this chapter to get a good understanding of the important aspects of SAN implementation. HP recommends that you first consider implementing one of the HP standard topologies or a variation of one of these designs. If your requirements cannot be met by a standard design, then you can implement a customized SAN topology design—provided you follow the design rules.

Why Design Rules?

HP performs extensive qualification of all HP SAN components, including application software, operating systems, host bus adapters, Fibre Channel switches, storage systems, and storage system management appliances. A sophisticated process is used to verify the interoperability of SAN components across a wide spectrum of supported configurations, taking into consideration potential customer requirements for mixed applications, servers, operating systems, and storage systems in a single environment. In order to ensure that a new SAN installation will function properly, certain guidelines must be followed. These guidelines are the result of actual laboratory testing—not theoretical projections of “what should work”—and reflect the designed-in capabilities of the various software and hardware components that are use in SAN storage systems.

The guidelines are captured in rule form to make it easier to design a SAN that will work properly and will be supported by HP. Chapter 3, "SAN Fabric Design Rules"and Chapter 4, "Heterogeneous SAN Platform and Storage System Rules", define the configuration rules. For additional information on operating system HBA/driver/firmware/software support, contact your HP field representative.

Switch Product Lines

HP supports three product lines of Fibre Channel switch products that may be used to build SAN fabrics. Each product line provides certain advantages that apply to specific applications. For more information on specific switch models, refer to the section Switch Model Selection Guidelines and the Fibre Channel switch product information at www.hp.com.

The B-Series product line includes a wide range of Fibre Channel switches, described as "SAN switches" and "Core switches." A partial list of products in this family includes the HP StorageWorks SAN Switch 2/16 and the HP StorageWorks Core Switch 2/64. This product line includes switches with 8, 16, 32, and 64 ports, including both full-function and entry-level models. The HP StorageWorks Core Switch 2/64 includes a pair of independent 64-port switches in a single chassis with a high level of internal redundancy.

The C-Series product line includes the Cisco MDS 9506 and 9509 Multilayer Directors and the MDS 9216, 9120, and 9140 Multilayer Fabric Switches. The MDS 9509 is supported with 224 ports and MDS 9506 is supported with up to 128 ports per chassis. MDS 9509 and 9506 offer 7 and 4 modular slots respectively that can be populated with 16-port, 32-port, or IP Storage services modules. The MDS 9216 has 2-slots – one is a fixed configuration with 16 ports. The second - an expansion slot that supports either a 16 or a 32 port card, for 32 or 48 ports in total. The second slot can also be populated with an IP Storage services module supporting FCIP via 8 ports of GE (Gigabit Ethernet).

The MDS 9100 Series of multilayer fabric switches is a fixed-configuration 1U platform consisting of the MDS 9120 and MDS 9140 switches supporting a fixed 20 port and 40 ports respectively. The MDS 9100 Series supports the same multilayer intelligent networking services as the MDS 9500 Series and MDS 9200 Series including the same command line interface (CLI) and embedded Fabric Manager suite.

The M-Series Fabric product line includes a wide range of Fibre Channel switches described as "Directors" and "Edge switches." A partial list of products in this family includes the HP StorageWorks Director 2/140 and the HP StorageWorks Edge Switch 2/32. This product line includes switches with 16, 24, 32, 64, and 140 ports, and all models use the same version of internal microcode. The HP StorageWorks Director 2/64 and 2/140 have a high level of internal redundancy.

The switch model numbering convention is the same in B-Series and M-Series product families. The number preceding the slash indicates the highest speed at which the switch ports can operate, measured in Gbps, and the number following the slash indicates the number of ports on the switch. The HP StorageWorks SAN Switch 2/16 is a 2 Gbps switch with 16 ports, and the HP StorageWorks Edge Switch 2/32 is a 2 Gbps switch with 32 ports.

For B-Series switches, entry level models are indicated by the suffix "-EL" in their product name.

All HP 2 Gbps Fibre Channel products implement ports that auto negotiate their signaling speeds. Each pair of ports uses the lower of the supported speeds, so if a 2 Gbps port is connected to a 1 Gbps port, they both run at 1 Gbps in each direction. This applies to pairs of ports that are directly connected together. The speed of a remote port does not affect the local port speed, because speed matching is done within the switches in the fabric.

Switch Product Line Interoperability

For new SAN deployments HP recommends you utilize switch models from a single product line exclusively. To meet the needs of customers desiring a mix of switch models from the different product lines however, HP does support two levels of SAN fabric interoperability. Specifically, HP supports:

- Within a multi-fabric SAN, one fabric with all B-Series switches and another fabric with all M-Series switches. This is referred to as a "dual heterogeneous SAN fabric"
- Within a single fabric, M-Series Director and Edge switch models intermixed with B-Series SAN switch models This is referred to as an "interoperable heterogeneous SAN fabric"
- Within a single fabric, C-Series Director and Fabric switch models intermixed with B-Series switch models.

Refer to Heterogeneous/Interoperable SAN Fabrics, page 77 for the specific fabric interoperability rules and supported switch models for these levels of interoperability.

Switch Model Selection Guidelines

Each of the three HP Fibre Channel switch product lines offers a range of switch models including core or director, and SAN, edge or fabric switch types. For the purposes of selection guidelines in this section of the guide, the terms “core” and “edge” are used generically in reference to switch placement in a core to edge fabric design. Elsewhere in this guide and in other HP literature, the use of these terms more formally within a product name describes very specific switch models such as “Core Switch 2/64”, “Director 2/140” or “MDS Fibre Channel Director”, and “SAN Switch 2/16”, “Edge Switch 2/16” or “MDS Fibre Channel Fabric Switch”.

For each switch product line, the general recommendations and guidelines presented are based on the combination of a number of factors such as switch cost, scalability, and availability features. Specific customer requirements may rank some factors higher than others in importance and need to be considered when selecting the appropriate switch model for a specific SAN implementation. Refer to the switch model features table for each product line for specific recommendations based on certain switch model features.

Note: The switch model selection information presented in this section provides general guidelines for usage, and is not meant be a substitute for a thorough architectural level topology design process. Refer to other sections of this guide for information about determining the optimal fabric topology design prior to selecting specific switch models.

B-Series Switch Model Selection Guidelines

The following two tables show the recommended usage of each B-Series switch model for core or edge switch placement in a fabric design. Refer to Table 4 for specific switch model features.

Table 2: B-Series switch model usage as a core switch

B-Series Core Switch Model Selection					
	1-96 User Ports	97-224 User Ports	225-500 User Ports	501-728 User Ports	728-1280 User Ports
Core Switch 2/64	Excellent	Excellent	Excellent	Excellent	Excellent
SAN Switch 2/32	Excellent	Very good	Good	Not recommended as a core switch	Not recommended as a core switch
SAN Switch 2/8, 2/8-EL and 2/16	Good	Good	Good	Not recommended as a core switch	Not recommended as a core switch
SAN Switch 16	Good	Good	Not Recommended	Not recommended as a core switch	Not supported
Note: The SAN Switch 16 is only recommended as a core switch when connected to other 1 Gbps SAN switches					

Table 3: B-Series switch model usage as a SAN switch

B-Series SAN Switch Model Selection					
	1-96 User Ports	97-224 User Ports	225-500 User Ports	501-728 User Ports	728-1280 User Ports
Core Switch 2/64	Excellent	Excellent	Excellent	Excellent	Excellent
SAN Switch 2/32	Excellent	Excellent	Excellent	Excellent	Excellent
SAN Switch 2/8, 2/8-EL and 2/16	Excellent	Very Good	Very Good	Good	Good
SAN Switch 16	Very Good	Very Good	Good	Good	Not Supported

Table 4: B-Series switch model features

	Redundant Power, Hot Swap Power	Redundant Cooling, Hot Swap Cooling	Redundant Control Processor	Non-disruptive Code Activation	Non-disruptive Port Expansion	High Availability (Redundant Active Components)
Core Switch 2/64	Yes, Yes	Yes, Yes	Yes	Yes	Yes	Yes
SAN Switch 2/32	Yes, Yes	Yes, Yes	No	Yes	No	No
SAN Switch 2/16	Yes, Yes	Yes, Yes	No	No	No	No
SAN Switch 16, 2/8, 2/8-EL	No, No	Yes, No	No	No	No	No

B-Series Multi-Protocol Support

B-Series switches are supported for iSCSI through the SR2122 iSCSI router. FCIP support is provided through the SAN Valley Gateway. Refer to Chapter 8, "SAN Extension" for more information.

B-Series Switch Model Features

- **Investment protection** Upgrading from EL switches to full fabric functionality without disruption in a production environment.
- **Compatibility** Plug and play installation with currently installed B-Series switch ports.

Power Pak Option License bundled software features include:

- **Advance Performance Monitor** - Provides complete resource utilization analysis on a fabric-wide basis.
- **Advance WebTools** - A browser-based application for managing B-Series switches, WebTools simplifies management by enabling administrators to configure, monitor, and manage switch and fabric parameters from a single online access point.
- **Advanced Zoning** - Providing secure access control over fabric resources. Both port and WWN zoning is hardware enforced at the frame level.
- **Extended Fabrics** - Enable Fibre Channel SAN connectivity at distances up to 100 km. Extended Fabrics applications improve disaster recovery operations and help ensure business continuance.
- **Fabric Watch** - Fabric Watch proactively monitors the health and performance of switches and the SAN fabric from a central point.
- **ISL Trunking** Inter-Switch Link Trunking is an ASIC based feature which combines multiple links between switches to form a single logical ISL with a total bandwidth of 8 Gbit/sec. ISL Trunking enhances performance via dynamic load balancing frames across links.
- **Remote Switch** Remote Switch enables B-Series switches to create one logical SAN that spans remote fabrics at unlimited distances. SAN to WAN connectivity enables one logical view of a SAN in which all components appear as local devices.

Additional software features and applications:

- **Secure Fabric OS** Secure Fabric OS is a comprehensive security solution for B-Series SAN fabrics. Secure Fabric OS provides flexible security and policy based administration that protects data from unauthorized access and corruption. Licensed separately.
- **Fabric Manager** Fabric Manager is a host based application which provides administrators with the ability to simplify B-Series SAN management. The Fabric Manager application is sold separately.

C-Series Switch Model Usage

The following table shows the recommended usage of each C-Series switch model for core or edge switch placement in a fabric. Refer to Table 6 for specific switch model features.

Table 5: C-Series switch model usage as a function of the fabric size

C-Series Director Switch Model Selection			
	Up to 48 Total Ports	48 to 224 Total Ports	224-512 Total Ports
Recommended Topology	Single Switch	Single Director	Core/Edge
MDS 9509 Director	Good[1,2]	Excellent	Excellent / Core Director
- 16-port Module - 32-port Module	Storage and ISL Host & Tape	Storage and ISL Host & Tape	Storage and ISL Host & Tape
MDS 9506 Director	Very Good[2]	Excellent / Up to 128 ports	Excellent / Core Director
- 16-port Module - 32-port Module	Storage and ISL Host and Tape	Storage and ISL Host and Tape	Storage and ISL Host and Tape
MDS 9216 Fabric Switch	Excellent / Up to 48 ports	Excellent Edge Switch	Very Good / Edge Switch
MDS 9120 Fabric Switch	Excellent / Up to 20 ports	Excellent Edge Switch	Excellent / Edge Switch
MDS 9140 Fabric Switch	Excellent / Up to 40 ports	Excellent Edge Switch	Excellent / Edge Switch

1. Excellent if planning to scale to larger port count in the near future
2. Excellent if ultra high availability at the device level is a requirement

C-Series Switch Model Features

All C-Series products come with the following standard features:

- Non-blocking architecture using Virtual Output Queuing
- VSAN (Virtual Storage Area Network) for deployment of secure, virtual SANs over the same physical infrastructure. (Please refer to page 74 for more details on this feature.)
- Advanced Diagnostics and Troubleshooting – FC Ping, FC Traceroute, SPAN, RSPAN, and Call Home
- Comprehensive Security - SSH, SFTP, RADIUS, SNMPv3, and Role Based Access Control (RBAC)
- Comprehensive Fabric Management – CLI, SNMP, and Java-based GUI
- Traffic Management – QoS and FCC (Fibre Channel Congestion Control)
- High Availability Software – Failed process restart
- Port-Channel – ISL link aggregation for highly resilient SAN architectures
- SAN Extension – FCIP (MDS 9506, 9509, 9216)
- FSPF

All C-Series Directors have the following additional features

- Hitless Software Upgrades – Ability to upgrade without disruption to traffic
- Hot swappable line-cards, supervisors, power supplies, and SFPs
- Redundant supervisor, cross-bar fabric, and power supplies

C-Series Modular Switches also support the following features

- Integrated Multi-protocol capability – FCIP

The following table highlights some of the key differences of the various C-series switch models in terms of features. The differences are mostly hardware and HA (high availability) related. Other features, built in the switch firmware, such as VSANs or Port-Channeling, are common to all models.

Table 6: C-Series switch model features

	Redundant Power, Hot Swap Power	Redundant Cooling, Hot Swap Cooling	Redundant Control Processor	Non-disruptive Code Activation	Port Module Support	Non-blocking	Multi-Protocol Support
MDS 9509 and MDS 9506 Directors	Yes	Yes	Yes	Yes	Yes	Yes	FC, FCIP,
MDS 9216 Fabric	Yes	Yes	No	No	Yes	Yes	FC, FCIP,
MDS 9120/40 Fabric	Yes	Yes	No	No	No	Yes	No

M-Series Switch Model Usage

The following two tables show the recommended usage of each M-Series switch model for director or edge switch placement in a fabric. Refer to Table 9 for specific switch model features.

Table 7: M-Series switch model usage as a director switch

M-Series Director Switch Model Selection			
	16-500 Total Ports	501-1000 Total Ports	1000-1632 Total Ports
Director Switch 2/140	Excellent	Excellent	Excellent
Director Switch 2/64	Excellent	Excellent	Excellent
Edge Switch 2/32	Very Good	Good	Good
Edge Switch 2/24	Very Good	Good	Good

Table 8: M-Series switch model usage as an edge switch

M-Series Edge Switch Model Selection			
	16-500 Total Ports	501-1000 Total Ports	1000-1632 Total Ports
Director Switch 2/140	Good	Very Good	Excellent
Director Switch 2/64	Good	Very Good	Excellent
Edge Switch 2/32	Excellent	Very Good	Good
Edge Switch 2/24	Excellent	Very Good	Good

M-Series Switch Model Features

All M-Series products come with the following standard features:

- Hot Code Activation Technology (HotCAT™) for non-disruptive activation of new code releases.
- Full non-blocking performance across all ports.
- Consistent latency across all ports
- Redundant and Hot swappable power and cooling systems
- Redundant, Dual power connections for separate connections (fish)
- Hot swappable short and long wave optical transceivers
- Embedded web sever for device and small fabric administration

All M-Series Director Switches have the following features:

- 4-ports per card for low service impact
- Non-blocking port density to minimize data center floor space usage
- Operational requirements with the lowest power consumption and heat generation
- Fully redundant hot swappable switching and processor logic cards
- High availability
- Non-disruptive port expansion
- Non-disruptive failover of redundant components with full performance
- Automatic health checks of redundant field replaceable units (FRUs)

All M-Series Edge Switches have the following features:

- Flexport Non-disruptive port expansion
- Edge Switch 2/24 supports Fibre Channel loop connectivity

Table 9: M-Series Switch Model Features

	Min / Max ports	Size 1U =1.75”	Redundant Control Processor, Switching	Non-disruptive Port Expansion	High Availability (Redundant Active Components)
Director Switch 2/140	32-140, 4 port cards	12 U	Yes	Yes	Yes
Director Switch 2/64	33-64, 4 port cards	9 U	Yes	Yes	Yes
Edge Switch 2/32	16, 24, 32	1.5 U	No	Yes	No
Edge Switch 2/24	8, 16, 24	1 U	No	Yes	No

M-Series Multi-Protocol Support

M-Series switches are supported for iSCSI through the SR2122 iSCSI router. FCIP support is provided through the SAN Valley Gateway. Refer to Chapter 8, "SAN Extension" for more information.

Definitions

In order to understand SAN design, it is important to understand the relationship between a SAN and a fabric.

The Storage Networking Industry Association (SNIA) offers the following (slightly reworded) definitions of these two terms. (Refer to www.snia.org)

> **SAN (Storage Area Network)**: A network whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements. A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage elements, and computer systems so that data transfer is secure and robust. The term SAN is usually (but not necessarily) identified with block I/O services rather than file access services. A storage system consisting of storage elements, storage devices, computer systems, and/or appliances, plus all control software, communicating over a network.
>
> **Fabric**: A Fibre Channel switch or two or more Fibre Channel switches interconnected in such a way that data can be physically transmitted between any two N_Ports on any of the switches. The switches that constitute a Fibre Channel fabric are capable of routing frames using only the D_ID in a FC-2 frame header.

This document discusses Fibre Channel SANs.

The SNIA definition of "fabric" refers to Fibre Channel and expresses the concept of fabric that is used in this document. An N_Port is an endpoint in the fabric, which is present in a server's Host Bus Adapter (HBA), a storage system, or a storage management appliance connected to the fabric. The D_ID is the address of the destination N_Port, and is contained in the header of every Fibre Channel packet. A Fibre Channel packet is also called a frame. FC-2 is the layer in the Fibre Channel protocol associated with packet routing.

Another way to define a fabric is to view it as a single FC-2 address space. Any valid FC-2 address that can be reached from a given N_Port in a fabric is part of that fabric.

The SNIA definition of "SAN" does not require that a SAN be implemented with Fibre Channel technology. When the term SAN is used in connection with Fibre Channel technology, use of a qualified phrase such as "Fibre Channel SAN" is encouraged. This usage is usually not required, because in most cases today, a SAN is a Fibre Channel SAN. According to the SNIA definition, an Ethernet-based network whose primary purpose is to provide access to storage elements would be considered a SAN. SANs are also sometimes used for system interconnection in clusters.

A given SAN can contain one or more fabrics. Most small SAN configurations use a single fabric. Larger storage environments may require very high levels of availability, and the best way to obtain this is by using a pair of redundant fabrics. HP storage systems, servers, and operating systems support both design approaches.

HP Standard SAN Topologies

The HP standard topology designs reflect the proper application of the HP SAN design rules. Each of the standard designs is tailored for a particular data access and connectivity need. Collectively, these designs provide a wide range of options for selecting the appropriate SAN design for your specific requirements. Variations of these designs, including additions or changes, can be validated by adhering to the appropriate rule set for each topology type. A subset of a standard design is always acceptable.

The different types of HP standard SAN topologies are described in detail in the following sections.

SAN Fabric Topologies

SAN fabric topology designs include:

- Cascaded Fabrics
- Meshed Fabrics
- Ring Fabrics
- Backbone Fabrics

Each of the design types can be:

- Implemented as a separate SAN for specific departments or applications within a company, to accommodate different data access needs.
- Implemented with centralized backup capabilities, reducing the cost of backup and restore operations.
- Deployed in one or more co-located groups.
- Deployed across a wide area with inter-switch distances up to 35 km (2 Gbps) and 100 km (1 Gbps.)

Note: Refer to Chapter 8, "SAN Extension", for additional information on extending SANs over long distances.

- Used to begin an ongoing deployment process using SANs and Fibre Channel technology in a modular, controlled approach. Storage consolidation can be implemented on a departmental or independent SAN basis. Future capabilities will allow for more switches within a single SAN, interconnection of multiple SANs to build larger fabrics, and provide for additional consolidation, if desired, or broader server-to-storage access.
- Centrally managed.
- Implemented with a wide range of SAN availability levels. See “Levels of Availability.”
- Upgraded to higher capacity topologies or topologies optimized for different data access types if needs change.

Single-Switch Fabrics

The smallest SAN consists of a single Fibre Channel switch, server, and storage system. This topology is a subset of all the other topologies, and forms the basis of the range of HP SAN solutions.

By choosing among various HP Fibre Channel switches, you can construct a wide range of single-switch SAN solutions. The smallest supported HP SAN uses a single 8-port switch, the HP StorageWorks SAN switch 2/8. If you need a large single switch SAN, the HP StorageWorks SAN Director 2/140 offers 140 ports. Furthermore, if there is a need for high SAN availability, two independent single-switch SAN fabrics may be used in a dual-fabric environment to give a total of 280 user ports.

A single-switch fabric maximizes SAN performance, because every port on the switch has full connectivity to every other port on the switch. This design is also very easy to install and configure, since there are no connections from one switch to another.

An example of a simple single-switch SAN is shown in Figure 1.

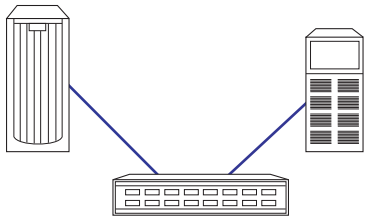


Figure 1: Single-switch SAN

Starting from a single-switch configuration, you can add more switches to your SAN fabric—following the support limits listed for each of the fabric topology designs—to increase the number of connections for servers and storage.

You can also view the various topology options as a way to connect existing smaller SANs or SAN islands. If you have already deployed several small SANs, you can connect them together to make a larger SAN. For example, if you have two single-switch SANs, you can connect them together into a cascaded fabric. Or, if you have deployed two four-switch meshed SANs as separate SANs, you can merge these into a larger single 8-switch meshed SAN as shown in Figure 4, "Modified Meshed Fabric SAN". If you have multiple single-switch SAN fabrics, you can connect these into a single larger SAN fabric by connecting them in a ring, or to a central backbone, using the backbone fabric topology.

Cascaded, Meshed, and Ring SAN Fabrics

The first three fabric topologies that involve more than a single switch are organized so that all of the switches in the fabric are used for connecting servers and storage. Every switch has at least one user port. Typically, in these types of fabric arrangements, a small percentage of the total number of switch ports is used for inter-switch connectivity in the form of Inter-Switch Links (ISLs). Refer to Chapter 1, "Connectivity", for more information about trading ports used for ISLs for ports used for servers and storage.

Cascaded Fabrics

A cascaded fabric SAN (see Figure 2) is a set of switches connected together, by one or more ISLs, in a tree-like arrangement.

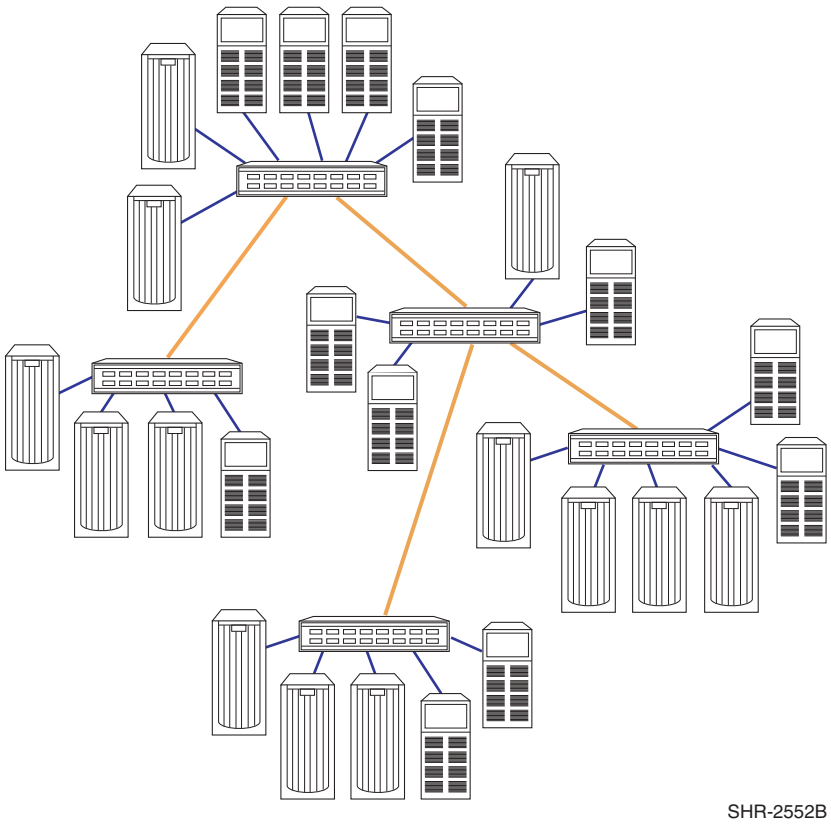


Figure 2: Cascaded Fabric SAN

Cascaded fabric designs are well suited to environments with local data access patterns. In these cases, I/O requests from a servers attached to a given switch are made most often to storage systems that are attached to the same switch. Groups of servers and their storage systems can be connected to the same switch to provide the highest level of I/O performance. Cascading provides a means to scale the SAN for additional connectivity of servers and storage, and allows for centralized management and backup, while maintaining the high I/O performance of local access.

Cascaded designs can also be used for centralized or distributed access; however, traffic patterns should be well understood and should be factored into the design to ensure that there are an adequate number of ISLs to meet performance requirements. Using more than one ISL between switches in a cascade also provides redundant paths between a given pair of switches in the fabric. HP highly recommends that cascaded designs be implemented with a minimum of two ISL connections on each switch, either as a pair of ISLs between the same two switches or by connecting every switch to at least two other switches in the fabric.

Very Large Cascaded Director Plus Edge Switch Fabric

The largest fabric supported by HP at this time is based on a cascaded fabric using HP StorageWorks Director 2/140 and StorageWorks Edge switches. Because the cascade configuration may be used to maximize user port count—if relatively low bandwidth between user ports that are on separate Directors is acceptable—this configuration can provide a level of connectivity that cannot be obtained by other means. Because of the availability features built into the SAN Director product, this configuration also offers high availability in a single-fabric topology.

The SAN Director product family is limited to a three-hop maximum. Hop count is a measure of distance or links between switches, measured in ISLs. A cascade configuration with 24 SAN Directors and Edge switches that meets the three-hop rule has one Director at the top of the tree, with 7 Directors attached under it, and 16 Edge switches under them. This gives a total of 24 SAN switches in one fabric. This supported configuration provides 1024 user ports.

Advantages of Cascaded Fabrics

- Accommodates diverse geographic conditions
- Scales easily for additional connectivity
- Shared backup is supported
- Shared management is supported
- Optimal local access is inherent in the fabric design
- Most efficient in cost per port

Meshed Fabrics

In a meshed fabric design, all of the switches are interconnected so there are at least two paths or routes from any one switch to any other switch in the fabric. This type of connectivity provides fabric resiliency. If a single ISL or ISL port interface fails, the fabric can automatically re-route data through an alternate path. The new route can even pass through additional switches in the fabric. An example of a meshed fabric is shown in Figure 3.

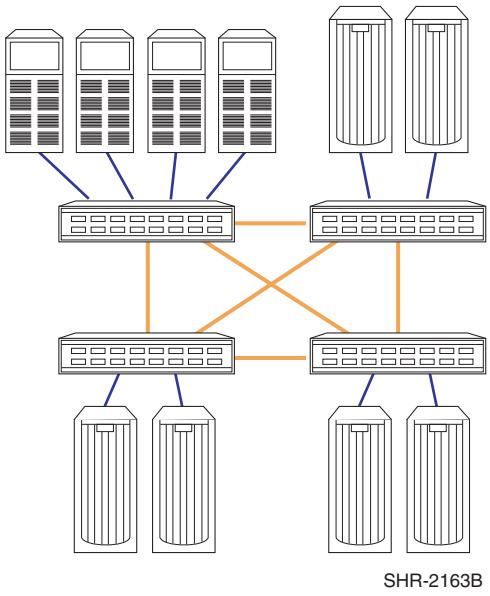


Figure 3: Meshed Fabric

As switches are added to a meshed topology, the number of ISLs required to maintain full connectivity between any switch and any other switch becomes excessive. This reduces the number of user ports in comparison to the total number of ports, which is a measure of the connection efficiency of the fabric. The connection efficiency of this fabric design can be improved by implementing a slightly modified mesh design, as shown in Figure 4. In this case the connectivity between switches is reduced, but the fabric availability is maintained because there are still multiple paths between switches.

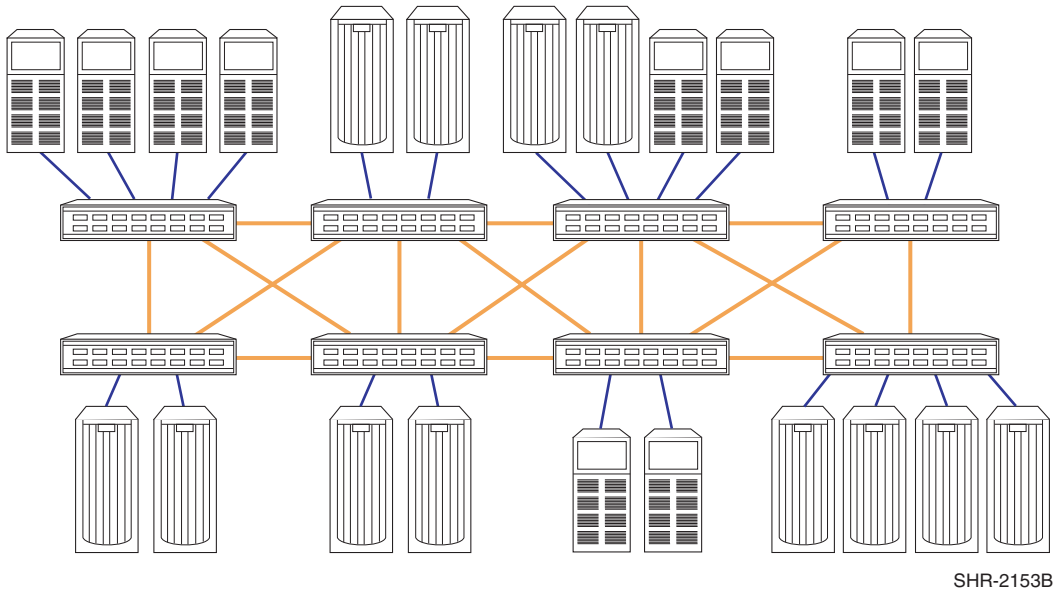


Figure 4: Modified Meshed Fabric SAN

In this example diagram, as switches are added, they are only connected to adjacent switches, not all other switches in the fabric. This still provides the benefits of full many-to-many connectivity without a decrease in connection efficiency.

Meshed fabrics are well suited to applications where data access is a mix of local and distributed. The full connectivity (or high connectivity, in the case of modified meshes) supports many-to-many access, while at the same time allowing localized access to individual switches, servers and storage.

Advantages of Meshed Fabrics

- Can be configured for any to any or local data access, or a mix
  Reduces staff effort by minimizing reconfiguration and re-cabling of existing Fibre Channel switches. Adapts easily to new or different storage needs.
- Provides protection against link and switch port failures
  Fabric design allows Fibre Channel switches to automatically re-route under failure conditions, saving time and effort to manually trace the problem and re-route.
- Scales easily
  The mesh design can be extended from a four-switch fabric to six or eight switches easily, and without disruption to the existing SAN. The mesh design affords ease of adding servers to the SAN without impacting existing connections or equipment. This is especially useful for companies where there is rapid growth, or computing and storage needs are changing frequently.
- Shared backup is supported
  One or more Automated Tape Libraries can be added to the mesh fabric at various points without impacting performance or management.
- Shared management is supported
  All Storage Management Appliance tools can navigate and manage the Storage Area Network in the mesh fabric, saving time and effort.
- Optimal distributed access is inherent in the fabric design

Ring Fabric

A ring fabric (see Figure 5, "Ring Fabric SAN") is a continuous ring of switches connected together into a single fabric. Each switch is connected to adjacent switches, with the last switch in the ring connected back to the first. This arrangement of switches provides almost the same level of fabric resiliency as the mesh design, with full fabric connectivity and at least two internal fabric paths or routes.

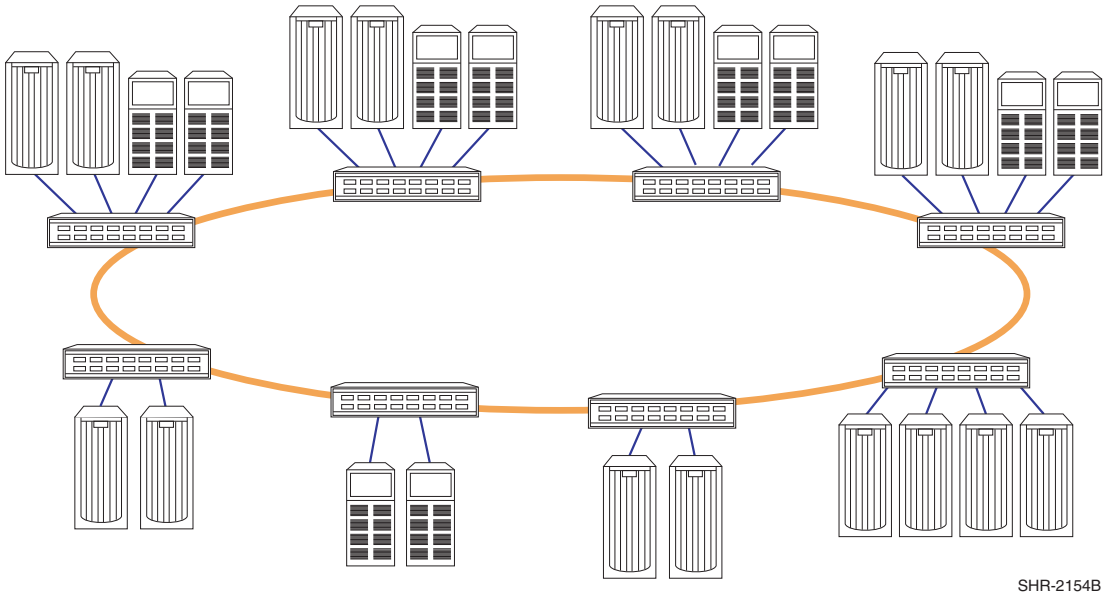


Figure 5: Ring Fabric SAN

If you use fewer than 12-switches in a ring constructed using B-Series product line switches, you can add additional switches to the outside of the ring. These satellite switches provide additional user ports with only a slight reduction in fabric availability. For example, 11 satellite switches can be connected to a 11-switch ring. This results in a 22-switch fabric and maintains the overall seven hop limit. Figure 6 shows a 22 -switch fabric.

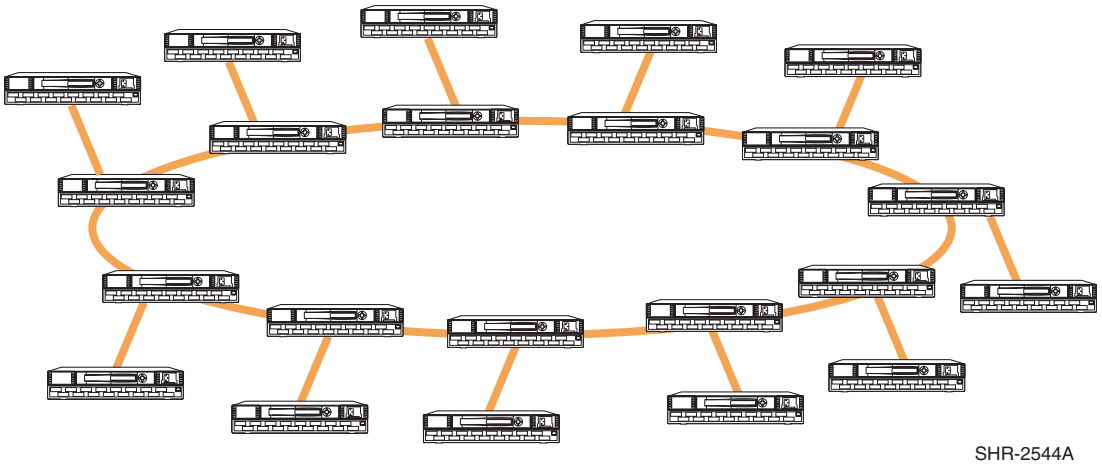


Figure 6: Ring Fabric SAN with Satellite Switches

Ring fabric designs are well suited to applications where data access is always localized. Servers and the storage that is accessed are on the same switch, and the majority of data traffic is handled within that switch. This implementation provides a way to scale the fabric in a modular fashion by adding a switch and groups of servers and storage as a cell, using a building block approach to increase the size of the SAN over time. This is particularly useful in situations where the storage capacity requirements vary over time, such as in a storage service provider environment.

A ring fabric can be pre-configured and installed before the server requirements are known. This is useful because the ability to install the fabric infrastructure beforehand can greatly simplify the installation of each incremental storage system or server. Interconnecting the switches in a ring topology provides a communication path that supports centralized SAN management and centralized backup.

The ring fabric is not recommended for applications that require many-to-many connectivity.

Advantages of Ring Fabrics

- Easy to build

  Each Fibre Channel switch can support servers and storage, thus saving time and effort on SAN design and implementation.

- Scaling is simple and non-disruptive

  Fibre Channel switches can be added one at a time, as storage and connection needs dictate. Each Fibre Channel switch can support identical servers and storage for controlled growth, or can support a variety of heterogeneous systems for new demands of the business.

- Shared backup is supported

  One or more Automated Tape Libraries can be added to the ring fabric at various points without impacting performance or management.

- Shared management is supported

  All Storage Management Appliance tools can navigate and manage a SAN with a ring topology, saving time and effort.

- Optimal local access is inherent in the fabric design

  The majority of the data traffic is within each switch in the ring, minimizing any allocation, fabric and performance issues.

- Modular design

  Saves time and effort on design and implementation by complementing the basic modularity of all StorageWorks products, including the raid array controllers, universal packaging, and secondary storage (Automated Tape Libraries).

Backbone Fabric

A backbone fabric has one or more Fibre Channel switches primarily dedicated to connecting to other switches within the fabric. The backbone switches provide high bandwidth and redundant connectivity to the other switches. This type of implementation offers the best "many-to-many" connectivity.

Backbone fabrics are well suited for implementations where the primary requirement is for full network “many-to-many” connectivity with high performance. They are the most conservative design approach in cases where the I/O traffic patterns are unknown or varying. They are also the best design to choose if you plan to implement SAN-wide storage pooling and sharing, and for environments that use storage virtualization.

Figure 7 shows a backbone fabric where the switches in the center are dedicated to providing connections between the other switches. The switches to which servers and storage can be connected are called “edge switches”, and the switches in the center are called “backbone switches”. Servers and storage can be connected to the user ports on any of the edge switches, which maximizes the flexibility of how you use the user ports.

If required, you may choose to connect centralized primary (disk) or secondary (tape) storage directly on the backbone switches. This approach may be useful if excess ports are available on the backbone switches.

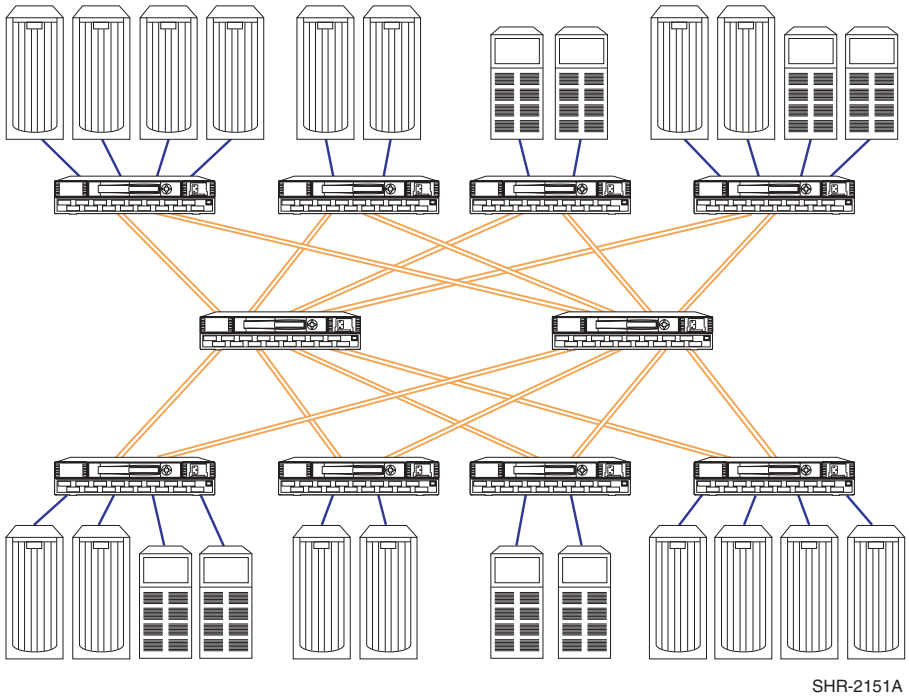


Figure 7: Backbone Fabric SAN

HP StorageWorks SAN fabrics currently support a large number of switches in a fabric. Figure 8 shows a large backbone fabric SAN with 20 switches. Configurations of this type can be used to support the most demanding requirements for storage system size and performance.

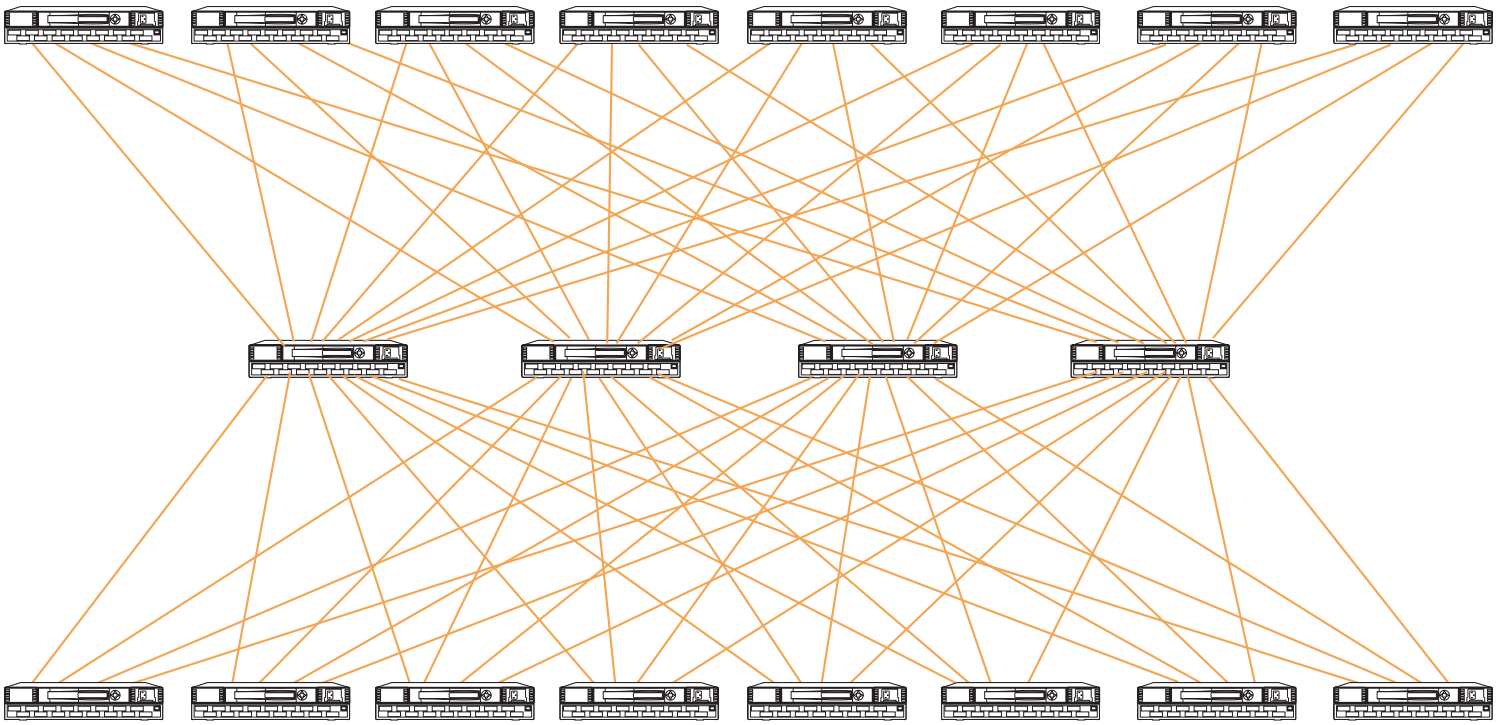


Figure 8: Backbone SAN with 20 Switches

Fat Tree and Skinny Tree Designs

The SAN shown in Figure 7 can be drawn with the backbone switches at the top and the edge switches collected together into a row at the bottom, as shown in Figure 9. This method of illustrating the topology is helpful when evaluating the potential performance of a given backbone configuration. It shows the switches in a hierarchy, where the edge switches form a layer that provides access to the SAN and the backbone switches form a layer that distributes I/O requests between edge switches.

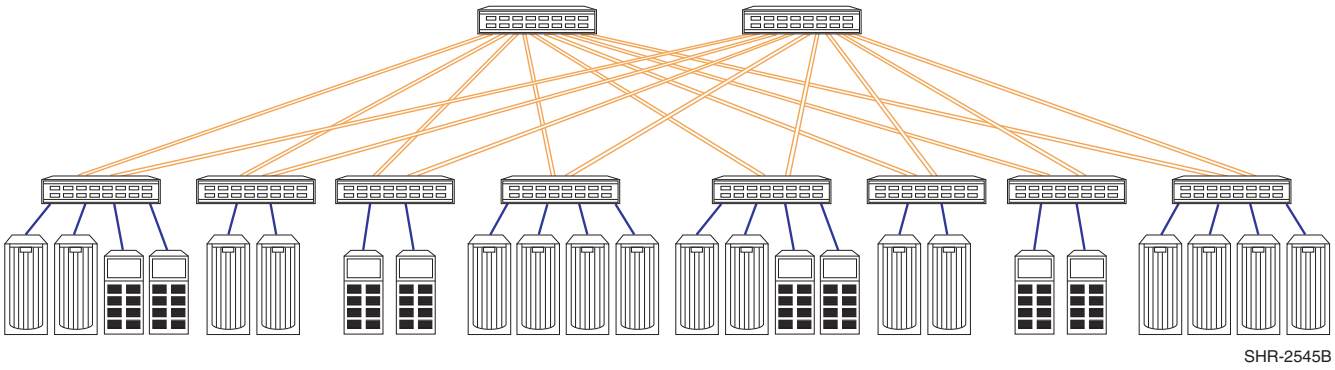


Figure 9: Backbone SAN, Drawn Hierarchically

Depending on how a backbone SAN is designed it can be classified as a “fat tree” or a “skinny tree”. The difference between fat and skinny trees is the number of ISLs used to connect the edge switches to the backbone switches. The number of ISLs subtracts from the number of end ports and therefore affects the total number of switches needed for a particular configuration. Fat trees use 50% of the edge switch ports as ISL connections while skinny trees use fewer than 50%.

Figure 10 shows two hierarchical SAN fabrics. The skinny tree illustration shows that if all the devices connected to user ports on the left-hand side of the tree want to communicate with the devices on the right-hand side of the tree, then there are not enough connections to the switch at the top of the tree for the required traffic. There are too many port-pairs trying to use the ISLs on the switch at the root of the tree. The fat tree illustration shows that by providing additional ISLs between the switches that are further up in the hierarchy, full-performance bandwidth can be provided for *any combination of port-pairs.* This important benefit is the basis for the use of fat tree configurations in application environments where the highest level of performance and capability are required.

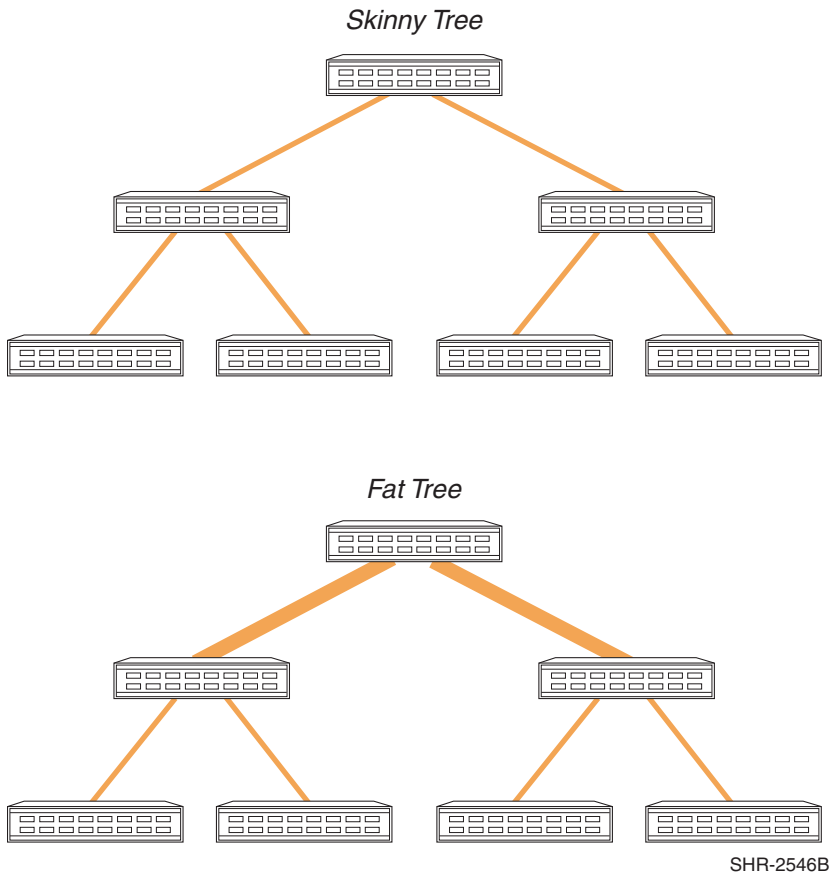


Figure 10: Skinny Tree and Fat Tree

This distinction in the number of ISL connections between fat and skinny trees results in two major differences:

1. Skinny trees require fewer switches than fat trees to supply the same number of user ports. Figure 11 shows how six 16-port switches in a skinny tree configuration yield 64 user ports, while the same switches wired in a fat tree as shown in Figure 12 yield only 32 user ports.
2. Fat trees have more ISL connections and therefore have higher cross sectional bandwidth capabilities than skinny trees. The term cross sectional bandwidth is used to refer to the maximum amount of data that can pass through the ISL connections at the midpoint of the fabric.

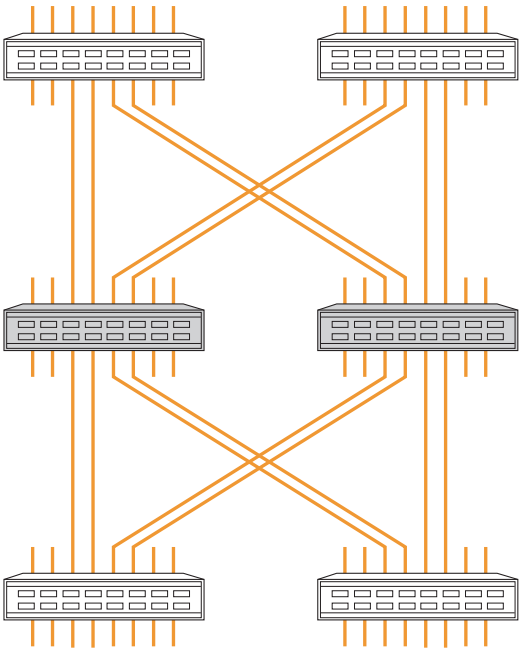


Figure 11: 64-Port Skinny Tree

The configuration shown in Figure 11 has six 16-port switches. Two are backbone switches (shaded) and four are edge switches. The edge switches each have 12 user ports available to connect to servers or storage. With the 48 ports on the edge switches and with the 16 available ports on the backbone switches the total number of user ports is 64.

There are 8 ISLs on each side of the backbone switches.

Note that a mix of 1 Gbps and 2 Gbps switches or devices makes the evaluation of this type of configuration more complicated.

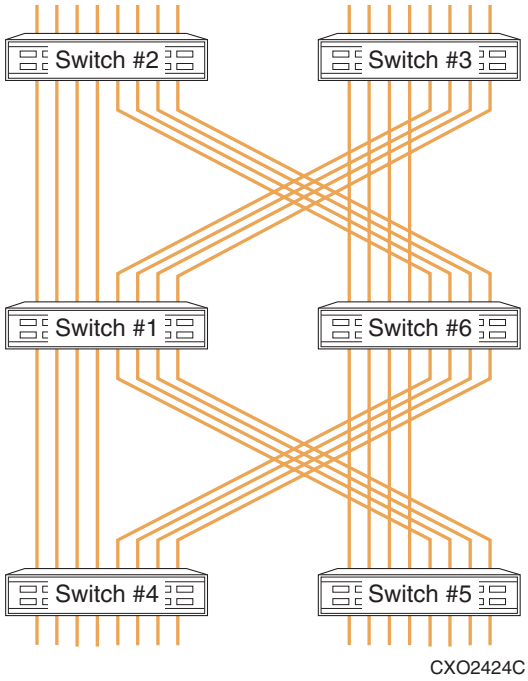


Figure 12: 32-Port Fat Tree

The configuration shown in Figure 12 also has six 16-port switches, with two backbone switches and four edge switches. The edge switches each have eight user ports available to connect to servers or storage. No ports are available on the backbone switches for user ports, so the total number of user ports is 32.

The two configuration designs shown are utilized in the HP Surestore FC Switch 6164 and the Compaq StorageWorks SAN Switch Integrated/32 and 64.

Backbone SANs Using Core Switches and Directors

With the introduction of switches with a higher number of ports, backbone fabrics may be constructed using a mix of small and large switches. The HP standard SAN designs using this approach are as follows.

The “4 x 12” configuration, shown in Figure 13, uses a mixture of HP StorageWorks Core Switch 2/64 and SAN Switch 2/16 or SAN switch 16 devices. Four core switches are connected in a mesh configuration with two ISLs between each pair of switches in the mesh. Twelve SAN switches are connected to the mesh with four ISLs between each SAN switch and the mesh. This gives a total of 304 user ports, including 160 on the mesh and 144 on the SAN switches.

This configuration is useful for situations where a large port count is required in a single fabric, and where many high-performance systems can make use of direct connections to the mesh. For example, high performance storage systems can make good use of a 2 Gbps connection, and should be connected directly to the mesh. Since each 16-port SAN switch has four ISLs connecting it to the core, the 8 Gbps (4 x 2 Gbps) total bandwidth between the SAN switch and the mesh must be shared between the 12 user ports on that switch. This means that the I/O performance requirement for each server attached to a SAN switch in this configuration must be reviewed to make sure that the ISLs are not an I/O bottleneck. Because of the limited number of ISLs between the switches in the mesh, this configuration is not appropriate for environments where many-to-many traffic patterns are predominant.

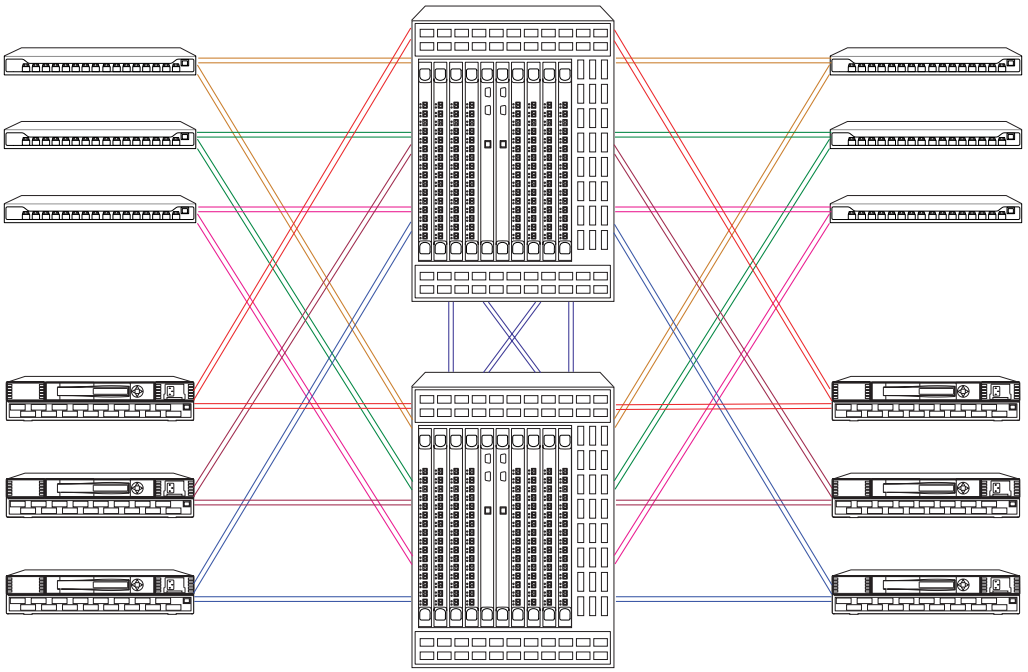


Figure 13: "4 x 12" Backbone SAN

The "4 x 24" configuration also uses a mixture of HP StorageWorks core switch and SAN switch devices. By using a larger number of switches, this topology design provides adequate internal connectivity within the mesh and also provides and more user ports than the 4 x 12 configuration.

In the 4 x 24 configuration, shown in Figure 14, four core switches are connected in a mesh with four ISLs between each pair of switches in the mesh. 24 SAN switches (1 Gbps or 2 Gbps models) are connected to the mesh, with a total of four ISLs on each SAN switch (just the same as in the 4 x 12 configuration). This gives a total of 400 user ports, including 112 on the mesh and 288 on the SAN switches. This configuration may provide a better trade-off of high-performance connections—directly to the core switches—and lower-performance connections on the SAN switches.

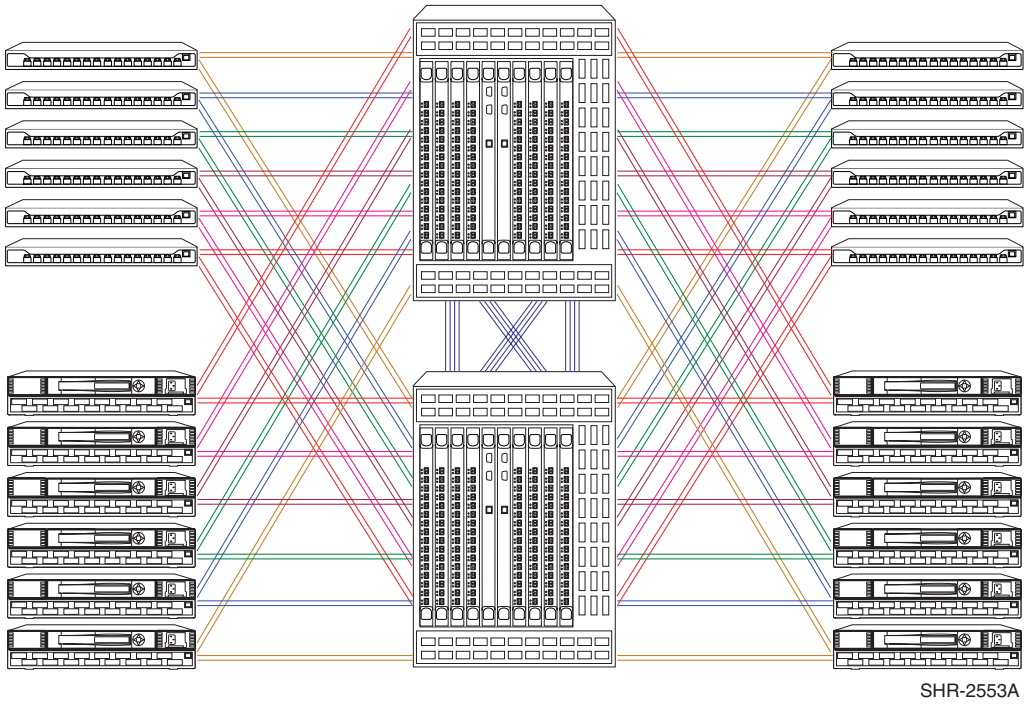


Figure 14: "4 x 24" Backbone SAN

Director Fabrics

Backbone fabrics may be constructed using Director and Edge switches. These products may be used in configurations where no more than half of the ports on a given switch is used for ISL connections. This means that a fat tree configuration cannot be constructed because the distribution layer cannot be fully populated. On the other hand, there are fewer topology restrictions for these products, so you can combine a mixture of Director and Edge switches, with a single Director as the backbone, to make a skinny tree fabric.

For example, a skinny tree using the design shown in Figure 11, but using 64-port Directors, meets the ISL port count and hop count requirements for this family of products while providing 256 user ports.

Figure 15 shows a "Director plus Edge switch" tree design using two HP StorageWorks Directors and 14 HP StorageWorks Edge switches. In this topology, high performance storage systems are connected directly to the Directors, because they can make use of the full bandwidth of the 2 Gbps Fibre Channel connections. Servers are connected to the edge switches, because they require only a smaller amount of bandwidth. Depending on the bandwidth requirements of the servers, the number of ISLs between the edge switches and the Directors can be varied.

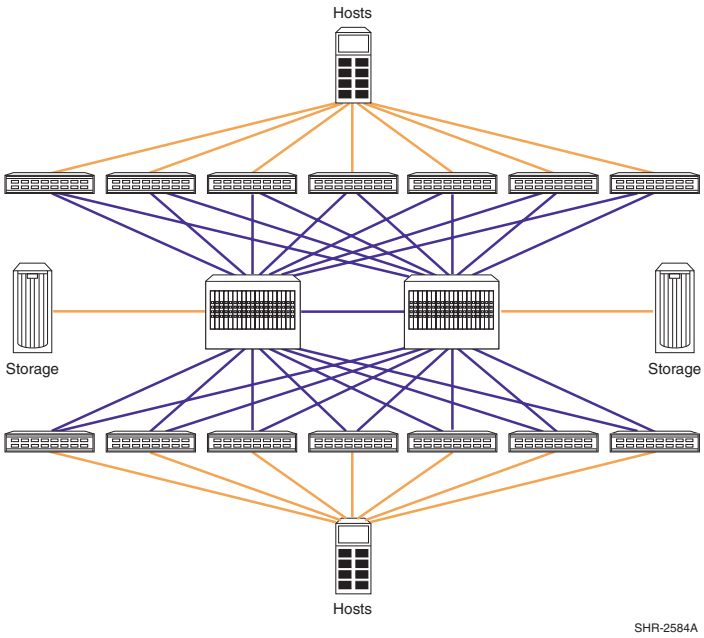


Figure 15: Director plus edge switch SAN

Advantages of Backbone SANs

- Efficient port expansion: new switches need only be connected to backbone switches.

  Saves time and effort during the design and implementation phases by isolating the new switches from the existing SAN backbone.

- All edge switches are only two hops apart.

  Saves design effort for adding new servers and storage to any point on the SAN. The uniformity of access supports new usage patterns without requiring redesign and re-cabling.

- When implemented with two or more backbone switches, provides a level of switch redundancy in a single fabric.

  Backbone design allows Fibre Channel switches to automatically re-route under failure conditions, saving time and effort to manually trace the problem and re-route.

- Can be centrally managed.

  All Storage Management Appliance tools can navigate and manage the Storage Area Network in a tree backbone fabric, saving time and effort.

- Full "many-to-many" connectivity with evenly distributed bandwidth and redundant connectivity.

  Supports varying connection and performance demands regardless of the location within the SAN. At the same time, provides uniform routing and redundancy from a single SAN design.

- Improved bandwidth with multiple parallel ISLs.

  Additional ISLs ensure that all data traffic within the tree backbone SAN will be managed with less performance degradation, regardless of the location of servers and storage relative to each other.

- Offer maximum flexibility for implementing mixed access types: Local, Distributed, or Centralized.

  Saves effort planning data traffic patterns; the tree backbone supports all access patterns.
- Can be implemented with centralized backup capabilities, reducing the cost of backup and restore operations
- Can be implemented with all availability levels

  Saves effort in the design and implementation phases by offering a single design for a variety of usage requirements.
- Can be an upgrade path from other SAN designs. Backbone SAN designs offer evenly distributed bandwidth and full many-to-many connectivity; they are the best solution for flexible SAN-wide storage pooling and sharing.
- Well-suited to take full advantage of expected future technological developments such as storage virtualization

  Saves the investment made in the SAN by continuing its use as more advanced tools, products, and designs become available.

Topology Data Access Usage

The various SAN topology options can be characterized by how well they support specific data access patterns. Refer to Chapter 1, "Data Locality". Table 10 provides a general characterization of the different topology designs as a means to compare each of the design types by optimal data access capabilities. Use the table as a basis for selecting the best-suited topology for your expected access needs.

Individual topologies can be tailored or modified to better meet specific requirements. For example, choosing a fat tree backbone design provides the best overall “many-to-many” connectivity, and allows portions of the tree implementation to be configured for local access. This can be accomplished by connecting servers and storage typically accessed on the same switch within portions of the tree backbone.

Table 10: Topology Usage Rating

SAN Topology	Data Locality		
	Local “One-to-One”	Centralized “Many-to-One”	Distributed “Many-to-Many”
Cascaded	Highest	Not Recommended	Not Recommended
Meshed	Medium	Medium	High
Ring	Highest	Medium	Not Recommended
Skinny Tree Backbone	Medium	High	High
Fat Tree Backbone	High	Highest	Highest
Single Switch	Highest	Highest	Highest

Topology Maximums

Table 11, Table 12, and Table 13 indicates the maximum number of switches and ports supported for each of the HP standard SAN topologies.

Note: The maximums shown assume the use of the minimum number of ISLs. Depending on your specific application, you may need more ISLs. This reduces the overall number of ports available for servers and storage. Attaching the Storage Management Appliance also reduces the total number of ports available for servers and storage. See Chapter 6, "SAN Management."

Table 11: Topology Maximums when using B-Series Product Line Switches

SAN Topology	Maximum Number of Switches	Maximum Total Number of Ports	Maximum Number of User Ports
Single Switch	1	64	64
Cascade	28	896	840*
Mesh	28	896	734*
Ring	15	480	450*
Ring with Satellite Switches	22	704	660*
Backbone (4 by 12 with 4 core switches and 12 SAN switches)*	28	640	608
Backbone (4 by 12 standard configuration)	28	640	496
Backbone (4 by 24)	28	1024 - 1280 (Refer to Chapter 3, SAN Fabric Design Rules, for specific configuration rules.)	728 - 1200

Note: *While this is a valid configuration, it achieves a high user port count by severely limiting the connectivity within the SAN by using 1 ISL between each switch pair.

Note: Refer to Chapter 3, SAN Fabric Design Rules, for specific configuration maximums.

Table 12: Topology Maximums when using M-Series Product Line

SAN Topology	Maximum Number of Switches	Maximum Total Number of Ports	Maximum Number of User Ports
Single Switch	1	140	140
Cascade	24 (maximum of 8 Directors)	1,632	1024 (cascade with 8 Directors, plus 16 edge switches)
Mesh	Not Applicable, Exceeds Hop Count Limit	Not Applicable	Not Applicable
Ring	7	980	966
Ring with Satellite Switches	Not Applicable	Not Applicable	Not Applicable
Backbone	24	1632	1024

Note: Refer to Chapter 3, SAN Fabric Design Rules, for specific configuration maximums.

Table 13: Topology Maximums when using C-Series Product Line Switches

SAN Topology	Maximum Number of Switches	Maximum Total Number of Ports	Maximum Number of User Ports
Single Switch	1	224	224
Cascade	11	512 (maximum of 2 Directors)	440 (cascade with 2 Directors and 9 fabric switches)
Backbone	11	512 (maximum of 2 Directors)	440

Data Availability in a SAN

Data availability in a computer installation is influenced by many factors, including the application software and operating systems in the servers, the server hardware, the SAN fabric infrastructure, and the primary and secondary storage. Operational parameters including backup schedule and machine room procedures, as well as personnel issues and overall administrative practice all make important contributions to the availability of data in a computer system environment.

In some environments, adequate data availability is established by a routine backup procedure performed on a scheduled basis. In other cases, online dynamic backup of primary data to a remote site is required. Some environments use clustered servers and redundant fabrics in their SAN systems in order to achieve their data availability goals.

When considering SAN fabric topology selection, the number of Fibre Channel switches and the number of ISLs between the switches have the largest effect on the data availability. The number of connections or paths between a given server or clustered servers and the fabric, and the number of storage controller connections or paths into the fabric also affect data availability.

From the perspective of SAN architecture and fabric topology design, fabric availability can be classified into at least four categories or levels. The different categories offer a range of availability levels from the most basic interconnect scheme with no redundancy, up to fully redundant No Single Point Of Failure (NSPOF) designs.

Levels of Availability

1. Single Fabric/Single Server and Storage Paths
2. Single Meshed Fabric/Single Server and Storage Paths
3. Single Meshed Fabric/Multiple Server and Storage Paths
4. Multiple Fabrics/Multiple Server and Storage Paths

Level 1: Single Non-meshed Fabric/Single Server and Storage Paths

These designs are implemented with single links between each switch, connected in one fabric. The Fibre Channel switches are arranged so that servers and storage connect into the fabric using single paths. This type of design does not provide any level of fabric or fabric path redundancy.

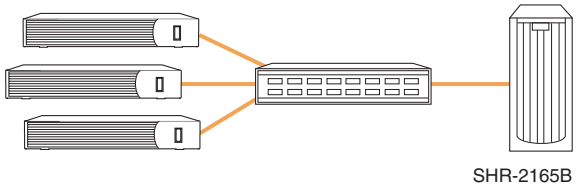


Figure 16: Level 1: Maximum Connectivity

Level 2: Single Meshed or Cascaded Fabric/Single Server and Storage Paths

These designs have more than one ISL between switches and/or multiple paths or routes to all switches in the fabric. Servers and storage connect into the fabric using single paths. This provides the benefit of fabric resiliency. If a single switch port or a link between two switches fails, the fabric automatically re-routes data to an alternate fabric link or route. The servers see no interruption in their I/O flow.

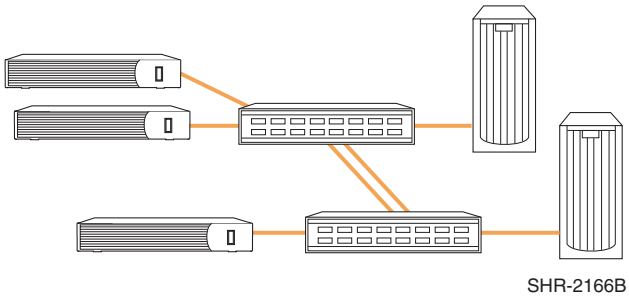


Figure 17: Level 2: Fabric Resiliency

Level 3: Single Meshed or Cascaded Fabric/Multiple Server and Storage Paths

These designs are the same as Level 2 with the addition of multiple data paths between servers and storage connecting into one fabric. Level 3 offers the benefits of both fabric resiliency and multiple server and storage paths. In the unlikely event of a switch, host bus adapter, or path failure, data is automatically re-routed to an alternate path in the servers and storage, and through the fabric. The servers see no interruption in their I/O flow. Level 3 may require (depending on the O/S) the use of fabric zoning to define a minimum of two separate paths in a single fabric. To ensure high availability, each HBA must be cabled to a different switch and be configured for access to a different storage system controller when set in multiple-bus failover mode. Each controller must be cabled to a different switch, as shown in Figure 18.

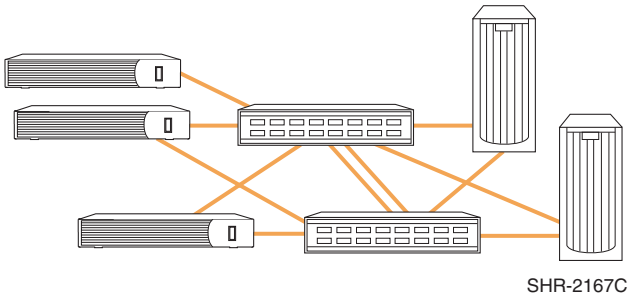


Figure 18: Level 3: Single Fabric High Availability Multi-Pathing

Level 4: Multiple Fabrics/Multiple Server and Storage Paths

Like Level 3, Level 4 provides for multiple data paths between servers and storage, but in the Level 4 designs these paths are connected to physically separate fabrics. This type of design provides the highest level of availability and offers no single point of failure protection (NSPOF). Any event that may affect the fabric performance or usability will be overcome by routing data to another alternate fabric. The servers see no interruption in their I/O flow.

The Level 4 design eliminates any vulnerability to fabric failures, for example, human error such as improper switch replacement procedure, inadvertent erroneous fabric configuration settings, or a fabric service failure. This type of design also provides the highest level of performance and a higher number of available ports, since all fabrics can be accessed and utilized simultaneously during normal operations. This also allows for nondisruptive upgrades.

This level of protection is available for all HP standard SAN topologies by replicating the chosen design in two separate fabrics. HP recommends that the two fabrics have similar or identical topologies. Although this may increase the overall cost of the implementation, the added benefit beyond the increase in data availability is an increase in total available ports. For example, choosing to implement a single meshed fabric design using four switches provides

up to 52 ports for server and storage connectivity. Implementing the same topology using two fabrics provides up to 104 ports for server and storage connectivity. This is shown in Figure 19.

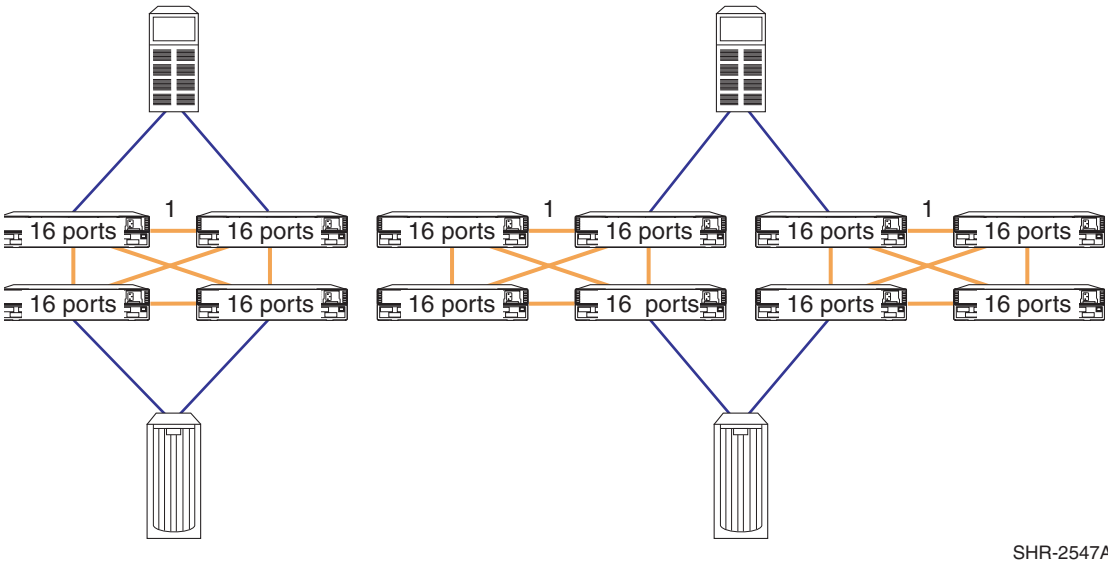


Figure 19: Single Fabric and Dual Fabric SANs

Using two fabrics allows for non-disruptive software and firmware code updates. For example, given the two fabrics shown in Figure 20, you can failover operations to Fabric B, upgrade Fabric A, then failback operations to Fabric A. The procedure can then be repeated in reverse to upgrade Fabric B.

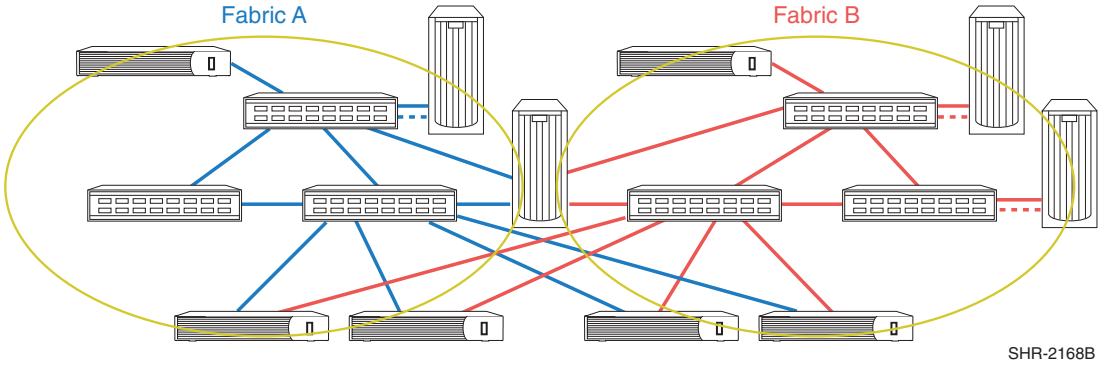


Figure 20: Level 4: Dual Fabric High Availability Multi-Pathing Fault Tolerant

Table 14 characterizes data availability and indicates the supported topologies for each level.

Table 14: Fabric Design Data Availability

Fabric Design		Availability Level	SAN Topologies
Single Fabric (Non-Meshed)	1	No Redundancy	Single Switch or Multiple Switches with Single ISL Cascade
Single Meshed Fabric Multiple Fabric Paths	2	Medium	Two ISL Cascade, Meshed, Ring, Tree
Single Meshed Fabric Multiple Fabric Paths Multiple Server and Storage Paths [1]	3	High	All
Two (or more) Fabrics Multiple Server and Storage Paths	4	Highest (NSPOF)	All

1. May require the use of zoning to define a minimum of two separate data paths within the single fabric. This is platform dependent.

Availability Design Considerations

Two major considerations in choosing an availability level are the criticality of data access and cost. For mission critical applications, first consider full redundant fabric designs. The additional cost can usually be justified when you consider the cost associated with the loss of access to critical data.

You should also remember that the additional cost of more than one fabric provides more than redundancy since the number of available ports will typically double. If this increased connectivity can be utilized by adding more servers and storage to the SAN, the cost factor is minimized. Figure 15 characterizes data availability levels relative to cost and total number of available ports.

Table 15: Availability Cost Factors

Fabric Design	Level	Hardware Cost Factor[1]	Available Ports[2]
Single Fabric (Non-Meshed)	1	x	n - #ISL Ports
Single Meshed Fabric Multiple Fabric Paths	2	x + Additional ISLs	n - #ISL Ports
Single Meshed Fabric Multiple Fabric Paths Multiple Server and Storage Paths [3]	3	x + Additional ISLs + Additional HBAs	n - #ISL Ports - Additional HBA Ports
Two (or more) Fabrics Multiple Server and Storage Paths	4	x + Additional ISLs + Additional HBAs + Additional Switches	2n - #ISL Ports - Additional HBA Ports

1. The variable x is the cost of a single non-meshed fabric. It is used as a reference for comparison.
2. The variable n is the total number of ports available for devices in a SAN fabric.
3. May require the use of zoning to define a minimum of two separate data paths within the single fabric. This is platform dependent.

Scalability and Migration

Each of the HP standard SAN topologies can be scaled incrementally to increase connectivity and overall capacity. You should always plan for expected future growth in your initial SAN design to minimize disruption when expanding capabilities and capacity over time. If you do exceed the capacity of a given topology, or find that data access needs have changed, it is possible to migrate one topology to another. Refer to Chapter 11, "Best Practices" for information about migrating topologies.

Table 16 lists the migration paths and the options for scalability for all topologies.

Table 16: Topology Migration & Scaling

SAN Topology	Migration	Scalability (For All Topologies)
Cascaded	Convert to Meshed, Ring or Tree	• Increase the number of switches
Meshed	Convert to Ring, or Tree	• Use higher port count switches
Ring	Convert to Meshed or Tree	• Transition to a different topology
Tree	Add additional backbone switches	• Deploy multiple fabrics

Custom-Designed SAN Topologies

The HP standard SAN topologies, or subsets of these topologies, as discussed in this chapter, can meet most SAN implementation requirements. There may be specific cases where HP standard topologies (or variants) do not meet your specific needs or requirements. In these cases, a custom SAN design can be created if the SAN design rules described in this document are strictly followed. Refer to Chapter 3, "SAN Fabric Design Rules", Chapter 4, "Heterogeneous SAN Platform and Storage System Rules", and Chapter 11, "Best Practices".

SAN Fabric Design Rules

3

The sections in this chapter contain SAN fabric design configuration rules for heterogeneous SANs implemented using the HP B-Series product line of Core and SAN Switch Fibre Channel switch models, HP M-Series product line of Director and Edge Fibre Channel switches, and for the HP C-Series product line of Cisco Director and Fabric Fibre Channel switch models resold by HP.

Support is provided for SAN fabrics consisting of the Fibre Channel switches listed in Table 17, HP StorageWorks B-Series Product Line Switches, the switches listed in Table 18, HP C-Series Product Line Switches, or the switches listed in Table 20, HP StorageWorks M-Series Product Line Switches.

For new SAN deployments HP recommends you utilize switch models from a single product line exclusively. To meet the needs of customers desiring a mix of switch models from the different product lines however, HP also supports two levels of SAN fabric interoperability. Specifically, HP supports:

- Within a multi-fabric SAN, one fabric with all B-Series switches and another fabric with all M-Series switches. This is referred to as a "dual heterogeneous SAN fabric"
- Within a single fabric, M-Series Director and Edge switch models intermixed with B-Series SAN switch models This is referred to as an "interoperable heterogeneous SAN fabric"
- Within a single fabric, C-Series Director and Fabric switch models intermixed with B-Series switch models.

Refer to Heterogeneous/Interoperable SAN Fabrics, page 77, for the fabric interoperability rules and configuration rules for these two levels of interoperability.

The configuration rules for a SAN begin with the SAN fabric rules. These are then modified depending on the specific topology implementation rules, platform or operating system and storage system rules described here and in Chapter 4, **"**Heterogeneous SAN Platform and Storage System Rules**",** and the requirements of applications being run on the SAN. Read the documentation and release notes for all hardware and software products that are being utilized in the SAN for additional configuration information details. See the Preface, "Related Documents" for a list of related documentation.

SNIA SSF Configurations

The Storage Networking Industry Association (SNIA) sponsors the Supported Solutions Forum (SSF). SSF is a storage industry program that improves the interoperability of Fibre Channel products. HP is a member of SNIA and SSF.

HP supports a number of Fibre Channel switch models in configurations that are compliant with the guidelines defined by the SNIA Supported Solutions Forum. SSF has defined numerous configurations with heterogeneous servers and heterogeneous storage systems.

For additional information on this program, refer to http://www.snia.org/ssf

Supported Switch Models – B-Series Product Line

HP supports a range of 1 Gbps and 2 Gbps SAN B-Series product line Fibre Channel switch models. These switch models represent products supported by both pre-merger HP and pre-merger Compaq. The relationship between the pre-merger and post-merger switch products is shown in Table 17. Refer to the section, SAN Fabric Rules – B-Series Product Line, for specific switch model support rules.

Table 17: HP StorageWorks B-Series Product Line Switches

HP StorageWorks Switch Name		Firmware Version	Number of Ports
HP StorageWorks MSA SAN switch 2/8		3.1x	8
HP StorageWorks SAN Switch 2/8 EL, 2/8 Power Pak			8
HP StorageWorks SAN Switch 2/16, 2/16 EL, 2/16 Power Pak			16
HP StorageWorks SAN Switch 2/32, 2/32 Power Pak		4.1x	32
HP StorageWorks Core Switch 2/64, 2/64 Power Pak			64 (2 switches per chassis, for a total of 128 ports per chassis)
HP Switch Name	**Compaq StorageWorks Switch Name**		**Number of Ports**
HP Brocade 2400 (HP reseller)	Compaq StorageWorks SAN Switch 8	2.6.1x	8
N/A	Compaq StorageWorks SAN Switch 8-EL		8
HP Brocade 2800 (HP reseller)	Compaq StorageWorks SAN Switch 16		16
N/A	Compaq StorageWorks SAN Switch 16-EL		16
HP Surestore FC Switch 6164 (64 ISL Ports)	Compaq StorageWorks SAN Switch Integrated/32 (64 ISL Ports)		32 (counts as 6 switches and 2 hops when applying configuration rules)
HP Surestore FC Switch 6164 (32 ISL Ports)	Compaq StorageWorks SAN Switch Integrated/64 (32 ISL Ports)		64 (counts as 6 switches and 2 hops when applying configuration rules)
HP Surestore FC 1Gb/2Gb Entry Switch 8B	N/A	3.1x	8
N/A	Compaq StorageWorks SAN Switch 2/8-EL		8
N/A	Compaq StorageWorks SAN Switch 2/16-EL		16
HP Surestore FC 1Gb/2Gb Switch 8B	N/A		8
HP Surestore FC 1Gb/2Gb Switch 16B	Compaq StorageWorks SAN Switch 2/16		16

SAN Fabric Rules – B-Series Product Line

All switch models shown in Table 17 are supported in the HP StorageWorks SAN provided that the same firmware versions and switch settings for each switch model family are utilized for the corresponding models listed, and specific switch model configuration rules are followed. For additional information on operating system HBA/driver/firmware/software support, contact your HP field representative.

- For SAN fabrics consisting exclusively of Compaq switch models or a mix of pre-merger HP and pre-merger Compaq switch models (Compaq StorageWorks switch name, HP switch name, or Brocade switch name sold by HP in the above table), use the Compaq default switch settings. Configuration files with these settings are available from HP Services.
- For SAN fabrics consisting exclusively of pre-merger HP switch models (HP switch name or Brocade switch name sold by HP in the above table), utilize pre-merger HP switch settings. Configuration files with these settings are available from HP Services.

Note: The HP StorageWorks switches listed utilize common settings by default.

Fabric and Switch Model Maximums - B-Series Product Line

The fabric maximums listed are for B-Series switch model SAN fabrics utilizing HP XP128/1024, XP48/512, XP256, VA7100, VA7110, VA7400, VA7410, Enterprise Virtual Array (EVA), EMA/ESA12000, EMA16000, MA/RA8000, MA6000, MSA1000, RA4000, or RA4100 storage systems. Refer to Chapter 4 for specific operating system support for each storage system type based on the switch product line used.

In general, these fabric rules also apply to Continuous Access XP, EVA, and DRM for EMA/ESA12000, EMA16000, and MA/RA8000. Refer to Chapter 4 of this guide and the Continuous Access EVA Design Reference Guide for additional details.

The following rules are for SAN fabrics implemented with versions 2.6.1x, 3.1x, and 4.1x switch FW unless otherwise stated.

1. Up to 28 switches and up to 1280 total ports in a single SAN fabric. Each fabric may contain any combination of supported 1 Gbps and 2 Gbps switch models listed, provided the individual switch model fabric limits listed below are not exceeded.
2. The HP StorageWorks core switch 2/64 – maximum of 10 chassis total per fabric, each chassis contains 2 logical switches (See Figure 21), thus 10 chassis add 20 to the fabric switch count. Maximum fabric configuration is 10 chassis with 8 other 8-port, 16-port, or 32-port switches.

   The Core Port Identifier (PID) addressing mode is required on all other switches in the same fabric with the HP StorageWorks SAN Switch 2/32 and Core Switch 2/64. Refer to SAN Core and SAN Switch Addressing Mode.
3. For SAN fabrics containing any 1 Gbps switch models utilizing 2.6.1x or later firmware, the maximum number of user ports supported is 728. With Security enabled, the maximum number of user ports supported is 500.
   For SAN fabrics containing exclusively 2 Gbps switch models, the maximum number of user ports supported is 1200. With Security enabled, the maximum number of user ports supported is 728.

4. For SAN fabrics with Security enabled, the Security database sizes are limited as follows.
   - In a mixed fabric with 1 and 2 Gbps switches, the maximum size of the security database is 32 KB, with only 16 KB active.
   - In a 2 Gbps only fabric, the security database size can be 128 KB, with 64 KB active.
   - For all 1 Gbps/2Gbps mixed fabrics, the maximum number of Device Connection Control (DCC) policies is limited to 620.
5. Zoning database size limits - For SAN fabrics containing 1 Gbps switch models utilizing 2.6.1x or later firmware, or 2 Gbps switch models utilizing 3.1x or later firmware, the zoning database size must not exceed 96 KB.
   For SAN fabrics containing 2 Gbps switch models utilizing 4.1x or later firmware, the zoning database size must not exceed 128 KB.

Note: Use the "cfgSize" command to determine the size of the Zoning database.

---

6. StorageWorks SAN Switch Integrated 32 or 64, HP Surestore FC Switch 6164 – maximum of 4 chassis total per fabric, each chassis adds 6 switches to the fabric switch count. Maximum fabric configuration is 4 chassis with 4 other SAN switch model switches.
7. Up to 7 switch hops (8 switches) maximum between any two devices in a SAN fabric. Each SAN Switch Integrated 32 or 64 or HP Surestore FC Switch 6164 model switch utilized in a fabric adds up to 2 hops to the hop count between devices depending on the specific device-to-switch connections and device-to-device access. (refer to Chapter 2, Figure 6 and Figure 7).
8. StorageWorks SAN Switch 2/8-EL – By default, this switch is supported in SAN fabrics with up to 4 switches total only. A license upgrade is available to allow these switches to be upgraded for support in larger fabrics with greater than 4 switches total.
9. HP Surestore FC 1Gb/2Gb Entry Switch 8B – Supported with a single E-port connection.
10. Compaq Fibre Channel Storage Switch 8 or Fibre Channel Storage Switch 16 models– up to 4 switches total per fabric using these model switches only, or when intermixed with 1 Gbps SAN switches.

Note: Intermixing of Compaq Fibre Channel Storage Switch 8 and Fibre Channel Storage Switch 16 models and 1 Gbps StorageWorks SAN Switch models requires compatibility mode (VC Encoded Address Mode) be set in the SAN Switches (refer to the SAN Switch documentation). Intermixing of 1 Gbps Compaq Fibre Channel Storage Switch 8 or Fibre Channel Storage Switch 16 switch models and 2 Gbps switch models is not supported

---

11. The Compaq FC-AL Switch 8 is supported for cascaded attachment to the SAN through a single FL-port on a Compaq SAN Switch 8, SAN Switch 16, SAN Switch 8-EL, or SAN Switch 16-EL. In this configuration, RA4000/4100 storage systems are accessible only from servers attached directly to the FC-AL switch.

Note: Cascaded attachment of the FC-AL Switch 8 connected to 2 Gbps switch models is not supported

---

12. Within a single fabric where switches are interconnected, each switch must have a unique domain number (Domain ID) and a unique World Wide Name (WWN). All switch configuration parameters in each switch must be the same.

Note: Do not configure any switches with a domain ID of 8. HP systems reserve domain 8 for Private Loop devices.

---

13. Optional switch features may be used on any switch in the fabric if the feature is supported on that switch. This includes features such as ISL Trunking, QuickLoop, Fabric Watch, Advanced Performance Monitoring, and Extended Fabrics. Refer to the switch model specific documentation to determine which features are available for a given switch model.
14. Any mix of servers and storage systems is allowed in a SAN provided the specific platform, operating system, and storage system fabric limits and rules are followed. Refer to the appropriate sections in this guide and the documentation listed in the section "Related Documents" in the preface.
15. HP requires that all switches in a single fabric or multi-fabric SAN use the same switch firmware revision for each switch model family. Two successive fabric firmware versions can be temporarily used in one fabric or multiple fabrics in a SAN during switch firmware rolling upgrades.
16. For B-Series product line, Table 17 Fibre Channel switches – Up to 15 switches configured in a single ring with a Ring SAN fabric topology and no cascaded switches. Up to 22 switches in a Ring SAN fabric with cascaded switches, provided that no more than 11 switches are in a ring and no more then 11 switches are outside of the ring. One outside switch is cascaded from each of the 11 ring switches.

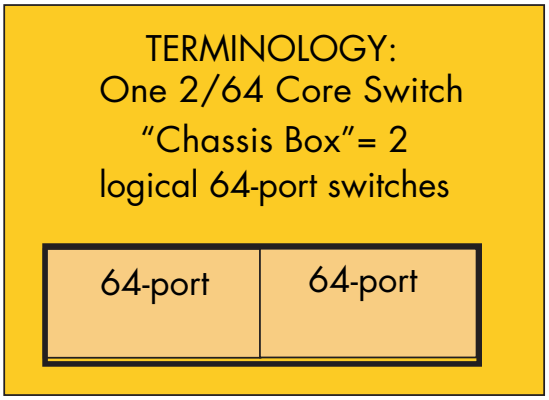


Figure 21: Core Switch definition

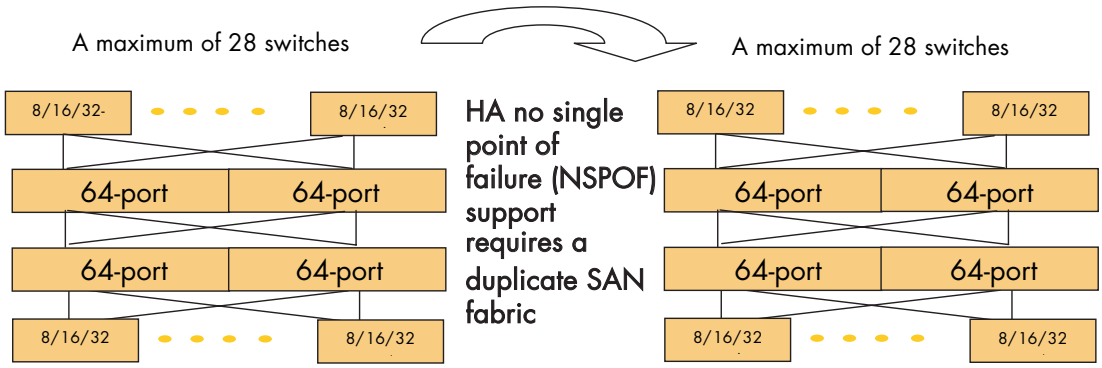


Figure 22: Two Fabrics for high availability

SAN Core and SAN Switch Addressing Mode

When using products from the B-series product line, two different addressing modes are available. As SAN configurations grow to include more switches, HP recommends that the "Core Switch" addressing mode should be used. This is obtained by setting the Core Switch PID configuration parameter bit.

Certain switches previously supplied by HP and Compaq were shipped with the Core Switch PID configuration bit cleared. When the switches are operated in this mode, certain restrictions apply regarding the maximum number of switches in a fabric and the maximum number of ports on a switch. If a StorageWorks Core Switch 2/64 or StorageWorks SAN switch 2/32 is used anywhere in a fabric, then all the switches in the fabric must have the Core Switch PID configuration bit set. Currently, all switches are shipped with the Core Switch PID bit set.

SAN managers with existing fabrics that have switches with the Core PID bit cleared must decide whether to set the Core Switch PID bit now or later. The trade-offs are as follows:

- All switches in a fabric must have the same Core Switch PID bit setting, whether it is set or cleared, otherwise the fabric will segment. It must be set on all switches if a StorageWorks Core Switch 2/64 or StorageWorks SAN switch 2/32 is part of the fabric.
- With two fabrics, the Core Switch PID can be changed on one fabric at a time, allowing the SAN storage system to operate during the changeover.
- HP-UX and IBM AIX systems use the address bits to identify logical units, when the addressing bits are changed, the logical unit definitions must also be changed. This requires a reboot of the servers and cannot be done without taking down the entire SAN storage system in a planned maintenance scenario.
- If the existing switches in a fabric have the Core PID bit cleared, this bit will need to be cleared on any new switches added, since all switches ship with the Core PID bit set.

HP recommends that this change be performed to avoid potential problems in the future. Additional information on the Core Switch PID is available on the HP SAN Storage website.

Supported Switch Models – C-Series Product Line

HP currently supports five models of the C-Series product line 2 Gbps Fibre Channel Switches, the Cisco MDS 9506, 9509, 9216, 9120, and 9140.

Table 18: HP C-Series Product Line Switches

Switch Name	Firmware Version	Number of Ports
MDS 9506	1.2.1a, 1.2.1b	128
MDS 9509	1.0.4, 1.2.1a, 1.2.1b	224
MDS 9216		48
MDS 9120	1.2.1a, 1.2.1b	20
MDS 9140		40

Note: An MDS 9216 or MDS 9509 running 1.0.4 firmware must be upgraded to 1.2.1a or 1.2.1b firmware when configured in the same fabric as an MDS 9506/9120/9140.

SAN Fabric Rules – C-Series Fabric Product Line

The following rules are for SAN fabrics implemented with 1.0.4 or 1.2.1a switch FW unless otherwise stated.

1. The MDS 9506 is supported with up to 128 ports, over 4 modular chassis (4-32 port modules). The 32-port module for the MDS 9000 product line utilizes 3.2:1 oversubscription for optimized connectivity of low to mid-range host devices as well as tape libraries. HP recommends the use of the 16 port module for performance intense host applications as well as ISLs. This will decrease the actual port count of the switch.
2. The MDS 9509 is supported with up to 224 ports, over 7 slots, each filled in with a 32-port module. The 32-port module for the MDS 9000 product line utilizes 3.2:1 oversubscription for optimized connectivity of low to mid-range host devices and low-end tape libraries. HP recommends the use of the 16 port module for performance intense host applications, disk storage systems, and high-end tape libraries. This will decrease the actual port count of the switch.
3. The MDS 9506, MDS 9509, and MDS 9216 models also support the IP Storage services 8-Port 1xGE module that provides integrated FCIP functionality. HP recommends the use of this blade for integrated deployment and FCIP implementation for business continuity applications.
4. The MDS 9216 has a basic configuration with 16 ports. It has an expansion slot that supports either a 16 or a 32 port Fibre Channel card as well as the IP Storage services 8-port GE.
5. The MDS 9120 is a fixed 20 port configuration. It has 4 full rate ports and 16 oversubscribed ports.
6. The MDS 9140 is a fixed 40 port configuration. It has 8 full rate ports and 32 oversubscribed ports.

Fabric and Switch Model Maximums - C-Series Product Line

The fabric maximums listed are for C-Series switch model SAN fabrics utilizing HP XP128/1024, XP48/512, VA7410, Enterprise Virtual Array (EVA), EMA/ESA12000, EMA16000, MA/RA8000, MA6000, and MSA1000 storage systems. Refer to Chapter 4 for specific operating system support for each storage system type based on the switch product line used.

In general, these fabric rules also apply to Continuous Access XP, EVA, and DRM for EMA/ESA12000, EMA16000, and MA/RA8000 storage systems. Refer to Chapter 4 of this guide and the Continuous Access EVA Design Reference Guide for additional details.

1. Up to 11 MDS switches with up to 512 ports total in a SAN fabric
2. Up to 2 MDS 9506 or MDS 9509 Directors with up to 9 MDS 9216, 9120, or 9140 Fabric switches.
3. Up to 4 MDS 9506 or 9509 Directors in an all Director fabric
4. Up to 3 switch hops (4 switches) maximum between any two devices in a SAN fabric.

Zoning and VSANs

The following table (Table 19), indicates how zoning is implemented for the Cisco MDS switches.

1. In HP C-Series SANs, Virtual Storage Area Networks (VSANs) are defined as separate instances of all fabric services, including address space. HP supports 3 VSANs per physical fabric.
2. The maximum number of zones across all VSANs is 2048.
3. The maximum number of zone members across all VSANs is 20,000.

Table 19: Zone Types on HP fabric switches

Switch Models	Configuration	Enforcement	Comments
Cisco MDS 9506 Cisco MDS 9509 Cisco MDS 9216 Cisco MDS 9120 Cisco MDS 9140	Define zones using all domain#/port# Define zones using all WWNs Define zones using a combination of domain#/port# and WWNs	Access authorization at frame level in hardware	HARD zoning

Mixed Storage Common SAN Rules

Refer to Chapter 4 for specific storage rules related to the C-Series switches.

Supported Switch Models – M-Series Fabric Product Line

HP supports a range of 1 Gbps and 2 Gbps M-Series Fabric product line Fibre Channel switch models. These switch models represent products supported by both pre-merger HP and pre-merger Compaq. The relationship between the pre-merger and post-merger switch products is shown in Table 20. Refer to the section, SAN Fabric Rules – M-Series Fabric Product Line, for specific switch model support rules.

Table 20: HP StorageWorks M-Series Product Line Switches

HP StorageWorks Switch Name		Firmware Version	Number of Ports
HP StorageWorks edge switch 2/12		05.05.00-12	4 to 12
HP StorageWorks edge switch 2/16		05.02.00-13	16
HP StorageWorks edge switch 2/24			8 to 24
HP StorageWorks edge switch 2/32			16 to 32
HP StorageWorks director 2/64			32 to 64
HP StorageWorks director 2/140			64 to 140
HP Switch Name	**Compaq Switch Name**		**Number of Ports**
N/A	McDATA ES-3016 (Compaq reseller)	05.02.00-13	16
N/A	McDATA ES-3032 (Compaq reseller)		32
McDATA ED-5000 (McDATA reseller)		04.01.01-2	32
HP Director FC-64	Compaq StorageWorks SAN Director 64	05.02.00-13	64

SAN Fabric Rules – M-Series Fabric Product Line

All switch models shown in Table 20 are supported in the HP StorageWorks SAN provided that the same firmware versions and switch settings are utilized for all models with the exception of the ED-5000 and the Edge Switch 2/12. The ED-5000 utilizes a unique firmware version, this version is compatible with the other switch model versions. The default switch settings for this family of switches from pre-merger HP and pre-merger Compaq are the same.

Note: The StorageWorks Edge Switch 2/12 currently has an interim firmware version specific for the Edge Switch 2/12, version 05.05.00-12. This firmware cannot be used for any other edge switch or director. This interim version is compatible with the ED-5000 firmware and the M-Series firmware version 05.02.00-13 used for the rest of the M-Series Fabric products. The next major firmware release will be a common firmware version for all the M-Series Fabric products.

Fabric and Switch Model Maximums - M-Series Fabric Product Line

The fabric maximums listed are for M-Series switch model SAN fabrics utilizing HP XP128/1024, XP48/512, XP256, VA7100, VA7110, VA7400, VA7410, Enterprise Virtual Array (EVA), EMA/ESA12000, EMA16000, MA/RA8000, MA6000, or MSA1000 storage systems. Refer to Chapter 4 for specific operating system support for each storage system type based on the switch product line used.

In general, these fabric rules also apply to Continuous Access XP, EVA, and DRM for EMA/ESA12000, EMA16000, and MA/RA8000. Refer to Chapter 4 of this guide and the Continuous Access EVA Design Reference Guide for additional details.

The following rules are for SAN fabrics implemented with 05.x switch FW and 07.x HAFM. The ED-5000 requires 04.01.00-16 switch FW and a minimum of 04.02.00 HAFM.

1. Up to 24 switches with up to 1632 total ports and a maximum of 1024 user ports are supported in a single SAN fabric. Each fabric may contain any combination of supported 1 Gbps and 2 Gbps switch models listed, provided the individual switch model fabric limits listed below are not exceeded.

   — HP StorageWorks director 2/64 and HP StorageWorks director 2/140 – maximum of 8 Directors total per fabric

---

Note: With eight fully populated HP StorageWorks director 2/140's, it is physically possible to exceed the 1024 user port maximum. The restriction is in the zoning configuration, as only 1024 unique zone members (user ports) can be configured. However, the remaining ports can be used as Inter Switch Link (ISL) connections in the fabric.

   — Up to 16 switches with up to 512 total ports in a single fabric that includes one or more McDATA ED-5000 Directors.

2. Up to 3 switch hops (4 switches) maximum between any two devices in a SAN fabric.
3. Within a single fabric where switches are interconnected, each switch must have a unique domain number (Domain ID) and a unique World Wide Name (WWN). All switch configuration parameters in each switch must be the same.

Note: Do not configure any switches with a domain ID of 8. HP systems reserve domain 8 for Private Loop devices.

---

4. Zoning maximums - The following table lists the configuration limits for zones members, zones, and zone sets in the HAFM.

Table 21: Zoning Configuration Limits for High Availability Fabric Manager

Zoning Configuration	Limit
Number of zones in Zoning Library	2,048
Number of zone sets in Zoning Library	64
Number of members in zone	1,024
Number of zones	1,024 (1,023 plus the default zone)
Number of unique zone members in a zone set	1,024
Number of members in a zone set (with duplicate members allowed)	8,192
Characters per zoning name	64

5. Any mix of servers and storage systems is allowed in a SAN provided the specific platform, operating system, and storage system fabric limits and rules are followed. Refer to the appropriate sections in this guide and the documentation listed in the section "Related Documents" in the Preface.
6. HP requires that all switches in a single fabric or multi-fabric SAN use the same switch firmware revision for the models that utilize the same firmware versions. Two successive fabric firmware versions can be temporarily used in one fabric or multiple fabrics in a SAN during switch firmware rolling upgrades.
7. For M-Series Fabric product line, Table 20 Fibre Channel switches – Up to 7 switches configured in a ring with a Ring SAN fabric topology.

General ISL Rules - All Fabric Product Lines

When designing a fabric using 8-port, 16-port, 24-port, and 32-port switches, all ports may be used as ISLs with a maximum of one half of the total port count as ISLs to the same destination (may be license limited on some switch models). This feature is used in the Surestore FC Switch 6164 and StorageWorks SAN Switch Integrated 32 and 64 configurations, which are made up of multiple 16-port switches in an integrated mechanical chassis package. However, there are restrictions in the use of ISLs on some higher port count Fibre Channel switch models, as shown in Table 22.

Table 22: Number of ISLs for Fibre Channel switch products

HP Switch Product Name	Compaq Switch Name	Total Number of Available Users Ports	Number of Ports That May Be Used as ISLs
HP StorageWorks core switch 2/64		64 per switch, 128 per chassis	64 per switch, 128 per chassis
McDATA ED-5000		32	4
Director FC64	StorageWorks SAN Director 64	64	32
HP StorageWorks director 2/64		64	48 or 75% of installed ports
HP StorageWorks director 2/140		140	70 or 50% of installed ports

Heterogeneous/Interoperable SAN Fabrics

HP supports three levels of heterogeneous SAN fabrics:

- A dual heterogeneous SAN where one fabric consists exclusively of B-Series Fibre Channel switches, and a second fabric consists exclusively of M-Series Fibre Channel switches
- An interoperable heterogeneous SAN fabric with a mix of B-Series and M-Series switch models.
- An interoperable heterogeneous SAN fabric with a mix of B-Series and C-Series switch models.

Dual Heterogeneous SAN Fabrics

Dual Heterogeneous SAN Fabrics are supported where one SAN fabric consists exclusively of the Fibre Channel switches listed in Table 17, HP StorageWorks B-Series Product Line Switches and the second SAN fabric consisting exclusively of the switches listed in Table 20, HP StorageWorks M-Series Product Line Switches.

While each fabric could be designed to the maximum configuration for the applicable HP StorageWorks Series of Fibre Channel switches, good practice is to use the same configuration on both SAN fabrics. Symmetry is not a requirement, however, as a general rule, this maintains balanced SAN performance and also aids in understanding the configuration. In order to accomplish this, both fabrics should be designed to the least common design maximums between the two series of Fibre Channel switches. For example; HP StorageWorks B-Series product line Switches support 7 switch hops and HP StorageWorks M-Series product line Switches support 3 switch hops.

- When implementing a SAN with these two switch product lines, both fabrics should be designed with a maximum of 3 switch hops.
- For HA applications, since servers will connect to both fabrics, common HBA/driver, multi-path software, and storage array firmware versions support are required.

Note: Dual Heterogeneous SAN Fabrics are not supported on MSA1000 or in Continuous Access/DRM configurations.

Interoperable SAN Fabrics

C-Series with B-Series Switches

Within a single fabric, C-Series Director and Fabric switch models intermixed with B-Series switch models. The specific rules and configuration settings for each type of SAN fabric are described in the *Fabric Interoperability: Merging Fabrics Based on C-Series and B-Series Fibre Channel Switches Application Notes (AA-RV1ZA-TE)*.

M-Series with B-Series Switches

Within a single fabric, HP supports M-Series switch models intermixed with B-Series SAN switch models. The specific rules and configuration settings for each type of SAN fabric are described in the *Fabric Interoperability: Merging Fabrics Based on M-Series and B-Series Fibre Channel Switches Application Notes (AA-RUQQC-TE)*.

Both documents are available at:

http://h18006.www1.hp.com/products/storageworks/san/documentation.html

---

Note: Refer to the Application Notes above for a list of specific products supported in interoperable SAN Fabrics. Interoperable SAN Fabrics are not supported on MSA1000 or in Continuous Access/DRM configurations.

Third party switch support

3rd party switches and connectivity reliability have been verified through testing. However, support is subject to the following:

- No support for 3rd party switch functionality. If a defect must be fixed within the switch product, the customer will need to work directly with the 3rd party switch support organization.
- HP will make a best effort attempt to help the customer resolve issues as they pertain to the HP supported products within the environment.
- HP can support switches and additional functionality resold through other vendors providing the customer purchases 3rd party support through the HP SAN Environmental Services Group (SAN-ES). Refer to http://www.hp.com/hps/storage/ for additional information.

Example of 3rd party switches:

- McData ED5000 = EMC Connectrix ED-1032
- InRange FC 9000

1 and 2 Gbps Fabric Topology Recommendations

There are no specific topology rules related to mixing of 1 and 2 Gbps components in a fabric. HP does however strongly recommend these guidelines be followed.

- When using both 1 and 2 Gbps switches in the same fabric, utilize 2 Gbps switches in the core for Core to SAN switch or Director to edge switch topologies.
- Connect 2 Gbps switches together to take advantage of the optional ISL Trunking feature when using Fibre Channel switch models that support this feature.

- Utilize 2 Gbps switches for connections to 2 Gbps capable devices. In general, for SANs with both 1 Gbps and 2 Gbps components, the transfer rate between devices and ports on switches is determined by the speeds supported by the individual ports that are connected. If two 2 Gbps devices or switch ports are connected together, the speed will be 2 Gbps for that segment in the fabric. If two 1 Gbps devices or switch ports are connected together the speed will be 1 Gbps for that segment in the fabric. If a 2 Gbps and a 1 Gbps port are connected together the speed will be 1 Gbps for that segment. Refer to the section General Fabric Performance Recommendations in this chapter for more information.
- Zoning rules, SAN security, and SAN management for 2 Gbps switches are the same as for 1 Gbps switches.

SAN Fabric Zoning Rules

The fabric zoning feature is supported with all HP Fibre Channel switch models. Zoning can be used to logically separate devices and different hardware platforms and operating systems in the same physical SAN. Use of zoning is required under these specific conditions:

- When mixing different storage system models and servers in the same SAN fabric. Refer to Chapter 4**, "**Heterogeneous SAN Platform and Storage System Rules**"** for more information.
- When mixing different hardware platforms, operating systems or storage systems that are currently only supported in homogenous SANs, and it is unknown whether there are interaction problems. Refer to Table 27 for specific information about zoning in heterogeneous SANs.
- When there are known interaction problems between different hardware platforms or operating systems and specific storage system types.
- When the number of nodes or ports in the SAN fabric exceeds a storage system connection support limit. There is a connection limit for storage systems using the EVA5000/EVA3000 (HSV controller) or EMA/ESA/MA/RA (HSG60/80 controller). The version of VCS or ACS controller code determines the specific limit.
- Overlapped zones are supported. Refer to the specific platform and storage system rules for more information.
- The maximum number of zones supported in a SAN fabric is based on specific switch product line in use. Refer to the fabric and switch model maximums for each switch product line for more information.

Storage Management Appliance Rules and Recommendations

Whenever a Storage Management Appliance is placed in a fabric with heterogeneous servers it is recommended that a dedicated storage management zone be created. This zone is specifically for the Storage Management Appliance and the elements it is to monitor and manage.

Currently, the Storage Management Appliance communicates with the EVA5000/EVA3000 (HSV controller) and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 storage systems (HSG controller) in-band, that is, within the Fibre Channel fabric itself. It is not necessary or recommended to include either the switch WWNs or server HBA WWNs in this zone. Management communication to these devices from the Storage Management Appliance is done out-of-band or outside the fabric via TCP/IP.

For example, create a zone called SANAPP_1_ZONE that would contain the Appliance host bus adapter WWN and the WWNs of all the HSG or HSV controllers managed by this Storage Management Appliance. Because fabric devices can be in multiple zones, this will have no effect on other zones containing the same HSG and HSV controller WWNs.

1. Within the same fabric, EVA5000/EVA3000s with V2.0x and V3.0x can be managed by the same instance of Command View EVA. A separate appliance is needed to manage an EVA5000/EVA3000 with V1.0x.
2. Any EVA storage system can only have one active SMA managing it. Any standby SMA can be powered on, but the Command View EVA or Continuous Access user interface must not control the storage system. For further information, refer to the HP StorageWorks Continuous Access EVA Operations Guide available on the HP web.
3. A Storage Management Appliance is required to manage EVA5000/EVA3000s. For EMA/ESA12000, EMA16000, MA/RA8000, MA6000 storage systems, it is recommended that a Storage Management Appliance be used to manage the SAN when a fabric contains more than four Fibre Channel switches. It is required when using the HSG element manager.
4. Multiple appliances per fabric are allowed as long as only one appliance is accessing a controller pair at a time. Zoning is required to actively isolate an appliance and its controllers from other appliances and their controllers.
5. Element Manager for HSG may manage up to 25 HSG controller pairs per appliance. Command View for HSV may manage up to 16 HSV controller pairs per appliance.
6. The HSV and HSG Element Managers can operate in a dual fabric configuration.
7. A license key is required for each EVA5000/EVA3000 managed by the Storage Management Appliance. Additional licenses are required to take advantage of value added software functionality.
8. For SANs with more than 1024 HBAs, an HSV controller must be zoned so that it can see no more than 1024 HBAs. It may be necessary to add a zone to a SAN to satisfy the 1024 HBA limit.

Refer to Chapter 4**, "**Heterogeneous SAN Platform and Storage System Rules**"**, for rules about mixing specific platforms in a Heterogeneous SAN without the need for fabric zoning.

SAN Component Interconnect Descriptions and Rules

The following sections describe rules for SAN component interconnects–switch port interfaces and physical cabling.

Fibre Channel Switch Interface Usage Descriptions

- E-Port interface for switch to switch connectivity (also referred to as ISLs)
- F-Port interface for fabric attached device–initiators (host bus adapters) and targets (storage ports)
- FL-Port interface for public loop fabric-aware, 24-bit Fibre Channel addressable devices–initiators or Compaq FC-AL Switch 8 SAN attachment
- FL-Port interface for private loop 8-bit Fibre Channel addressable devices–private FC-AL initiators and targets. This requires use of the B-Series product line switches QuickLoop Feature. This is a license-enabled feature on certain switch models, refer to the specific switch model product documentation for information about support of this feature. Typically this feature is only required when a specific platform can only be configured with a private FC-AL host bus adapter driver.
- G-Port, default interface when no devices appear to be attached to the port.

Access with QuickLoop

The QuickLoop switch feature allows private FC-AL initiators and targets configured in a QuickLoop to communicate with each other through the switch. Since all initiators configured *inside* a QuickLoop are private they cannot communicate with targets outside of the QuickLoop. QuickLoop is only supported on the B-Series product line of Fibre Channel switch models when used with MA6000, MA8000, RA8000, EMA12000/16000, and ESA12000 RAID Array systems.

Fiber Optic Interconnect Rules

1. 2 Gbps components utilize industry standard “LC” connectors for the Fibre Channel optical connections. 1 Gbps components utilize industry standard “SC” connectors. Cables and adapters are available with SC connectors on one end and LC connectors on the other end. Refer to the 2 Gbps switch QuickSpecs documents for additional information.

Note: Certain fiber optic cable configurations may require the use of SC or LC connector sleeves to couple two cable connector ends together such as when using wall jacks or connecting to existing pre-installed cables. Duplex couplers are available from various manufacturers. Use of these couplers is supported provided the overall cable losses specified in this chapter are not exceeded in the cable segment that includes the couplers.

---

2. The minimum allowable bend radius of fiber optic cable is 25 mm for 50, 62.5, and 9 micron fiber optic cable.
3. There is a minimum fiber optic cable segment length between Fibre Channel devices (a transmitter and a receiver). The minimum length is 0.5 meters for 50 and 62.5 micron cable and 2.0 meters for 9 micron cable. The minimum length does not apply to patch cords through a passive patch panel; it only applies to the total distance between the transmitter and receiver of the devices being connected through the patch panel.

4. For longer 50-micron short wave multi-mode optical fiber cables up to 300 meters (2 Gbps) or up to 500 meters (1 Gbps), a third party vendor must be contacted. The cables must be duplex, tight buffered multi-mode 50/125 µm (Belcore GR-409 compliant) and the connectors must be SC or LC duplex low metal Belcore and IEC compliant.
5. For 9-micron long wave single-mode optical fiber cables up to 100 km (1 Gbps) or 35 km (2 Gbps), 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 or LC duplex low metal (NTT-SC Belcore 326, IEC-874-19 SC compliant).
6. The mixing of 9-micron, 50-micron, and 62.5-micron fiber cables in the same cable segment is not supported.
7. Extended Fabrics – See Chapter 8, SAN Extension. Also refer to the *Extended Fabric User Guide, AA-RR7QA-TE*, for more information.

2 Gbps Fiber Optic Interconnects/Distance Rules

1. Up to 300 meters maximum distance per cable segment between devices and switches or switches and switches using 50/125 micron multi-mode fiber optic cable and short wavelength SFPs
2. Up to 150 meters maximum distance per cable segment between devices and switches or switches and switches using 62.5/125 micron multi-mode fiber optic cable and short wavelength SFPs

---

Note: Information on the use of 62.5 micron fiber optic cable is provided to facilitate use of previously installed cable. HP recommends 50 micron fiber optic cable for any new installation requiring multi-mode fiber.

---

3. Up to 10 km (6.2 miles) maximum distance between two switches using 9/125 micron single-mode fiber optic cable and long wavelength SFPs.
4. Up to 35 km (21.7 miles) maximum distance between two switches using 9/125 micron single-mode fiber optic cable and extended reach SFPs.
5. For B-Series product line switches:

- Maximum of 160 km (100 miles) total distance across the SAN using multiple segments. This can be implemented using four 35km segments and two 10 km segments (6 hops.) In all cases the individual segments must be configured with the proper SFP and cable type and a maximum of 7 hops must not be exceeded across the SAN.
- ISL connections up to 10 km are supported between 1Gb and 2Gb switches at the "L0" portcfglongdistance setting only.

6. For C-Series product line switches:

- Maximum of 30 km (18.6 miles) total distance across the SAN using multiple segments. This can be implemented using three 10 km segments (3 hops.) In all cases the individual segments must be configured with the proper SFP and cable type and a maximum of 3 hops.

7. For M-Series product line switches:

- Maximum of 105 km (64 miles) total distance across the SAN using multiple segments. This can be implemented using three 35 km segments (3 hops.) In all cases the individual segments must be configured with the proper SFP and cable type and a maximum of 3 hops must not be exceeded across the SAN.

Note: WDM may be used to increase the switch-to-switch distance beyond the distances listed above. Refer to Chapter 8, SAN Extension.

Note: Refer to the Data Replication Manager (DRM) solution documentation, including the DRM Design Guide, for specific interconnect and distance rules related to DRM configurations. See:
http://h18000.www1.hp.com/products/sanworks/drm/documentation.html

Note: Refer to the Continuous Access EVA solution documentation, including the Continuous Access EVA Design Reference Guide, for specific interconnect and distance rules related to Continuous Access EVA configurations. See:
http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html

1 Gbps Fiber Optic Interconnects/Distance Rules

1. Up to 500 meters maximum distance per cable segment between devices and switches or switches and switches using 50/125 micron multi-mode fiber optic cable and short wavelength GBICs or GLMs[1].
2. Up to 200 meters maximum distance per cable segment between devices and switches or switches and switches using 62.5/125 micron, multi-mode fiber optic cable and short wavelength GBICs or GLMs[1].

Note: Information on the use of 62.5 micron fiber optic cable is provided to facilitate use of previously installed cable. HP recommends 50 micron fiber optic cable for any new installation requiring multi-mode fiber.

3. For B-Series product line switches:

- Up to 10 km (6.2 miles) maximum distance between any two switches using 9/125 micron single-mode fiber optic cable and long wavelength GBICs.
- Up to 100 km (62 miles) distance between any two switches using 9/125 micron single-mode fiber optic cable and very long distance GBICs. A maximum of one 100 km very long distance segment per SAN.
- Maximum of 160 km (100 miles) total distance across the SAN using multiple segments. This can be implemented using a single 100 km segment and six 10 km segments (7 hops) or other combinations such as two 50 km segments and five 10 km segments (7 hops). In all cases the individual segments must be configured with the proper GBICs and cable type and the maximum of 7 hops must not be exceeded across the SAN.
- ISL connections up to 10 km are supported between 1Gb and 2Gb switches at the "L0" portcfglongdistance setting only.

4. For C-Series product line switches:

- Maximum of 30 km (18.6 miles) total distance across the SAN using multiple segments. This can be implemented using three 10 km segments (3 hops.) In all cases, each segment must be configured with the proper SFP and cable type and a maximum of 3 hops.

1. GLMs are used in the HSG60 (MA6000) and HSG80 (MA/RA8000, EMA/ESA12000, EMA16000) storage controllers

5. For M-Series Fabric product line switches:

- Up to 10 km (6.2 miles) maximum distance between any two switches using 9/125 micron single-mode fiber optic cable and long wavelength SFPs.
- Up to 35 km (21.7 miles) maximum distance between two switches using 9/125 micron single-mode fiber optic cable and extended reach SFPs.
- Maximum of 105 km total distance across the SAN using multiple segments. This can be implemented using three 35 km segments (3 hops.) In all cases the individual segments must be configured with the proper SFP and cable type and a maximum of 3 hops must not be exceeded across the SAN.

Note: WDM may be used to increase the switch-to-switch distance beyond the distances listed above. Refer to Chapter 8, SAN Extension.

Note: Refer to the Data Replication Manager (DRM) solution documentation, including the DRM Design Guide, for specific interconnect and distance rules related to DRM configurations. See:
http://h18000.www1.hp.com/products/sanworks/drm/documentation.html

Note: Refer to the Continuous Access EVA solution documentation, including the Continuous Access EVA Design Reference Guide, for specific interconnect and distance rules related to Continuous Access EVA configurations. See:
http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html

Fiber Optic Cable Loss Budgets

The information in this section is based on the Fibre Channel Physical Interface Specification. Refer to the specification document for more information. The maximum distances specified are based on the use of nominal bandwidth fiber optic cable. This specifies modal bandwidth of 500 MHz-km for 50 micron fiber optic cable, and 200 MHz-km for 62.5 micron fiber optic cable.

Note: Media losses are not specified due to variances between different fiber optical cable manufacturers. In all cases the specification that must be followed is the total channel insertion loss, which includes media losses.

Note: Information on the use of 62.5 micron fiber optic cable is provided to facilitate use of previously installed cable. HP recommends 50 micron fiber optic cable for any new installation requiring multi-mode fiber.

Table 23: Optical Cable Losses

Speed	Cable	Maximum Distance	Total Channel Insertion Loss[1]	Loss per Mated Connector Pair	Notes
2 Gbps	62.5/125 micron	150 meters	2.1 dB	0.75 dB	
2 Gbps	50/125 micron	300 meters	2.62 dB	0.75 dB	
2 Gbps	9/125 micron	10 km	7.8 dB	0.75 dB	
2 Gbps	9/125 micron	35 km	19 dB	0.75 dB	
1 Gbps	62.5/125 micron	200 meters	3.0 dB	0.75 dB	
1 Gbps	50/125 micron	500 meters	3.85 dB	0.75 dB	
1 Gbps	9/125 micron	10 km	7.8 dB	0.75 dB	
1 Gbps	9/125 micron	100 km	21.5 dB	0.75 dB	A minimum loss of 8 dB is required

1. Channel insertion loss is the combined passive loss from connectors, splices, and media between the transmitter and receiver.

Use of optical fiber patch panels is supported provided the total channel insertion loss between the transmitter and receiver for the cable segment routed through the patch panel does not exceed the maximum listed for the connector and cable type in use.

Table 24: Storage Product Interconnect/Transport Support

Interface/ Transport	Storage Product		
	Heterogeneous SAN	DRM and Continuous Access EVA	Enterprise Backup Solutions (EBS)
2 Gbps Fibre Channel via 50 micron multi-mode fiber optic cable and short-wave SFPs	Up to 300 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 300 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 300 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.
2 Gbps Fibre Channel Via 62.5 micron multi-mode fiber optic cable and short-wave SFPs	Up to 150 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 150 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 150 meters per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.
2 Gbps Fibre Channel via 9 micron single-mode fiber optic cable and long-wave SFPs	Up to 10 km per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 10 km per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 10 km per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.
2 Gbps Fibre Channel via 9 micron single-mode fiber optic cable and extended reach SFPs	Up to 35 km per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Up to 35 km per cable segment. Refer to 2 Gbps Fiber Optic Interconnects/Distance Rules, page 82, for maximum supported distance across the SAN.	Not Supported
1 Gbps Fibre Channel via 50 micron multi-mode fiber optic cable and short-wave GBICs	Up to 500 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 500 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 500 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.
1 Gbps Fibre Channel via 62.5 micron multi-mode fiber optic cable and short-wave GBICs	Up to 200 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 200 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 200 meters per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.
1 Gbps Fibre Channel via 9 micron single-mode fiber optic cable and long-wave GBICs	Up to 10 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 10 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 10 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.

Table 24: Storage Product Interconnect/Transport Support (Continued)

Interface/ Transport	Storage Product		
	Heterogeneous SAN	DRM and Continuous Access EVA	Enterprise Backup Solutions (EBS)
1 Gbps Fibre Channel via 9 micron single-mode fiber optic cable and very long distance GBICs	Up to 100 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 100 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.	Up to 10 km per cable segment. Refer to 1 Gbps Fiber Optic Interconnects/Distance Rules, page 83, for maximum supported distance across the SAN.
1 Gbps and 2 Gbps Fibre Channel via Wavelength Division Multiplexing (WDM)	Supported up to 160 km total distance across the SAN. Refer to the SAN Extension Chapter.	Supported up to 160 km total distance across the SAN. Refer to the SAN Extension Chapter.	Not Supported
ATM over single T1/E1 Wide Area Network (WAN)	Not Supported	Supported Refer to page 139 Supported on DRM using an FC to ATM convertor with no limit on delay, and as the intersite backbone for Continuous Access EVA with an FC to IP convertor with up to 100 ms of delay	Not Supported
ATM over single T1/E1 WAN (Inverse Multiplexing)	Not Supported	Supported Refer to page 139 Supported on DRM using an FC to ATM convertor with no limit on delay, and as the intersite backbone for Continuous Access EVA with an FC to IP convertor with up to 100 ms of delay	Not Supported
ATM over T3/E3 WAN	Not Supported	Supported Refer to page 139 Supported on DRM using an FC to ATM convertor with no limit on delay, and as the intersite backbone for Continuous Access EVA with an FC to IP convertor with up to 100 ms of delay	Not Supported
ATM over fractional and/or shared T3/E3 and OC3 WAN	Not Supported	Supported Refer to page 139 Supported on DRM using an FC to ATM convertor with no limit on delay, and as the intersite backbone for Continuous Access EVA with an FC to IP convertor with up to 100 ms of delay	Not Supported

Table 24: Storage Product Interconnect/Transport Support (Continued)

Interface/ Transport	Storage Product		
	Heterogeneous SAN	DRM and Continuous Access EVA	Enterprise Backup Solutions (EBS)
10/100 Copper Ethernet FC over IP (FCIP)	Supported on EVA, EMA/ESA12000, EMA16000, MA/RA8000 and MA6000 with up to 100 ms of delay.MSA1000 supported up to 160 km total distance	Supported on DRM and Continuous Access EVA with up to 100 ms of delay.	Not Supported
1 Gbps Optical Ethernet FC over IP (FCIP)	Supported on EVA, EMA/ESA12000, EMA16000, MA/RA8000 and MA6000 with up to 100 ms of delay.MSA1000 supported up to 160 km total distance	Supported on DRM and Continuous Access EVA with up to 100 ms of delay.	Not Supported
iSCSI bridging using the HP SR2122-2 storage router	Supported on EVA, MSA1000, EMA/ESA12000, EMA16000, MA/RA8000 and MA6000 up to 160 km total distance	Not Supported	Not Supported
FCIP SAN extension using the HP SR2122-2 storage router	Supported on EVA, EMA/ESA12000, EMA16000, MA/RA8000 and MA6000 up to 160 km total distance. (B-Series and M-Series switches only)	Suported on DRM, Continuous Access EVA, and Continuous Access XP with up to 100ms of delay.	Not Supported

General Fabric Performance Recommendations

The performance of an application on a heterogeneous SAN is usually seen from the perspective of "storage performance". The intervening SAN and competing workloads are not usually considered. The fact is that the performance of the storage will be dependent on the interaction of all the components and applications in the SAN. Some of the possible component limiting factors include the host CPU(s), FC HBA, SAN topology, SAN traffic, RAID controllers, or the specific configuration of disks used behind the controllers. This is a dynamic workload environment and at any given moment any part of the SAN can dominate the performance. This complexity can be simplified if the environment is divided into the categories of servers, SAN infrastructure, and data storage devices. This document is primarily interested in the SAN infrastructure. There are issues with storage and servers that are unique to SAN implementations and we will address some of those as well.

SAN Infrastructure Performance

For the purposes of discussion assume a multi-switch fabric, since single switches always offer the highest performance with minimum latency. A multi-switch fabric has two factors that decrease overall fabric-wide infrastructure performance:

- latency through multiple switches (hops)
- oversubscription or congestion of ISLs

Performance testing and measurement by HP has shown switch latency to be less than 5% (at 1 Gbps) of the time lost due to congestion of a full frame from another path. This implies that the number of switches and hops between devices is not a major factor for performance.

However, as devices send frames through more switches and hops, the chances are increased that other traffic in the SAN may be routed over the same ISL/path. This may decrease performance due to oversubscription of a particular ISL/path that is serving multiple devices.

Oversubscription has been determined to be the largest contributing factor to reduced Fibre Channel performance. When devices must contend for the same ISL or path, the best result will be that each competing device will receive 1/n of the available bandwidth on the path (where n is the number of contending devices).

While the topology and size of the SAN have been seen to affect performance, staying within the rules and recommendations outlined in this guide minimizes these factors. The topology designs have been defined to accommodate a particular data access or data locality type. Recommendations on the number of ISLs based on device-to-device access ratios serve to ensure that adequate bandwidth is available across the SAN, minimizing oversubscription.

HP recommends following these guideline in configuring your SAN.

- Whenever possible, devices that exchange the highest amount of data should be connected to the same Fibre Channel switch.
- For high bandwidth, the number of application servers should be balanced with storage by using as much one-to-one access as possible
- When devices exchanging data are on different switches:
  - Minimize the number of hops between devices
  - For high bandwidth (large transfer size) applications, configure a maximum of two active storage controller ports per ISL
  - For high throughput (small transfer size) applications, configure a maximum of 20 active storage controller ports per ISL
  - For mixed applications, configure a maximum of 4 active storage controller ports/ ISL

Performance Considerations for Mixed 1 Gbps and 2 Gbps SAN Fabrics

For SAN fabrics consisting of a mixture of 1 and 2 Gbps switches and devices, the individual fabric segment connections negotiate the speed at which specific devices communicate. The presence of 1 Gbps devices in a fabric will not force other independent 2 Gbps devices to a lower speed. That is, switch ports or user ports in a fabric capable of 2 Gbps will always communicate at their highest supported speed, 2 Gbps, when connected to other switch or user ports capable of 2 Gbps. The sustained data rate between the devices will be 200 MB/second assuming the entire path between the devices through the fabric is capable of 2 Gbps.

If you have 1 Gbps and 2 Gbps devices connected to the same 2 Gbps switch, or if an intermediate path or route between devices is 1 Gbps, the switch will buffer data coming from the 2 Gbps device to prevent overrunning the 1 Gbps port or device. Over time the sustained data rate will be 100 MB/second.

It is recommended that devices capable of 2 Gbps always be connected to 2 Gbps switches and other 2 Gbps devices. Ensure that the entire path or route between 2 Gbps devices consists of 2 Gbps capable ports.

On the C-Series switches ensure that Fibre-Channel Congestion Control (FCC) is enabled on all the switches. The FCC is a feature of the C-Series switches which allows these switches to intelligently regulate traffic across ISLs and ensure each host-target pair of devices will have the required bandwidth for data transfer. The C-Series switches also have the ability to prioritize frames originating from a particular port hence applications can be prioritized using the Quality of Service (QOS) feature.

Performance Specifications

Contact your HP representative for specific product performance information.

Heterogeneous SAN Platform and Storage System Rules

4

This chapter describes rules related to specific platforms, operating systems, and storage products. For additional information refer to the relevant platform and individual product specific documentation. Refer to the section About this Guide for a list of related documentation.

General Platform/Operating System and Storage System Rules

1. Each platform listed is supported in all SAN Fabric topology configurations unless otherwise noted in this guide or the applicable platform documentation.
2. Any mix of heterogeneous servers, clustered and standalone, is allowed in a SAN provided that you follow all individual platform rules, fabric rules, applicable server application rules, and the maximums listed in this guide and in the platform specific documentation.
3. All HP and multi-vendor hardware platforms and operating systems that are supported in a homogeneous SAN are supported in a heterogeneous SAN. Refer to Table 25, and Table 27 to determine if zoning is required for specific combinations of supported heterogeneous platforms.
4. Servers can attach to multiple fabrics. The number of separate fabrics per server is based on the specific server model capabilities and the maximum number of Fibre Channel host bus adapters supported.
5. Refer to the section **"**High Availability Configuration Considerations**"** in this chapter for cabling scheme options for platforms that support high availability multi-pathing.
6. Any mix of storage systems is allowed in a SAN, provided that you follow all applicable fabric rules, platform/operating system rules, storage system rules, and mixed storage common SAN rules.
   - Fabric Rules - Refer to Chapter 3
   - Platform/Operating System Rules - Based on the storage system type(s) and switch product line(s) utilized, refer to:
   - "Specific Platform/Operating System Rules – EVA5000/EVA3000 (VCS v3), EMA/ESA12000, EMA16000, MA/RA8000, MA6000 (ACS 8.7) Storage Systems, B-Series and M-Series Switches"
   - "Specific Platform/Operating System Rules – Enterprise Virtual Array (VCS v3.010), EMA/ESA12000, EMA16000, MA/RA8000 (ACS 8.7) Storage Systems, C-Series Switches"
   - "Specific Platform/Operating System Rules – HP XP and VA Storage Systems"
   - "Specific Platform/Operating System Rules – MSA1000, RA4100, RA4000
   - Storage System Rules - Based on the storage system type(s) utilized, refer to:
   - HP XP and VA Configuration Rules
   - EVA5000/EVA3000 Configuration Rules
   - EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Configuration Rules
   - MSA1000 Configuration Rules
   - RA4100 and RA4000 Configuration Rules
   - Mixed Storage Type SAN Rules - B-Series, C-Series, M-Series Switches - For SAN fabrics containing a mix of different storage system types
7. Refer to the section "**Platform Interoperability for Single Shared EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems – ACS 8.7"** for information related to mixing heterogeneous platforms on a single shared EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage system. In certain situations multiple storage systems may be required to accommodate the requirements of different platforms or operating systems.

8. Currently, there are different limits relative to the number of switches supported in a SAN Fabric based on the Fibre Channel switch product line in use. Refer to Chapter 3, "SAN Fabric Design Rules" for more information.

Blade Server Support

The BL20P and BL40P are supported with B-Series, C-Series, and M-Series product line switches. Refer to the *hp ProLiant BL p-Class system overview and planning white paper* at:

ftp://ftp.compaq.com/pub/supportinformation/papers/5981-6911en_rev1_us.pdf

Mixed Storage Type SAN Rules - B-Series, C-Series, M-Series Switches

HP supports SANs consisting of a mixture of storage system types. This section defines the rules for mixing different storage system types within a SAN using switch models exclusively from one product line of Fibre Channel switch products. For information about interoperability rules and support for SANs or SAN fabrics with mixed switch product line types, refer to Heterogeneous/Interoperable SAN Fabrics in Chapter 3.

Common SAN Access

In general, support in the same SAN for mixed storage system families is provided by implementing separate zones for servers and the storage system families being accessed as shown in Figure 23 for the B-Series product line of switches, Figure 24 for the M-Series, and Figure 25 and Figure 26 for the C-Series.

As depicted in Figure 26, C-Series switches provide a capability to build secure virtual fabrics using the VSAN feature called VSAN. Each VSAN is a separate virtual fabric that can be dedicated to a different type of storage system and zoning can be implemented on a per-VSAN basis for additional security.

Common Server Access

Common server access allows for simultaneous connectivity to different disk storage system families from the same server and, in some cases, the same HBA.

In addition, certain storage solutions utilizing multiple storage types, for example, disk and tape, may also specify support for common server access. In those cases, refer to the specific storage solution documentation for the supported common access configurations and rules.

Common Server, Separate HBAs

Common server access using separate HBAs is supported for XP, VA, and EVA storage systems for these specific configurations. Contact your HP storage representative for a configuration review prior to deployment.

- **XP and EVA on Sun Solaris** - Connection to a common server requires separate VxVM DMP for XP and Secure Path for EVA HBAs and zones. Specific minimum versions of VxVM DMP and Secure Path are required. This is supported with B-Series and M-Series switches only.
- **XP and EVA on IBM AIX** - Connection to a common server requires separate Autopath for XP and Secure Path for EVA HBAs and zones. Specific minimum versions of Auto Path and Secure Path are required. This is supported with B-Series and M-Series only.
- **XP/VA, MSA, EVA/EMA/ESA12000, EMA16000, MA/RA8000, MA6000 on Microsoft Windows** - Connection to a common server requires separate HBAs and zones for XP/VA, MSA, and EVA/EMA/ESA12000, EMA16000, MA/RA8000, and MA6000. All products are supported using a common version of Secure Path for Windows. This is supported with B-Series and M-Series switches only.
- **XP/VA, MSA, EVA/EMA/ESA12000, EMA16000, MA/RA8000, MA6000 on OpenVMS and Tru64 UNIX**- Connection to a common server requires separate HBAs and zones for XP/VA, MSA, and EVA/EMA/ESA12000, EMA16000, MA/RA8000, and MA6000. Multi-path is native for these OSes . This is supported with B-Series, C-Series, and M-Series switches .
- **MSA on all supported operating systems** - Connection to a common server with other storage systems requires dedicated HBAs and zones for the MSA1000.

Common Server, Common HBAs

Simultaneous access to different storage system types from the same Server/HBA is supported when the storage system families listed use common HBA model numbers, drivers, and multi-path software versions. HP currently supports the following storage types and operating systems for common server, common HBA access.

XP/VA and EVA on HP-UX - Connection to a common server with a common HBA is supported. Specific minimum versions of Secure Path and AutoPath are required. Contact your HP storage representative for a configuration review prior to deployment.

EVA and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 on Microsoft Windows and Linux - Connection to a common server with a common HBA is supported on the following operating systems:

- **Microsoft Windows** - HP recommends use of the EVA V3.0B platform kit (minimum version). This ensures that Windows servers attached to storage types utilizing VCS V2.x or higher and ACS 8.7-x can be accessed simultaneously. The EVA platform kit can also be used for Windows servers that have only an EVA or only an EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage system.
- **Linux** - HP recommends use of the EVA V3.0B platform kit (minimum version). This ensures that Linux servers attached to storage types utilizing VCS V2.x or higher and ACS 8.7-x can be accessed simultaneously. The EVA platform kit can also be used for Linux servers that have only an EVA or only an EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage system.

XP, EVA, and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 on Alpha - Connection to a common server with a common HBA is supported on the following operating systems:

- Tru64 UNIX
- OpenVMS

This is supported with B-Series, C-Series, and M-Series switches.

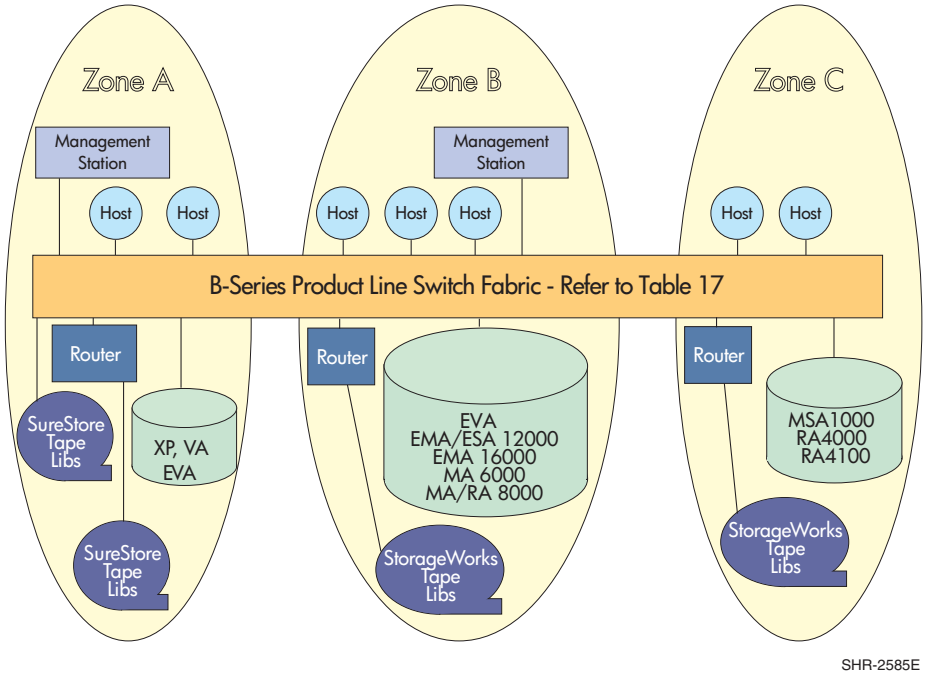


Figure 23: HP StorageWorks SAN using B-Series Switches

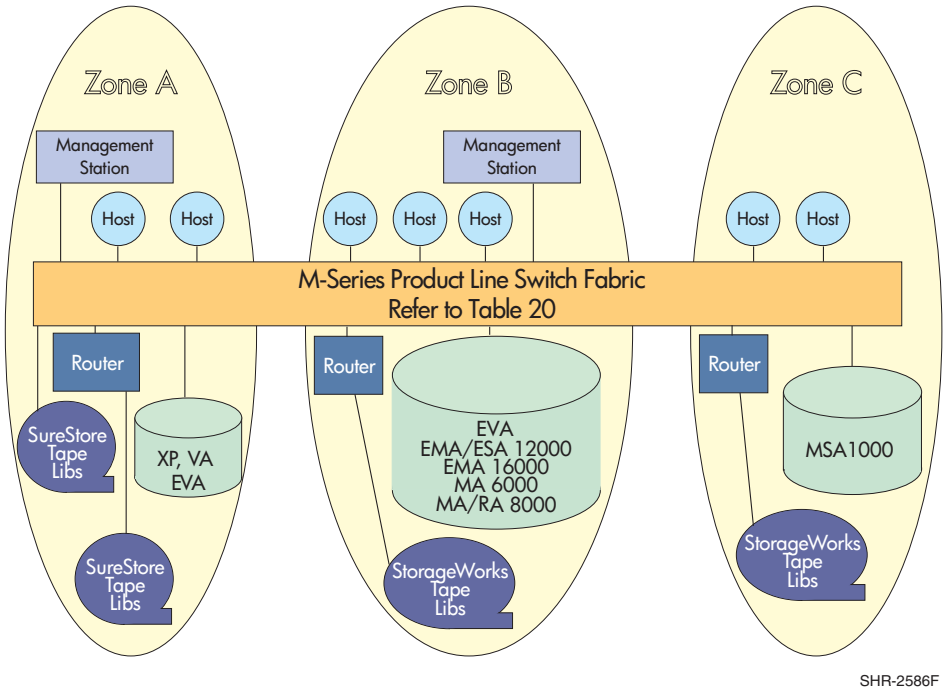


Figure 24: HP StorageWorks SAN using M-Series Switches

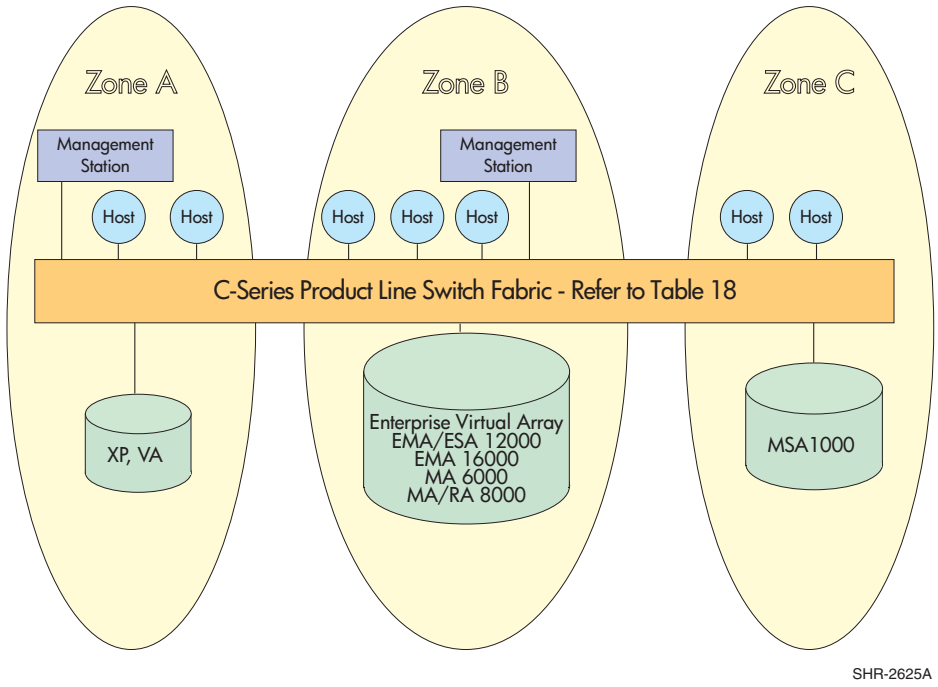


Figure 25: HP StorageWorks SAN using C-Series Switches

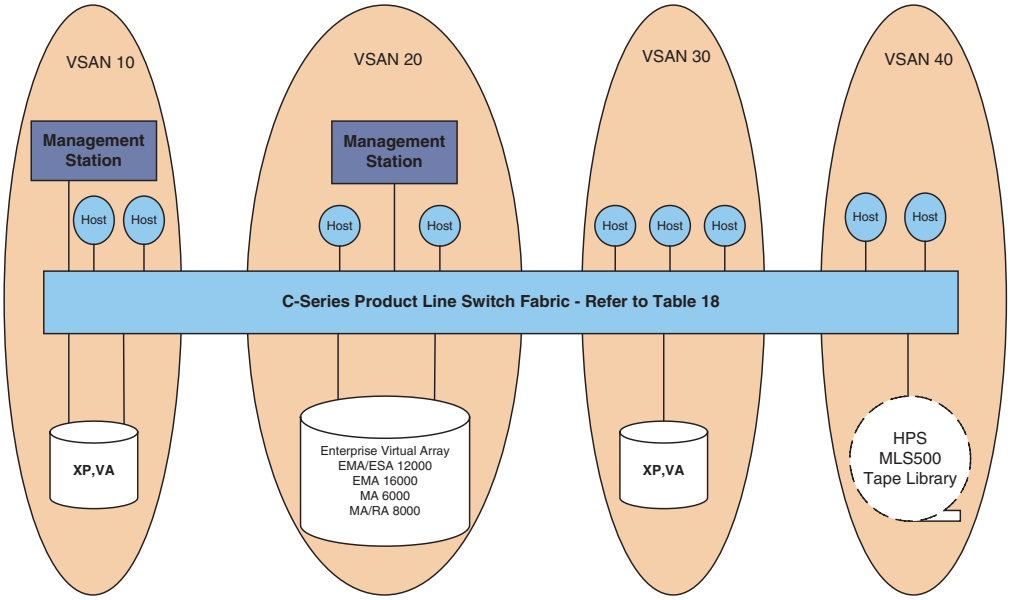


Figure 26: C-Series based SAN with VSANs

Specific Platform/Operating System Rules – HP XP and VA Storage Systems

Specific platform support rules and SAN fabric configuration rules for SANs consisting of HP XP and VA storage systems are described here.

This section defines the rules and guidelines surrounding the design of SAN infrastructures for XP and VA arrays. For additional information on operating system HBA/driver/firmware/software support, contact your HP field representative.

These rules are sub divided into the following categories for ease of reference and are described briefly in the following pages.

- Legacy SAN Support
- High Availability/Mission Critical SAN Support
- SAN connectivity rules
- XP and VA with multiple OS's shared switch fabric
- XP, VA and tape with multiple OS's shared switch fabric
- Heterogeneous Storage support
- Secure Manager Support
- Third party switch support
- Boot support

Legacy SAN Support

Separate SANs are required if the environment consists of a mixture of legacy switches, devices, discontinued arrays and current products. Legacy products include..

- Discontinued storage devices
- Discontinued switches F16(HP first generation 16-port switch), SANBox-16 (Ancor/Qlogic)
- Storage devices like FC60, 12H etc.,

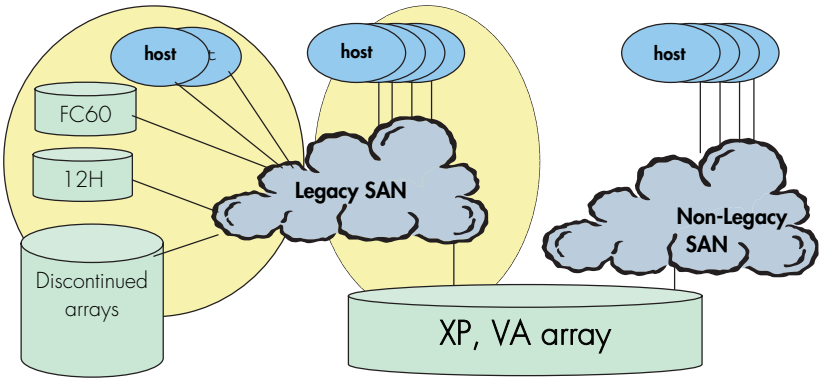


Figure 27: Legacy SAN Support

High Availability/Mission Critical SAN Support

High availability environments like HP Service Guard running on HP-UX servers require dual fabric SAN configurations for achieving “no single point of failure” and meeting customer expectations of “no infrastructure or application downtime” for mission critical applications. This is true for other operating systems also supporting similar high availability solutions.

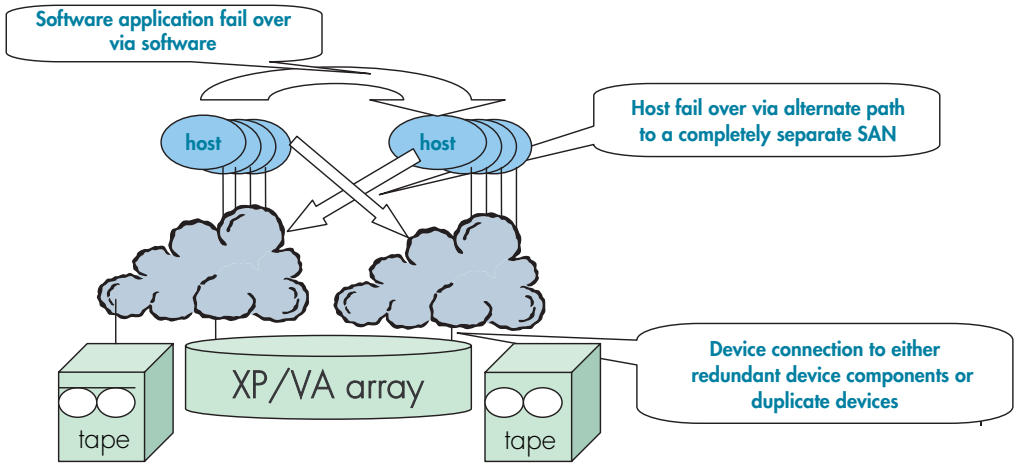


Figure 28: High Availability SAN with XP/VA

However, SANs consisting of a single B-Series Core switch, C-Series Director switch, or M-Series Director switch can be supported for Level 3 high availability as shown in Figure 29. Refer to Chapter 2, "Data Availability in a SAN" for more information.

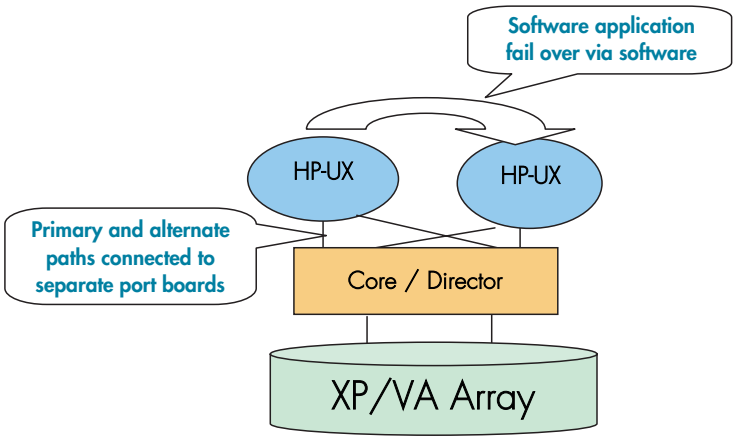


Figure 29: Software application fail-over

XP and VA with multiple operating systems in a shared switch fabric

- Multiple OS’s and multiple clusters can be supported on the same switch/fabric with appropriate zoning
  - host zones must contain homogeneous operating system types only
  - overlapping storage port zones supported if more than one operating system needs to share an array port

- Heterogeneous operating systems may share an XP array port with the appropriate host group/mode settings (see XP array documentation); All others must use a dedicated XP array port.
- Secure Manager XP and Secure Manager VA required for LUN isolation with multiple hosts connected through a shared array port

Table 25: Zoning requirement for OSs sharing the same fabric with XP/VA storage

Platform OR OS type	HP-UX	Linux	Windows	Tru64 UNIX	OpenVMS	Sun Solaris	IBM AIX	Novell NetWare	SGI IRIX
HP-UX	Yes*	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required
Linux	Zoning Required	Yes*	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required
Windows	Zoning Required	Zoning Required	Yes*	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required
Tru64 UNIX	Zoning Required	Zoning Required	Zoning Required	Yes*	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required
OpenVMS	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes*	Zoning Required	Zoning Required	Zoning Required	Zoning Required
Sun Solaris	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes*	Zoning Required	Zoning Required	Zoning Required
IBM AIX	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes*	Zoning Required	Zoning Required
Novell NetWare	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes*	Zoning Required
SGI IRIX	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes*

*Yes indicates these OSes can be part of the same zone in a fabric with XP/VA.

The above table indicates that OS types do not mix in the same zone, however, they can selectively share the storage ports that support this feature across zones. Storage ports can be overlapped in multiple zones.

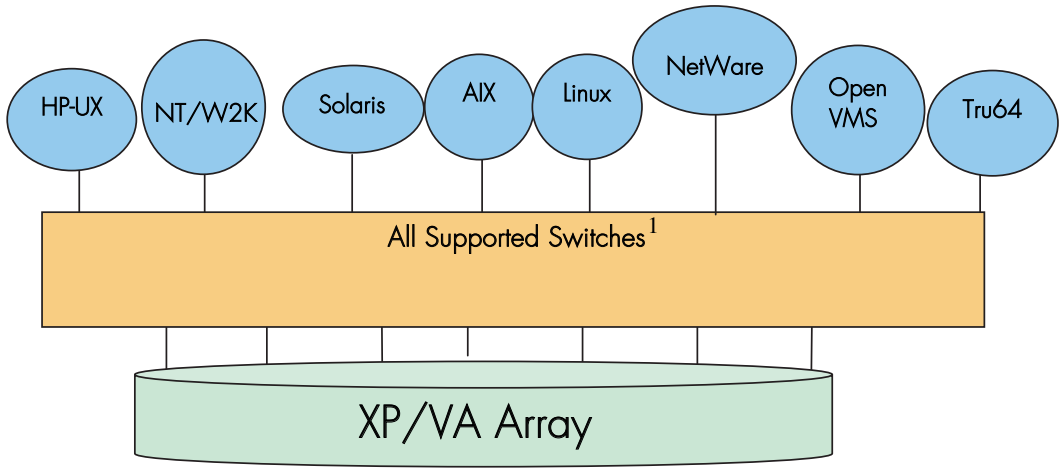


Figure 30: XP/VA with multiple OS's on a shared SAN fabric[1]

XP/VA and Tape with multiple OS's shared switch fabric

- Overlapping zones supported with disk and tape.
- Separate or common HBAs for disk and tape connections.
- Dedicated tape HBA connection is recommended for servers with backups requiring more than 4 DLT8000 tape drives or 2 Ultrium (LTO) tape drives.
- Secure Manager XP and Secure Manager VA required for LUN isolation with multiple hosts connected through a shared array port.
- Contact your HP representative for more information on tape support.

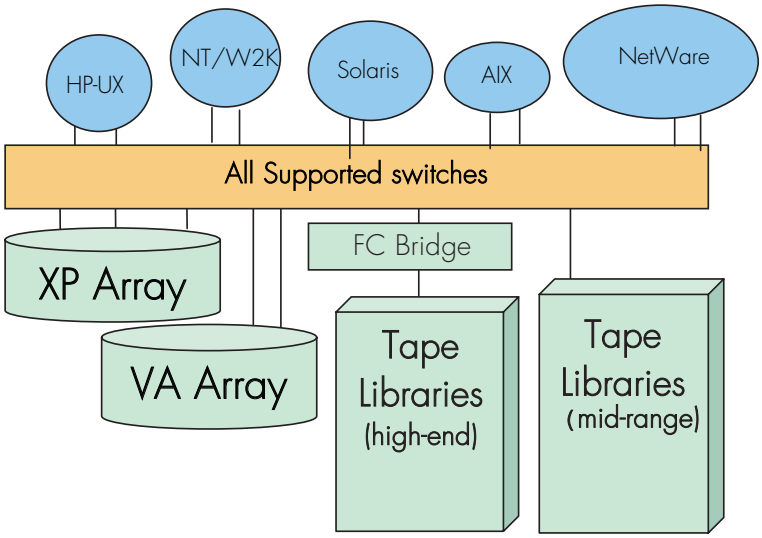


Figure 31: XP/VA with multiple OS's and tapes on a shared SAN fabric, fabric only[1]

Heterogeneous Storage Support

These configuration rules apply for heterogeneous SAN storage with the XP/VA:

- Zone the storage ports to isolate from all other storage vendor zones; no overlapping zones containing multiple storage ports
- Storage ports may be accessed from heterogeneous operating system types and multiple clusters for HA and non-HA configurations; overlapping zones are supported
- Secure Manager required for LUN isolation with multiple hosts connected through a shared array port
- Other vendor array zones governed by their vendor's configuration guidelines.
- Shared HBAs or hosts across 3rd party storage vendors are NOT supported.
- Supports connection to a common server with XP/VA and EVA storage systems. Refer to "Common Server Access."

1. Contact your HP representative for model and firmware versions for supported switches. Third party switches like ED-5000 and Inrange FC 9000 are also supported with some XP arrays, limited to a maximum two switch configurations.

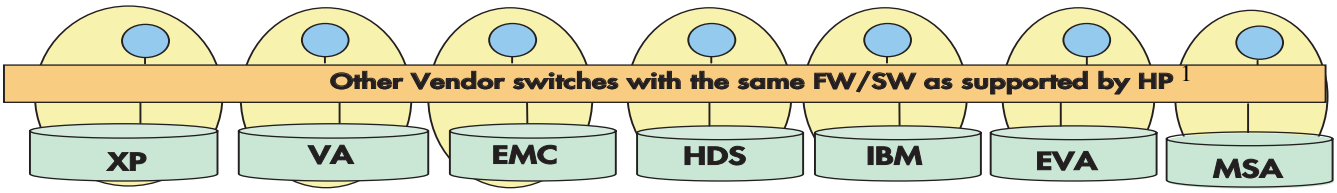


Figure 32: Heterogeneous storage support[1]

Secure Manager Support

Definition:

- HP SureStore E Secure Manager XP is an array based, LUN security and configuration tool.
- Provides the ability to limit access between hosts and array LUNs
- Use host world-wide names to identify host access per LUN

Advantages:

- Provides LUN security at the array level to secure data, irrespective of switch port or direct connect between host and the XP array
- Provides consolidated and consistent data access management independent of switch vendor
- Improves boot performance during ioscan by limiting the visibility between host and targets

---

Note: Product cost must be compared to cost of additional array ports and switch cost requirements

---

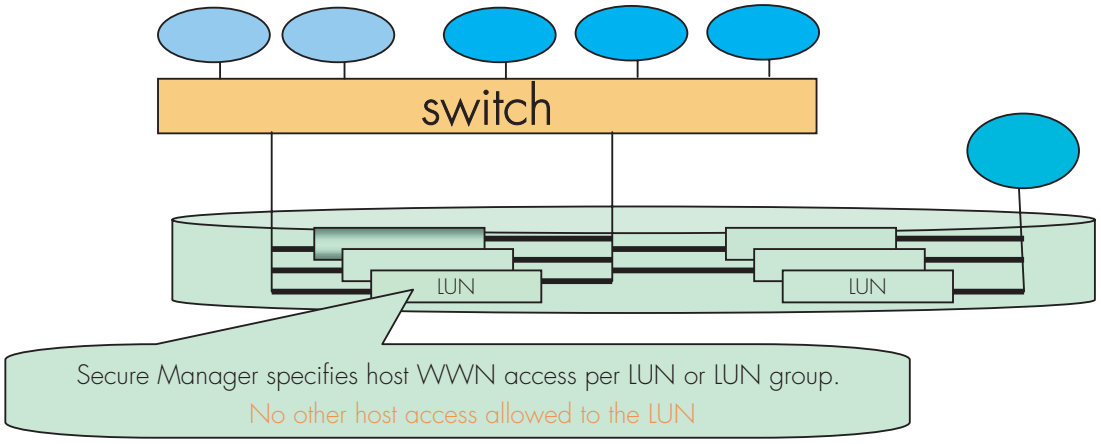


Figure 33: Secure Manager for XP support

---

1. There is support for third party switches like the ED-5000 and the Inrange FC 9000 with some XP arrays, limited to a maximum two switch configuration. Contact your HP representative for specific details.

Note: Since LUNs may be shared across array ports, limiting a host's visibility to a switch port does not limit it's access to LUNs. Array based configuration management, such as Secure Manager, is the only way to ensure data security.

Fabric Boot support for XP/VA

XP and VA LUNs can be booted from the SAN using both SAN B-Series product line switches and SAN M-Series product line switches (contact your HP representative for exceptions.)

Booting from the SAN has dependencies that include PDC code, firmware, HBA, OS version/type, platform speed, and Fibre Channel port speed.

For more information, contact your HP field representative.

The following table describes boot support at a high level. This table does not cover different versions and flavors within each OS type and switch type. "Yes" indicates at least one combination of array, HBA, OS type, and switch is supported as a bootable configuration.

Table 26: XP/VA SAN Boot by Operating System

OS/ Array	HP-UX	Linux	Windows	Tru64 UNIX	Open-VMS	Sun Solaris	AIX	Net-Ware	SGI-IRIX	B-Series Switches	M-Series Switches
XP-1024/128	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
XP-512/48	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
VA-7410	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
VA-7400	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
VA-7110	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
VA-7100	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes

Specific Platform/Operating System Rules – EVA5000/EVA3000 (VCS v3), EMA/ESA12000, EMA16000, MA/RA8000, MA6000 (ACS 8.7) Storage Systems, B-Series and M-Series Switches

This section defines the rules and guidelines related to specific platforms/operating systems for EVA and EMA/ESA/MA/RA8000 storage systems, when used with B-Series and M-Series switches. For operating system storage attachment, HBA attachment, current HBA/driver/FW revision support, multi-pathing software versions, and specific VCS minor release and ACS version patch level support, contact your HP field representative.

HP-UX 11.0, 11.11, 11.23

- Zoning is required when HP-UX is used in a Heterogeneous SAN with other operating systems.
- Supports MC/ServiceGuard. A.11.14/A.11.15 (11.11 only), A.11.15+ (11.23)

VCS v3

EVA5000/EVA3000:

- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover if configured with two or more paths.
- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software at:

  ftp://ftp.compaq.com/pub/products/storageworks/whitepapers
- Supports connection to a common server with EVA and XP/VA storage systems. Refer to "EVA5000/EVA3000 Configuration Rules."
- Does not support L-Port attachment.
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, and MA6000 Storage Systems:

- Supports Transparent failover mode and Multiple-Bus failover mode. Multiple-Bus failover mode is supported for HP-UX version 11.0 and 11.11 using the Secure Path multi-path driver. Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths.
- Supports L-Port attachment with Table 17 Fibre Channel SAN switches that support the QuickLoop feature
- Requires ACS 8.7P or later for DRM support

- Requires that all servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.
- HP-UX 11.23 is not supported with HSG-based storage at this time.

OpenVMS 7.2-2, 7.3, 7.3-1

- Supports OpenVMS Clusters
- Supports Multiple-Bus failover mode. Multi-path driver is embedded in the operating system
- Supports multi-path high availability configuration implemented in separate fabrics or a single fabric
- Zoning required when used in a Heterogeneous SAN with HP-UX, IBM AIX or Linux
- Supports booting over the SAN Fabric. Refer to the section "Booting from the SAN."

VCS v3

- EVA5000/EVA3000 storage is supported.
- Supports connection of single HBA servers, refer to the whitepaper “Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software” (SingleHBAforEVA_F.pdf) at:

  ftp://ftp.compaq.com/pub/products/storageworks/whitepapers
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- All servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.

Tru64 UNIX

- Tru64 UNIX version V5.1 supports TruCluster Server Version 5.1
- Tru64 UNIX version V5.1A supports TruCluster Server Version 5.1A
- Tru64 UNIX version V5.1B supports TruCluster Server Version 5.1B

- Supports multi-path high availability configuration implemented in separate fabrics or a single fabric
- Zoning is required when used in a Heterogeneous SAN with HP-UX, IBM AIX or Linux
- Supports booting over the SAN Fabric. Refer to the section "Booting from the SAN."

5.1, 5.1A, 5.1B – VCS v3

EVA5000/EVA3000:

- Supports Multiple-Bus Failover mode. Multi-path driver is embedded in the V5.1/V5.1A operating systems.
- Supports connection of single HBA servers, refer to the whitepaper “Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software” at:

  ftp://ftp.compaq.com/pub/products/storageworks/whitepapers
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

4.0F, 4.0G, 5.1, 5.1A, 5.1B – ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Tru64 UNIX version 4.0F/4.0G supports Transparent failover mode only.
- Tru64 UNIX version 5.1and 5.1A supports Transparent and Multiple-Bus failover mode. Multi-path driver is embedded in the V5.1/V5.1A/V5.1B operating systems.
- Zoning is required when a SAN is configured for multiple TruCluster products with Tru64 UNIX 4.0F/4.0G. Each TruCluster configured with Tru64 UNIX 4.0F/4.0G must be in its own zone.
- All servers and storage systems configured for DRM (supported on Tru64 versions 5.1, 5.1A, and 5.1B only), must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.

IBM AIX 4.3.3, 5.1, 5.2

- Supports HACMP/ES Clusters 4.4.1 ES, 4.5
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover. Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths.

VCS v3

EVA5000/EVA3000 storage is supported.

- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

For EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems (AIX 5.2 not supported):

- All servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.

Secure Path for IBM AIX

- When using Multiple-Bus Failover and Secure Path for IBM AIX, zoning is required to limit each IBM server HBA access to one controller port per controller since typical installations in a heterogeneous SAN utilize more then one controller port cable connection per controller. Refer to the *Secure Path for IBM AIX Installation and Reference Guide, AA-RLTOC-TE,* for more information. Zoning is required for the AIX servers for instances where the storage system is being shared with other heterogeneous servers that require cabled access to more than one controller port per controller.

Linux

VCS v3 - Red Hat 7.2 (ProLiant x86), Advanced Server 2.1 (BL20P, BL40P, ProLiant x86), SuSE SLES 7 (ProLiant x86), SLES 8, United Linux 1.0

EVA5000/EVA3000:

- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.
- Supports Lifekeeper Clusters 4.4 plus Service Guard 11.14.02/11.15.01 (version is HBA dependant)

- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software" at: http://h18006.www1.hp.com/storage/arraywhitepapers.html
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

ACS 8.7 - Red Hat 7.2 (ProLiant x86), Advanced Server 2.1 (BL20P, BL40P, ProLiant x86), 7.1, 7.2 (Alpha), SuSE 7.2 (ProLiant x86), SuSE SLES 7 (ProLiant x86)

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports Lifekeeper Clusters 4.2
- Supports Transparent failover mode
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software" at:

  http://h18006.www1.hp.com/storage/arraywhitepapers.html
- Multi-pathing with Secure Path is supported on Red Hat Advanced Server 2.1 and SuSE SLES 7 only.

ACS 8.7 - Secure Path for Linux, Red Hat Advanced Server 2.1 (BL20P, BL40P, Proliant x86) SLES 7 (ProLiant x86)

- Supports Multiple-Bus failover mode
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

Microsoft Windows 2000 Server, Advanced Server w/SP2, SP3, SP4 for VCS3.x only, Windows NT 4.0 w/SP6a (BL20P, BL40P, Intel and Proliant x86), Windows 2003 Server

- Supports MSCS for EMA/ESA12000, EMA16000, and MA/RA8000 system in a 2-node configuration only
- Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths
- Zoning is required when used in a heterogeneous SAN with HP-UX, IBM AIX or Linux
- BL20P and BL40P are only supported with Windows 2000 and Windows 2003

VCS v3

EVA5000/EVA3000:

- Supports MS Windows 2003 Enterprise edition (32 bit)
- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover if configured with two or more paths.
- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software at:

  http://h18004.www1.hp.com/products/storageworks/enterprise/documentation.html
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only

Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports MS Windows 2003 Enterprise edition (32 bit) and Standard edition (32 bit) with Multiple-Bus failover only.
- Supports Transparent failover mode and Multiple-Bus failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- All servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.
- Supports booting over the SAN Fabric. Refer to the section "Booting from the SAN."
- Extended Configurations with Microsoft Windows NT 4.0

  If you configure greater than 4 (up to 8) servers (assuming one Fibre Channel HBA per server) for access to a single controller host port on an MA6000, MA/RA8000, EMA/ESA12000, and EMA16000 storage system, and 1 or more of those servers is Windows based, select the "Extended Configuration" check box in the StorageWorks Windows NT/Windows 2000 Platform Kit Fibre Channel Software Setup utility custom installation setup for each Windows server. Select this option to adjust registry settings for your KGPSA host bus adapter to operate in an "Extended Configuration" environment.

Note: The default for this option is checked, so be sure to uncheck this option when you have 4 or fewer servers configured for access to a single controller host port.

Microsoft Windows 2000 Datacenter

- Supports MSCS
- Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths.
- Zoning is required when used in a heterogeneous SAN with HP-UX, IBM AIX or Linux.

VCS v3

EVA5000/EVA3000:

- VCS v3 is supported on WS2003 32/64 bit
- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only

Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports Transparent failover mode and Multiple-Bus failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- Supports heterogeneous operating system shared access to a single storage system when using ACS 8.7. Heterogeneous operating system shared access is not supported with ACS 8.6.

Secure Path for Windows

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports using single host bus adapter with Secure Path and Multiple-Bus failover. Refer to the white paper, *Using Secure Path for Servers with Single Host Bus Adapter (HBA)*, 14JK-0301A-WWEN, available at:

  http://h18006.www1.hp.com/products/sanworks/library/whitepapers/14JK-0301A-WWEN.html
- One instance of the Secure Path Manager can support multiple managed entities called profiles. For 4.x versions of Secure Path, a single profile can consist of up to 128 servers total, standalone or clustered, connected to and sharing up to 128 storage systems. For 3.x versions of Secure Path, a single profile can consist of up to 8 standalone servers connected to and sharing up to 8 storage systems, or up to 8 clustered servers connected to and sharing up to 8 storage systems. For 3.x versions, you cannot manage both standalone and clustered servers in the same profile.
- Secure Path configurations utilizing 4 active controller ports connected to the same server or servers offer the flexibility to use the 4 active ports for either increased total LUN count, or increased PATH accessibility to a lesser number of LUNs. Refer to the section “High Availability Configuration Considerations” in this chapter for more information.
- Provides for dynamic port I/O load distribution in non-clustered servers when configured for maximum paths.
- Distribute units equally across both controllers for proper static load balancing using the Unit Preferred Path parameter to assign units to a specific controller at initial boot.
- SSP/LUN level masking - Storagesets (LUNs) must be enabled for access from all server or clustered server paths using the storage LUN presentation or Unit Connection Name parameter feature.
- For Windows NT or Windows 2000, when using Secure Path in single or dual fabric configurations with both Multiple-bus Failover and Transparent Failover storage systems, the Transparent Failover storage systems must be in a different fabric zone and not be accessed by servers running Secure Path multipath software.

Novell NetWare

- Supports NetWare Clusters 1.7 (NetWare 6.5) for EVA5000/EVA3000 only, 1.06 (NetWare 6) and 1.01 (NetWare 5.1)
- Zoning required when used in a Heterogeneous SAN with Sun, HP-UX, IBM AIX, or Linux

5.1, 6, 6.5 – VCS v3

EVA5000/EVA3000:

- NetWare 6.5 is supported with VCS v3 only.
- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover if configured with two or more paths. Multiple-Bus Failover configurations currently support clusters with a maximum of two nodes.
- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software" at:

  http://h18006.www1.hp.com/storage/arraywhitepapers.html
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

4.2 – ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems supported using Transparent failover mode only.

5.1 SP6, 6 SP3– ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports NetWare Clusters.
- Supports Transparent failover mode and Multiple-Bus failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths.
- All servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined inTable 27.

Sun Solaris 2.6, 7, 8, 9

- Supports Sun Clusters v2.2 (Solaris 7 and 8), Veritas Clusters 3.5 (Solaris 7, 8, and 9), and VxVM 3.2/Veritas clusters 2.0 No DMP (Solaris 7, 8.) Each cluster must be in its own zone.
- Zoning required when used in a Heterogeneous SAN with NetWare, HP-UX, IBM AIX, or Linux
- Supports multi-path high availability configuration implemented in separate fabrics or in a single fabric with zoned paths.

VCS v3

EVA5000/EVA3000:

- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover if configured with two or more paths.
- Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software" at:

  ftp://ftp.compaq.com/pub/products/storageworks/whitepapers
- Supports Sun Clusters and Veritas Clusters 2.0 and 3.5. A cluster must be in its own zone.
- Supports 64-bit cPCI HBA on Solaris 8 and 9 (64 bit SBUS and 32 bit PCI are supported on 2.6, 7, 8 only)
- 32-bit Sbus HBA not supported
- When using Continuous Access on EVA5000 with VCS v3 or EVA 5000/3000 on V3.01, HP recommends that all servers and storage systems configured for Continuous Access EVA be in a High Availability SAN of two fabrics (Figure 44), and contain only Continuous Access EVA supported operating systems. If servers running non-supported operating systems exist within the SAN, they should be excluded from the Continuous Access management environment via zoning. In addition, that SAN (or management zone within a larger SAN) is limited to a maximum of 16 EVA, and 256 HBA per EVA. Additional operating system specific zones within the larger Continuous Access environment zone may be required as defined in Table 27. See the *Continuous Access EVA Design Reference Guide* for additional details and configuration limitations.

ACS 8.7

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems:

- Supports Transparent failover mode and Multiple-Bus failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- Supports Sun Clusters and Veritas Clusters. A cluster must be in its own zone.
- Supports 64-bit cPCI HBA on Solaris 8 and 9 (64 bit SBUS and 32 bit PCI are supported on 2.6, 7, 8 only)

All servers and storage systems configured for DRM must be in a zone or group of zones that excludes all non DRM supported operating systems. Multiple DRM zones are supported to reduce the size and/or complexity of a particular DRM solution instance. Multiple zones may be required due to multiple operating systems as defined in Table 27.

Specific Platform/Operating System Rules – Enterprise Virtual Array (VCS v3.010), EMA/ESA12000, EMA16000, MA/RA8000 (ACS 8.7) Storage Systems, C-Series Switches

This section defines the rules and guidelines related to specific platforms/operating systems for EVA and EMA/ESA/MA/RA8000 storage systems, when used with C-Series switches. For operating system storage attachment, HBA attachment, current HBA/driver/FW revision support, multi-pathing software versions, and specific VCS and ACS version patch level support, refer to you HP representative for more information.

HP-UX 11.0, 11.11, 11.23

- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Clusters are supported with Service Guard version A.11.14 for HP-UX v11.0 and 11.11.

VCS v3.010

Enterprise Virtual Array:

- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- Supports SAN extension over FCIP with the MPS 9000 IP Storage Services Module.

Microsoft Windows 2000 Server, Advanced Server w/SP3, NT 4.0, Windows 2003

- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Clusters are not supported at this time.

Supported HBAs:

- KGPSA-CB
- FCA2355
- FCA2101
- FC Mezzanine Card
- FCA2214, FCA2214DC

Boot Support (EVA):

- FCA2355 (Windows 2000, 2003 only)

VCS v3.010

Enterprise Virtual Array:

- Supports Multiple-Bus Failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.
- Windows 2003 (64-bit) supported on Itanium class servers only.

ACS 8.7

- Supports Transparent failover mode and Multiple-Bus failover mode. Secure Path multi-path driver is required for Multiple-Bus failover.

OpenVMS 7.3-2, 7.3-1, 7.2-2, Tru64 UNIX 5.1A, 5.1B

- Supports TruCluster Server and OpenVMS Clusters.
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Failover between C-Series to B-Series switches or to M-Series switches is not supported
- EVA is supported with VCS 3.010

Supported HBAs:

- DS-KGPSA-CA
- DS-KGPSA-DA
- DS-KGPSA-EA

Supported storage systems:

- EMA/ESA12000, EMA16000, MA/RA8000
- EVA5000/EVA3000

Boot Support:

- DS-KGPSA-DA
- DS-KGPSA-EA

IBM AIX 4.3.3, 5.1

- Clusters are supported with HACMP/Es 4.4.1
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- EVA is supported with VCS 3.010

Supported HBAs:

- DS-SWIA1-PD (197819-B21)

Linux Red Hat AS 2.1(32-bit, 64-bit), SuSE 8(32-bit)

- Clusters are supported with LifeKeeper Clusters 4.2
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Red Hat AS 2.1 (64-bit) is not supported with clusters
- EVA is supported with VCS 3.010

Sun Solaris 8, 9

- EVA is supported with VCS 3.010
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

Supported HBAs:

- SWSA4-PC
- FCA2257P
- FCA2257C

Supported Servers:

- V480
- V880
- V880Z
- Sunfire 4800, 4810, 6800

Specific Platform/Operating System Rules – XP128/1024, XP48/512, XP256, C-Series Switches

This section defines the rules and guidelines related to specific platforms/operating systems for XP128/1024, XP48/512, and XP256 storage systems, when used with C-Series switches. For operating system storage attachment, HBA attachment, current HBA/driver/FW revision support, multi-pathing software versions, and specific VCS and ACS version patch level support, refer to you HP representative for more information.

HP-UX 11.0, 11.11, 11.23

- Supported with a single-switch fabric only.
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Clusters are supported with Service Guard version A.11.14 .

Contact your HP Representative for supported server models.

Red Hat Linux 7.1, AS 2.1, SuSE Enterprise Server 8 (i386)

- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Single-path support only.
- Clustering is not supported.
- XP256 is not supported.

Windows Server 2003 32-bit Enterprise and Standard Edition 64-bit Datacenter and Enterprise Edition, Windows NT 4.0, 2000 with SP3, SP4

- Boot is not supported
- Clustering is not supported.
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

Contact your HP Representative for supported HBAs.

Sun Solaris 2.6, 7, 8, 9

- Not supported with XP256
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

IBM AIX 4.3.3, 5.1

- Not supported with XP256
- Zoning is required when used in a Heterogeneous SAN with other operating systems.

Supported HBA:

- FC6228

Supported server:

- P610

Tru64 UNIX 5.1A, 5.1B
OpenVMS 7.2-2, 7.3-1

- Boot is not supported.
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- Clustering is not supported.
- Failover from C-Series to B-Series or to M-Series switches is not supported.

Supported HBAs:

- DS-KGPSA-EA
- DS-KGPSA-BC

Specific Platform/Operating System Rules – VA7410, VA7110, C-Series Switches

This section defines the rules and guidelines related to specific platforms/operating systems for the VA7410 and VA7110 storage systems, when used with C-Series switches. For operating system storage attachment, HBA attachment, current HBA/driver/FW revision support, multi-pathing software versions, and specific VCS and ACS version patch level support, refer to you HP representative for more information.

HP-UX 11.00, 11.11

- Zoning is required when used in a Heterogeneous SAN with other operating systems.

Supported HBAs:

- A6795A
- A5158A

Supported servers:

- N-class: rp7410
- L-class: rp5470
- A-class: rp2450

Linux Suse Enterprise Server 7 (i386)

- Single-path support only
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- No clustering support

Windows 2000 Server, Advanced Server SP3, SP4

- No boot support
- Zoning is required when used in a Heterogeneous SAN with other operating systems.
- No clustering support

Supported HBAs:

- FCA2101
- FCA2355
- LP8000
- FCA2214
- BL20P Mezzanine HBA

Heterogeneous SAN Platform Interoperability for EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems

For the EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 heterogeneous SAN platform interoperability is defined in Table 27. A "*Yes*" in the table indicates that the listed platforms can be configured for shared access to the same storage system. "*Zoning Required*" indicates the platforms listed must be configured in different fabric zones in order to co-exist in the same physical SAN or share the same EVA5000/EVA3000 or EMA/ESA12000, EMA16000, MA/RA8000, MA6000. For C-Series switches, each operating system type must be in a separate zone or a separate VSAN.

For EMA/ESA12000, EMA16000, MA/RA8000, MA6000 storage systems there are three levels of heterogeneous interoperability rules: platform zoning rules, controller SCSI-modes, and controller failover modes.

The platform zoning rules define which platforms or operating systems must be in different fabric zones in order to coexist in the same physical SAN. Refer to Table 27, "SAN/Platform Zoning Requirements for EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems (B-Series and M-Series switches)."

The controller SCSI-mode and controller failover rules define which platforms or operating systems can be configured for shared access to a single shared storage system based on controller SCSI-mode and failover mode compatibility. Refer to Table 28, "Compatible SCSI Modes for EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems Using ACS 8.7" and Table 29, "Compatible Failover Modes for EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems Using ACS 8.7."

An additional table, Table 30, combines (and to some extent repeats) the information from the other tables into a single table that can be quickly referenced to determine the settings and rules for mixing all possible combinations of any two platforms.

Platform Zoning Rules

This table summarizes the zone compatibility for different platforms in a SAN using B-Series or M-Series switches. Platforms in the same columns can coexist in the same zone. For C-Series switches, each operating system type must be a separate zone.

Table 27: SAN/Platform Zoning Requirements for EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems (B-Series and M-Series switches)

Platform or Operating System	HP-UX	OpenVMS	Tru64 UNIX	IBM AIX	Linux	Microsoft Windows	Novell NetWare	Sun Solaris
HP-UX	Yes	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Zoning Required
OpenVMS	Zoning Required	Yes	Yes	Zoning Required	Zoning Required	Yes	Yes	Yes
Tru64 UNIX	Zoning Required	Yes	Yes	Zoning Required	Zoning Required	Yes	Yes	Yes
IBM AIX	Zoning Required	Zoning Required	Zoning Required	Yes	Zoning Required	Zoning Required	Zoning Required	Zoning Required
Linux	Zoning Required	Zoning Required	Zoning Required	Zoning Required	Yes	Zoning Required	Zoning Required	Zoning Required

Table 27: SAN/Platform Zoning Requirements for EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems (B-Series and M-Series switches)

Platform or Operating System	HP-UX	OpenVMS	Tru64 UNIX	IBM AIX	Linux	Microsoft Windows	Novell NetWare	Sun Solaris
Microsoft Windows	Zoning Required	Yes	Yes	Zoning Required	Zoning Required	Yes	Yes	Yes
Novell NetWare	Zoning Required	Yes	Yes	Zoning Required	Zoning Required	Yes	Yes	Zoning Required
Sun Solaris	Zoning Required	Yes	Yes	Zoning Required	Zoning Required	Yes	Zoning Required	Yes

Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
NetWare OpenVMS Tru64 UNIX Microsoft Windows	Sun OpenVMS Microsoft Windows	Linux	HP-UX	IBM AIX

Note: The above table is summarized as:

- NetWare and Sun platforms are incompatible in the same zone.
- HP-UX, IBM AIX, and Linux platforms are each incompatible in zones with all other platforms.

Compatible Controller SCSI-Modes and Controller Failover Modes

The following tables summarize information about supported controller SCSI modes and failover modes for all platforms. Table 28 summarizes information about compatible SCSI modes and Table 29 summarizes information about supported storage system failover modes for all platforms for EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems using ACS 8.7.

Table 28: Compatible SCSI Modes for EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems Using ACS 8.7

SCSI-2 CCL	SCSI-2 No CCL	SCSI-3
HP-UX	HP-UX	HP-UX
		OpenVMS
Tru64 UNIX 4.0F, 4.0G	Tru64 UNIX 4.0F, 4.0G	
Tru64 UNIX 5.1, 5.1A, 5.1B	Tru64 UNIX 5.1, 5.1A, 5.1B	Tru64 UNIX 5.1, 5.1A, 5.1B
IBM AIX	IBM AIX	IBM AIX
		Linux
	Microsoft Windows	Microsoft Windows
Novell NetWare	Novell NetWare	Novell NetWare
Sun Solaris	Sun Solaris	Sun Solaris

Table 29: Compatible Failover Modes for EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems Using ACS 8.7

Transparent	Multiple-Bus
HP-UX	HP-UX
	OpenVMS
Tru64 UNIX 4.0F, 4.0G, 5.1, 5.1A, 5.1B	Tru64 UNIX 5.1, 5.1A, 5.1B
IBM AIX	IBM AIX
Linux	
SuSE SLES 7 (ProLiant x86)	
Microsoft Windows	Microsoft Windows
Novell NetWare	Novell NetWare
Sun Solaris	Sun Solaris

Combined Shared Access Interoperability Table

Table 30 combines the information from the previous tables into a single table. The table can be used to determine controller settings for a single EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems using ACS 8.7, being shared between two or more platforms and operating systems.

Table 30: Platform Interoperability for Single Shared EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems – ACS 8.7

Platform or Operating System	HP-UX MC/ ServiceGuard Clusters	OpenVMS Clusters	Tru64 UNIX 4.0F, 4.0G Trucluster Software Products V1.6	Tru64 UNIX 5.1, 5.1A, 5.1B TruCluster Server Version 5.1, 5.1A, 5.1B	IBM AIX	Linux	Microsoft Windows MSCS	Novell NetWare 5.1, 6, 6.5 Clusters 1.01, 1.06	Sun Solaris Sun Clusters VERITAS Clusters
HP-UX MC/ Service-Guard Clusters	Fabric attachment Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3 FC-AL attachment, Transparent or Multiple-Bus LOOP_HARD SCSI-2	Fabric attachment With Zoning Multiple-Bus FABRIC SCSI-3	Fabric attachment With Zoning Transparent FABRIC SCSI-2	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	Fabric attachment With Zoning Transparent FABRIC SCSI-3	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	Fabric attachment With Zoning Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3
OpenVMS Clusters	Fabric attachment With Zoning Multiple-Bus FABRIC SCSI-3	Multiple-Bus FABRIC SCSI-3	Requires two storage systems	Multiple-Bus FABRIC SCSI-3	With Zoning Multiple-Bus FABRIC SCSI-3	Requires two storage systems	Multiple-Bus FABRIC SCSI-3	5.1, 6: Multiple-Bus FABRIC SCSI-3 4.2: Requires two storage systems	Multiple-Bus FABRIC SCSI-3
Tru64 UNIX 4.0F, 4.0G Trucluster Software Products V1.6	Fabric attachment With Zoning Transparent FABRIC SCSI-2	Requires two storage systems	Transparent FABRIC SCSI-2	Transparent FABRIC SCSI-2	With Zoning Transparent FABRIC SCSI-2	Requires two storage systems	Transparent FABRIC SCSI-2 No CCL	Transparent FABRIC SCSI-2	Transparent FABRIC SCSI-2
Tru64 UNIX 5.1, 5.1A, 5.1B TruCluster Server Version 5.1, 5.1A, 5.1B	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	Multiple-Bus FABRIC SCSI-3	Transparent FABRIC SCSI-2	Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Transparent FABRIC SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3

Table 30: Platform Interoperability for Single Shared EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems – ACS 8.7

Platform or Operating System	HP-UX MC/ ServiceGuard Clusters	OpenVMS Clusters	Tru64 UNIX 4.0F, 4.0G Trucluster Software Products V1.6	Tru64 UNIX 5.1, 5.1A, 5.1B TruCluster Server Version 5.1, 5.1A, 5.1B	IBM AIX	Linux	Microsoft Windows MSCS	Novell NetWare 5.1, 6, 6.5 Clusters 1.01, 1.06	Sun Solaris Sun Clusters VERITAS Clusters
IBM AIX	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Multiple-Bus FABRIC SCSI-3	With Zoning Transparent FABRIC SCSI-2	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Transparent FABRIC SCSI-3	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	With Zoning Transparent or Multiple Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3
Linux	Fabric attachment With Zoning Transparent FABRIC SCSI-3	Requires two storage systems	Requires two storage systems	With Zoning Transparent FABRIC SCSI-3	With Zoning Transparent FABRIC SCSI-3	Transparent FABRIC SCSI-3	With Zoning Transparent FABRIC SCSI-3	With Zoning Transparent FABRIC SCSI-3	With Zoning Transparent FABRIC SCSI-3
Microsoft Windows MSCS	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	Multiple-Bus FABRIC SCSI-3	Transparent FABRIC SCSI-2 No CCL	Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	With Zoning Transparent FABRIC SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 No CCL or SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3
Novell NetWare 5.1, 6, 6.5 Clusters 1.01, 1.06	Fabric attachment With Zoning Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	5.1, 6: Multiple-Bus FABRIC SCSI-3 4.2: Requires two storage systems	Transparent FABRIC SCSI-2	Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	With Zoning Transparent or Multiple Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	With Zoning Transparent FABRIC SCSI-3	Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 No CCL or SCSI-3	Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	With Zoning Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3
Sun Solaris Sun Clusters VERITAS Clusters	Fabric attachment With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	Multiple-Bus FABRIC SCSI-3	Transparent FABRIC SCSI-2	Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3	With Zoning Transparent FABRIC SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 No CCL or SCSI-3	With Zoning Transparent or Multiple-Bus (5.1, 6) FABRIC SCSI-2 or SCSI-3	Transparent or Multiple-Bus FABRIC SCSI-2 or SCSI-3

Booting from the SAN

Table 31 indicates the platforms and operating systems that are currently able to boot from SAN storage.

Table 31: EVA, EMA/ESA12000, EMA16000, MA/RA800, MA6000 SAN Boot by Operating System

Platform/Operating System	Comments
Microsoft Windows 2000 Server, Advanced Server, Windows NT 4.0 MSCS MS Windows Server 2003 Standard Edition and Enterprise Edition (32-bit)	EVA5000/EVA3000 EMA/ESA12000,EMA16000, MA/RA8000, MA6000, MSA1000 (B-Series and M-Series switches only) HBA's supported for Windows NT, Windows 2000 & 2003: DS-KGPSA-CB, FCA2101, FCA2355 HBA's supported for Widows 2000 & 2003 only: FC2214, FCA2214DC, FCA2404 Refer to *Booting Windows from a Storage Area Network* (AA-RS2UG-TE) for more information
OpenVMS Clusters	EVA5000/EVA3000: HBA: DS-KGPSA-CA (B-Series and M-Series switches only), DS-KGPSA-DA, DS-KGPSA-EA EMA/ESA12000, EMA16000, MA/RA8000, MA6000, MSA1000, HBA: DS-KGPSA-CA/DA/EA Requires use of *wwidmgr,* SRM console firmware v6.5 (minimum)
Tru64 UNIX TruCluster Software Products	
Linux (32-bit)	Refer to *Booting 32-Bit Linux Systems from a Storage Area Network* (AA-RV1AB-TE) for more information.
Red Hat Enterprise Linux 2.1 (Red Hat) - QU2 SUSE Linux Enterprise Server 8 (SUSE8) - Service Pack 2a	B-Series and M-Series switches only FCA2214, FCA2214DC Dual Port Fibre Channel Mezzanine Card (2 Gb) for BL20Gp2 G2 Enterprise Virtual Arrays (EVA5000 and EVA3000) with VCS 3.010 Enterprise Modular Arrays (RA8000, MA8000, EMA12000, EMA16000, ESA 12000 Fibre Channel) with ACS 8.7-3

Any version of Continuous Access EVA or DRM also supports the replication of the boot disk as long as the page and swap files are not on that disk. HP recommends that these two disks be placed on storage internal to the server due to the high performance needed. This support is limited to those operating systems listed in Table 31.

Specific Storage System Rules

HP XP and VA Configuration Rules

1. XP storage systems are supported in all SAN fabric topology configurations described in this guide in SANs using the Fibre Channel switches listed in Table 17 (B-Series), Table 18 (C-Series), and Table 20 (M-Series) except when otherwise listed below.
2. VA storage systems are supported in all SAN fabric topology configurations described in this guide in SANs using the Fibre Channel switches listed in Table 17 (B-Series), Table 18 (C-Series), and Table 20 (M-Series).
   - C-Series switches support VA7410 and VA7110 models only.
3. VA storage systems supported shared between MSCS (Windows) and MC/Service Guard (HP-UX) clusters. Requires proper assignment and securing of LUNs to the individual clusters.
4. In general, servers accessing HP XP or VA storage systems must not have access to EVA5000/EVA3000, EMA/ESA12000, EMA16000, MA/RA8000, MA6000, MSA1000, RA4100, or RA4000 storage systems. Zoning is required when configuring these storage system types in the same physical SAN. Refer to "Common Server Access", page 94, for supported common server access configurations.

EVA5000/EVA3000 Configuration Rules

1. The EVA5000/EVA3000 Storage System is supported in all SAN Fabric topology configurations described in this guide. The EVA5000/EVA3000 is compatible in SANs using the Fibre Channel switches listed in Table 17, Table 18, and Table 20.
2. For SANs with more than 1024 HBAs, an HSV controller must be zoned so that it can see no more than 1024 HBAs. It may be necessary to add a zone to a SAN to satisfy the 1024 HBA limit. (The limit is 256 HBAs when using Continuous Access EVA.)
3. The supported platforms and operating systems are listed in this section on page 104.
4. Shared access and heterogeneous platform zoning requirements are listed in Table 30.
5. Supports Multiple-Bus Failover mode only. Generally, Multiple-Bus Failover requires a minimum of 2 Fibre Channel HBAs and native operating system or layered multi-path driver functionality. Refer to the whitepaper listed below for exceptions.
6. Supports connection of single HBA servers, refer to the whitepaper "Connecting Single HBA Servers to the Enterprise Virtual Array without Multipathing Software" at:

   ftp://ftp.compaq.com/pub/products/storageworks/whitepapers and also

   http://storage.inet.Compaqcorp.net/Document_Storage/whitepapers/new_library/SingleHBA_for_EVA-HP3_121002.pdf

---

Note: Servers without multi-pathing software are NOT supported by Continuous Access EVA at this time.

---

7. Overlapping zones are supported with disk and tape.
8. Overlapping storage port zones supported if more than one operating system needs to share an array port.

9. Supports simultaneous access to EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage systems and the EVA5000/EVA3000 from the same Server/HBA when both storage system families use common HBA, driver, and multi-path software versions. Refer to "Common Server Access", page 94 for more information.

   Refer to Chapter 3 for information about configuring the Storage Management Appliance to manage EVA5000/EVA3000s and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 storage systems in the same SAN.

10. In general, servers accessing EVA5000/EVA3000s must not have access to HP XP or VA storage systems, or MSA1000, RA4100 or RA4000 storage systems. Zoning is required when configuring these storage system types in the same physical SAN. Refer to "Common Server Access", page 94 for supported common server access configurations.
11. SSP/LUN level masking – Use storage system LUN presentation to enable/disable LUN access to specific hosts.
12. All host table entries must have the proper operating system type parameter set based on the platform type accessing the assigned LUNs.

Note: Shared access between different servers to the same storage unit (LUN) requires specific application software (i.e., cluster software) to ensure proper data preservation.

EVA5000/EVA3000 Maximums

Table 32 lists the maximum connections supported by EVA5000 and EVA3000 storage systems. In addition, Table 32 lists the maximum supported storage limits for each hardware platform or operating system. The maximums shown here are for access to a single EVA5000/EVA3000 with dual redundant controllers. If the connection requirements for the number of servers in a particular SAN exceed the maximums, then deploy multiple storage systems within the SAN.

Note: This section specifies general EVA limits. Specific solution subset configurations such as high availability clusters or applications such as Continuous Access (see SAN/Continuous Access EVA Integration) may impose lower level limits on connectivity for the solution. In these instances, the solution limits must be adhered to as specified by the solution configuration documentation.

- Maximum of 1024 Host Bus Adapters (HBA)
- Maximum of 512 LUNs
- Maximum of 256 Hosts: A Host is defined to contain one or more HBAs
- The total number of LUN Presentations for all LUNs must not exceed 8192
  A LUN Presentation is defined as the number of Hosts a LUN is presented to, irrespective of how many adapters might be in any given Host
  (e.g.If a LUN is presented to 8 Hosts then that LUN has 8 LUN Presentations
  If a LUN is presented to 2 Hosts then that LUN has 2 LUN Presentations).

  Ex:

LUNs #001 thru #032 are presented to a 8 Node Cluster	= 0256 LUN Presentations
LUNs #033 thru #064 are presented to a 8 Node Cluster	= 0256 LUN Presentations
LUNs #065 thru #096 are presented to a 8 Node Cluster	= 0256 LUN Presentations
LUNs #097 thru #128 are presented to a 8 Node Cluster	= 0256 LUN Presentations
LUNs #129 thru #160 are presented to a 8 Node Cluster	= 0256 LUN Presentations

LUNs #161 thru #192 are presented to a 4 Node Cluster = 0128 LUN Presentations
LUNs #193 thru #200 are presented to a single host = 0008 LUN Presentations
Total LUN Presentations = 1416 LUN Presentations

- When all LUNS are presented to all Hosts then the following simpler rule applies: The # of LUNs times the # of Hosts must not exceed 8192

Table 32: SAN/Platform Storage Maximums - EVA5000

Platform or Operating System	Host Bus Adapters per Server	Active Controller Ports (Targets) per HBA	LUNs per HBA Target
See **Reference Notes**	1	2	3, 4
HP-UX	16	4	128
OpenVMS	26	128	511 (9999)
Tru64 UNIX	64	128	255
IBM AIX	16	4 (2 storage systems)	32
Linux	4	4 (2 storage systems)	32 (128)
Microsoft Windows	8	4 (2 storage systems)	8/64
Novell NetWare	4	16 (8 storage systems)	128
Sun Solaris	16	4 (2 storage systems)	128

Reference Notes

1. The maximum number of HBAs supported per server is dependent on the specific server model.
2. For Tru64 UNIX and OpenVMS this column typically represents the total number of active controller ports per HBA when accessing all ports of a storage system or ports on multiple storage systems. For all other platforms, this column typically represents 2 ports per storage system, or a total of 4 ports across 2 storage systems. Use of zoning may be required to limit the number of active targets presented to each HBA to the maximums stated for each platform in this column.
3. Microsoft Windows NT supports 8 LUNs per HBA target with Large LUN feature disabled and 64 LUNs per HBA target with Large LUN feature enabled. Windows 2000 supports Large LUN by default (LUNs 0 - 199), Secure Path for Windows supports usage of LUNs 0 - 63.
4. For Sun configurations configured with the same HBA accessing both an EVA5000/EVA3000 and an EMA/ESA12000, EMA16000, MA/RA8000, or MA6000, the maximum number of LUNs per HBA target is 64 for the EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage system.

EVA5000/EVA3000 Microsoft Windows Cluster Maximums

The maximum number of nodes which are part of a Microsoft cluster attached to one Enterprise Virtual Array may not exceed a total amount of 32 nodes. For example, the following configurations are all valid:

- sixteen 2-node Windows 2000
- four 8-node Windows Server 2003
- two 2-node Windows 2000, three 4-node Windows Server 2003, and two 8-node Windows Server 2003

While using Continuous Access an Enterprise Virtual Array may not exceed these figures, even after a failover has been performed, as the limits are based on numbers of nodes/hosts whether or not LUN are actively presented to the node/host.

Additional standalone servers of any supported type, or non-Windows clustered servers, up to the limit per EVA specified for the particular clustered operating system, may be added up to the total published EVA limit of 256 servers.

EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Configuration Rules

1. These storage systems are supported in all SAN Fabric topology configurations described in this guide. These storage systems are supported in SANs using the Fibre Channel switches listed in Table 17, Table 18, and Table 20.
2. Limit the number of connections visible to each storage system to a maximum of 96 by using fabric zoning. (This is the maximum supported limit for ACS 8.7).
3. See this section beginning on page 104 for supported platforms and operating systems
4. Shared access and heterogeneous platform zoning requirements are listed in Table 30. The heterogeneous platform and operating system mix in the SAN determines the appropriate controller topology attachment, SCSI mode, and Command Console LUN settings for shared storage systems.
5. Overlapping zones are supported with disk and tape.
6. Overlapping storage port zones supported if more than one operating system needs to share an array port.
7. Single or dual redundant controller configurations are supported. For dual redundant controllers, the available failover modes are Transparent and Multiple-Bus. Multiple-Bus failover requires native operating system or layered multi-path driver functionality.

Note: Windows 2003 is not supported with Transparent failover mode.

---

8. All host connection table entries must have the proper operating system type parameter set based on the platform type accessing the assigned LUNs.
9. Supports simultaneous access to EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage systems and the EVA5000/EVA3000 from the same Server/HBA when both storage system families use common HBA, driver, and multi-path software versions. Refer to“Common Server Access”, page 94 for more information.

   Refer to Chapter 3 for information about configuring the Storage Management Appliance to manage EVA5000/EVA3000s and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 storage systems in the same SAN.
10. Servers accessing EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage systems must not have access to HP XP or VA, storage systems, or MSA1000, RA4000, or RA4100 storage systems. Zoning is required when configuring these storage system types in the same physical SAN.
11. SSP/LUN level masking – Use storage system Selective Storage Presentation to enable/disable LUN access to specific connections. Use the unit offset feature to provide needed LUN numbering for host connections. The default LUN numbering for Transparent Failover mode is 0 to 99 for controller port 1 and 100 to 199 for controller port 2. For Multiple-bus Failover mode the default LUN numbering is 0 to 199 on all controller ports.

Note: Shared access between different servers to the same storage unit (LUN) requires specific application software (i.e., cluster software) to ensure proper data preservation.

12. F-Port fabric attachment to the SAN is available through all Fibre Channel switches listed in Table 17 and Table 20. Controller setting is FABRIC topology.
13. FL-Port fabric loop attachment to the SAN with QuickLoop is available through certain Fibre Channel SAN switch models. Refer to Table 17 and the specific Fibre Channel SAN switch model documentation for more information. Controller port topology set to "LOOP_HARD".
14. All controller ports must be set to the same topology type.

Maximum Paths or Maximum LUNs

For EMA/ESA12000, EMA16000, MA/RA8000, or MA6000 storage systems, use the HSG60/80 controller Unit Offset feature to maximize path accessibility or to maximize the number of LUNs.

- **For Maximum Controller Path Accessibility to the same set of LUNs**

  Use a common unit offset value for all 4 controller ports. Access to a common set of LUNs through all 4 controller host ports is provided by using the same unit offset value on all controller host port connections for each server. For example, set the unit offset value for connections on all 4 controller ports to zero (0) for a given server. The server will be capable of accessing one set of LUNs beginning with LUN 0 (LUN 0 is the Command Console LUN if set to SCSI-3 mode) from all 4 controller host ports. This method provides for the highest number of paths to a given set of LUNs.

- **For Maximum LUN Count**

  Use distinct controller port unit offsets for each port pair. Access one set of LUNs with controller port 1 of each controller and access a different set of LUNs with controller port 2 of each controller. For example, set the unit offset value for connections on controller port 1 of each controller to zero, and then set a unit offset value for connections on controller port 2 of each controller to 100 for a given server. The server will be capable of accessing one set of LUNs beginning with LUN 0 (LUN 0 is the Command Console LUN if set to SCSI-3 mode) through controller port 1 on each controller, and a second set of LUNs beginning with LUN 100 through controller port 2 of each controller. This method provides the highest number of LUNs accessed through a reduced number of paths. It also allows for the highest number of servers. Refer to Figure 34.

EMA/ESA12000, EMA16000, MA/RA8000, and MA6000 Maximums

Table 33 lists the maximum supported storage limits for each hardware platform or operating system. The maximums shown are for access to MA6000 storage systems with dual redundant HSG60 controllers, and EMA/ESA12000, EMA16000, or MA/RA8000 storage systems with dual redundant HSG80 controllers. If the maximums listed are below the requirements for the number for servers required, deploy multiple storage systems within the SAN.

Table 33: Platform Maximums - MA6000, MA/RA8000, EMA/ESA12000, EMA16000 Storage Systems Using ACS 8.7

Platform or Operating System	Host Bus Adapters per Server	Active Controller Ports (Targets) per HBA	LUNs per HBA Target	Port Maximums HBAs per Active Controller Port		Storage System Maximums HBAs per Storage System	
Controller Failover Mode				TF	MB	TF	MB
HP-UX 11.0, 11.11	16	2/4	8/128	8	8	16	32
OpenVMS 7.2-2, 7.3, 7.3-1	26	128	128 (10000)	N/A	24	N/A	48
Tru64 UNIX 4.0F, 4.0G	32	4	8	4	N/A	8	N/A
Tru64 UNIX 5.1, 5.1A, 5.1B	64	128	128 (255)	48	24	96	48
IBM AIX 4.3.3, 5.1	8	4/8	32	12	12	24	24
Red Hat Linux 7.2, (Proliant x86) Red Hat Linux 7.1, 7.2 (Alpha)	2	2/4	64	4	N/A	8	N/A
Advanced Server 2.1 (BL20P, BL40P, Proliant x86)	2	2/4	64	4	4	8	16
SuSE Linux 7.2 (ProLiant x86)	2	2/4	64	4	N/A	8	N/A
SuSE SLES 7(ProLiant x86)	2	2/4	64	4	4	8	16
Microsoft Windows 2000 Server, Advanced Server SP2, SP3 Windows 2000 Datacenter	8	2/4	8/64	8	16 (See Figure 36)	16	32 (See Figure 36)
MS Windows Server 2003 Standard Edition and Enterprise Edition (32-bit)	8	3/6	8/64	N/A	16 (See Figure 36)	N/A	32 (See Figure 36)
Microsoft Windows NT 4.0 SP6a	8	2/4	8/64	8	8 (See Figure 35)	16	32 (See Figure 35)
Novell NetWare 5.1, 6, 6.5	4	2/4	32	8	8	16	32
SUN Solaris 2.6, 7 & 8 (32/64 bit)	16	2/4	64	8	8	16	32
Reference Notes	1	2	3, 4, 5, 6	7, 8, 9, 10		7, 9, 10	

Reference Notes

1. The maximum number of HBAs supported per server depends on the specific server model.
2. For Tru64 UNIX and OpenVMS this column typically represents the total number of active controller ports per HBA when accessing all ports of a storage system or ports on multiple storage systems. For most other platforms this column typically represents 2 ports per storage system, or a total of 4 ports across 2 storage systems. Windows 2003 is supported for access to 6 ports across 3 storage systems. Use of zoning may be required to limit the number of active targets (controller ports) presented to each HBA to the maximums stated for each platform in this column. A minimum of OpenVMS 7.2-2 is required for the indicated maximum.
3. Numbers in this column are reduced by one if the command console LUN is enabled.
4. Microsoft Windows NT supports 8 LUNs per HBA target with Large LUN feature disabled and 64 LUNs per HBA target with Large LUN feature enabled. Windows 2000 supports Large LUN by default (LUNs 0 - 199), Secure Path for Windows supports usage of LUNs 0 - 63.

5. For Tru64 5.1, 5.1A, 5.1B, the operating system maximum is 255 LUNs per target. For OpenVMS, the operating system maximum is 10000 LUNs. The single storage system maximum is 128 LUNs.
6. For HP-UX, 128 LUNs per HBA target when the connection operating system type is set to HP_VSA.
7. Use of a Storage Management Appliance requires 2 connection table entries per fabric. However, these connection table entries do not affect the total number of servers or HBAs supported as long as there are available entries in the table. For example, under Windows, the maximum number of servers supported is 16 whether using a Storage Management Appliance or not. Since the Storage Management Appliance executes management commands through its Fibre Channel connection, it is not counted when determining the total number of servers allowed on a single storage system from an I/O load perspective.
8. The maximum number of HBAs that can be configured for access to an active controller port. Assumes 1 HBA per server for single path using controller transparent failover or 2 HBAs per server for multi-path using controller multiple-bus failover. For transparent failover, the limit is specified by controller port pair–1 active and 1 standby controller port. For multiple-bus failover, the limit is specified per single active port.
9. The maximums specified for each platform are the result of one or more of following limiting conditions:
   - A qualification limit
   - Command flow queuing characteristics of specific HBA drivers
   - Connection table size in the array controller software in conjunction with the number of HBA to controller port paths.

   For maximum server or HBA connectivity using controller transparent failover, limit the number of active HBA to controller port paths to one per server (Figure 34.) The use of zoning is required to limit the number HBAs visible to each active controller port.

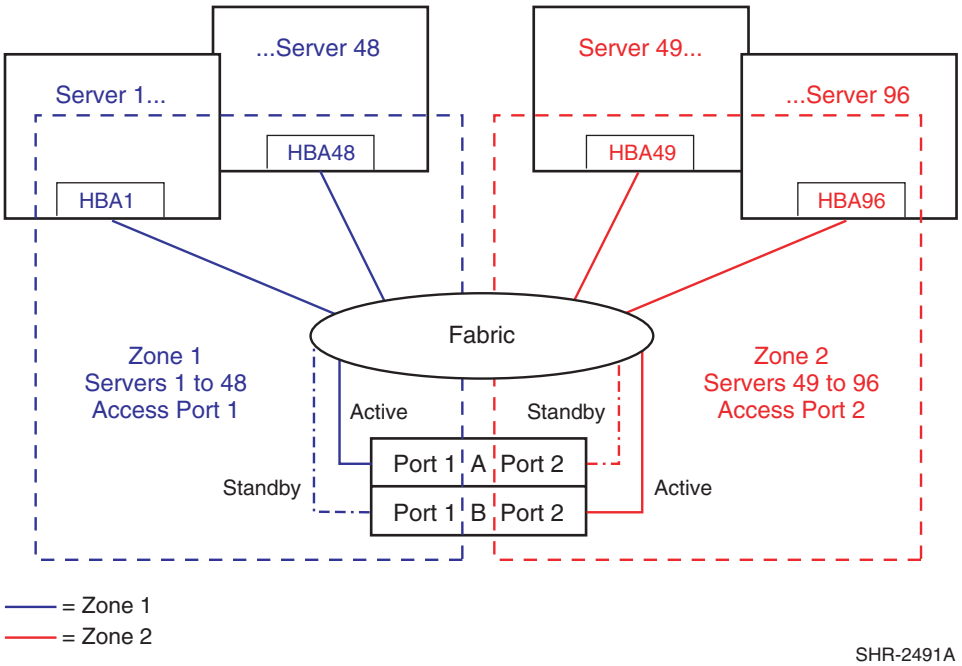


Figure 34: Maximum server example for Tru64 UNIX 5.x with transparent failover using 96 connections and one path per server

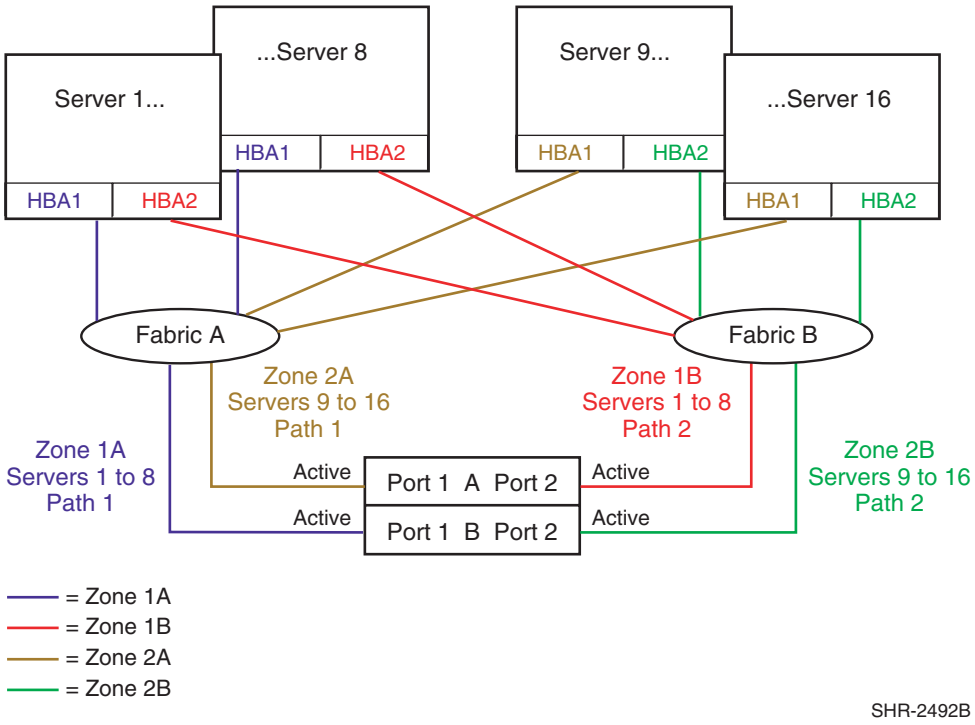


Figure 35: Maximum server example for Windows NT using 16 servers with multiple-bus failover and two paths per server

---

Note: Zones for the figure above are visible on-screen or on a color printout.

For maximum server or HBA connectivity on most operating systems, when using controller multiple-bus failover, limit the number of active HBA to controller port paths to two per server (Figure 35) The use of zoning is required to limit the number of HBAs visible to each active controller port.

For OpenVMS, Tru64 UNIX, and Windows 2000, the maximum server or HBA connectivity is available with up to four paths per server in multiple-bus failover mode. The maximum Windows 2000 configuration is shown in Figure 36.

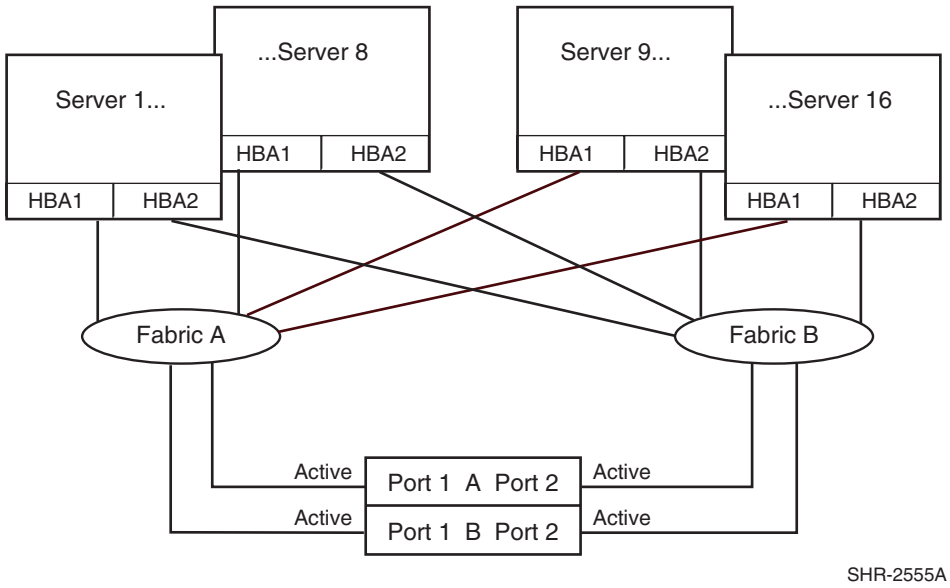


Figure 36: Maximum server example for Windows 2000 using 16 servers with multiple-bus failover and four paths per server

10. In a heterogeneous SAN environment where different platform or operating system types are sharing a single storage system, the maximum number of servers or HBAs supported is equal to the lowest maximum listed in these columns for the operating systems that are sharing the storage system. All platforms or operating systems listed are supported for shared access to the same storage system provided the rules listed in "Heterogeneous SAN Platform Interoperability for EVA5000/EVA3000 and EMA/ESA12000, EMA16000, MA/RA8000, MA6000 Storage Systems" in this chapter are followed. Refer to Table 30 for specific information about sharing a single storage system across multiple platform or operating system types.

Note: Refer to SAN/DRM Integration in this chapter for the maximum number of servers supported for storage systems configured for DRM.

Note: Refer to the SAN/Continuous Access EVA Integration section in this chapter for the maximum number of servers supported for storage systems configured for Continuous Access EVA.

Specific Platform/Operating System Rules – MSA1000, RA4100, RA4000

This section defines the rules and guidelines related to specific platforms/operating systems for MSA1000, RA4100, and RA4000 storage systems. For operating system storage attachment, HBA attachment, current HBA/driver/FW revision support, and specific MSA and RA4x FW version support, contact your HP field representative. Information about the latest MSA1000 support is available at:

http://www.hp.com/go/msa1000

MSA1000 FW 4.24, 2.38 (Intel servers only), B-Series and M-Series Switches

Linux Red Hat AS 2.1 (32-bit) (64-bit single-path only), SLES8 SP2a (32-bit)(64-bit single-path only, SLES 8/United Linux 1.0 32-bit and 64-bit

- Supports LifeKeeper Clusters v4.4
- Supports ServiceGuard v11.15.01

Windows Server 2003 Enterprise Edition (32-bit), 2000 Server and Advanced Server (SP3, SP4), Windows NT 4.0 SP6A, MSCS Clusters, Server 2003 (IA-64), Enterprise Edition (64-bit), Datacenter (64-bit)

- MSCS cluster supported up to 8 nodes

MSA1000 FW 4.24 (Alpha servers only), B-Series and M-Series Switches

OpenVMS 7.3-2, 7.3-1, 7.3, 7.2-2

- 7.3-1 requires DEC-AXPVMS-V731_FIBRE_SCSI-V0400
- 7.3 requires DEC-AXPVMS-V73_FIBRE_SCSI-V0500
- 7.2-2 requires DEC-AXPVMS-V22_FIBRE_SCSI-V0400
- OpenVMS Clusters versions 7.3-1, 7.3, and 7.2-2 are supported
- OpenVMS requires a dedicated MSA1000

Tru64 UNIX 5.1A, 5.1B

- 5.1A requires Patch Kit 4 and New Hardware Delivery kit 6 (NHD6)
- 5.1B requires Patch Kit 1
- TruClusters versions 5.1A and 5.1B are supported
- Tru64 UNIX requires a dedicated MSA1000

Novell NetWare 5.1, 6.0, 6.5

- Novell NetWare Clusters versions 1.01, 1.6, 1.7 are supported

---

Note: For specific Secure path and Erratta support please refer to the Compatibility guide http://www.hp.com/go/MSA

MSA1000 FW 4.24, C-Series Switches

Linux Red Hat AS 2.1 (32-bit) (64-bit), SuSE8 (32-bit), LifeKeeper Clusters v4.2, Red Hat AS 2.1 (64-bit, single-path only), SuSE8 (64-bit, single-path only)

- No boot support

Windows server 2003 Enterprise Edition (32-bit, 64-bit), 2000 Server and Advanced Server (SP3, SP4), Windows NT 4.0 SP6A

Supported HBAs:

- FCA2101
- FCA2214 and FCA2214DC
- AB232A (64-bit only)

OpenVMS 7.3-2, 7.3-1, 7.3, 7.2-2

- 7.3-1 requires DEC-AXPVMS-V731_FIBRE_SCSI-V0400
- 7.3 requires DEC-AXPVMS-V73_FIBRE_SCSI-V0500
- 7.2-2 requires DEC-AXPVMS-V22_FIBRE_SCSI-V0400
- OpenVMS requires a dedicated MSA1000
- Boot is not supported.

Supported HBAs:

- DS-KGPSA-CA
- DS-KGPSA-DA

Tru64 UNIX 5.1A, 5.1B

- 5.1A requires Patch Kit 4 and New Hardware Delivery kit 6 (NHD6)
- 5.1B requires Patch Kit 1
- Tru64 UNIX requires a dedicated MSA1000
- Boot is not supported.

Supported HBAs:

- DS-KGPSA-CA
- DS-KGPSA-DA

Heterogeneous SAN Platform Interoperability for MSA1000 Storage

This section specifies the rules for shared heterogeneous access to a single MSA1000 storage system. MSA1000 storage systems are supported for shared access with combinations of operating systems.

Single MSA1000 shared heterogeneous access:

Any mix of:

- Windows 2003 Enterprise Edition
- Windows 2000 SP3/SP4
- Windows NT 4.0 SP6a
- Novell NetWare 5.1, 6, 6.5
- Red Hat Linux 7.2 (2.38), Advanced Server 2.1
- SuSE SLES 7 single path
- SLES 8/United Linux 1.0 32-bit and 64-bit (2.38)
  SuSE is Homogeneous when operating in a Secure Path environment.

Additionally, standalone servers and clustered servers are supported on the same MSA1000.

Homogeneous SAN Platform Support for MSA1000 Storage

MSA1000 supports homogeneous access with the following operating systems:

- Tru64 UNIX 5.1A, 5.1B
- OpenVMS 7.3-2, 7.3-1, 7.3, 7.2-2

Each operating system requires a dedicated MSA1000.

Additional rules:

- For Tru64 UNIX supports standalone servers or up to a four node cluster
- For OpenVMS supports standalone servers or up to an eight node cluster

MSA1000 Configuration Rules

- The MSA1000 storage systems are supported in all all SAN fabric topology configurations described in this guide and can be configured in a SAN directly using the switch models shown in Table 17, Table 18, and Table 20, unless otherwise specified. The section Specific Platform/Operating System Rules – MSA1000, RA4100, RA4000 lists the platforms and operating systems that are supported using these storage systems.
- MSA1000 storage systems with the MSA SAN Switch 2/8 are supported with B-Series product line switches only.
- MSA1000 storage systems are supported with B-Series, C-Series, and M-Series product line switches.
- For standalone server and cluster maximums per MSA1000, refer to the *MSA1000 Compatibility Guide* available at:

  http://www.hp.com/go/msa1000
- Multi-pathing with Linux, Novell NetWare, and Microsoft Windows is supported
- The attachment of non-Secure Path (single HBA) servers to an MSA1000 with dual controllers having servers with Secure Path (dual HBA) attached is supported where the operating systems are Microsoft or Novell. Users must realize that in the event of a controller fail-over, (failure of active controller) the single path servers will lose access to their data on the MSA1000.

Note: If Secure Path for Linux is used on any node or cluster attached to an MSA1000, all nodes must also have Secure Path installed, regardless of operating systems. Refer to http://www.hp.com/go/securepath for the latest Secure Path parameters.

- Use ACU to enable/disable LUN access to specific connections
- Servers accessing MSA1000 storage systems must not have access to EVA5000/EVA3000, HP XP or VA, EMA/ESA12000, EMA16000, MA/RA8000, MA6000, RA4100 or RA4000 storage systems. Zoning is required to prevent access from servers to multiple storage system types when configuring these storage systems in the same physical SAN.

  As an exception to this rule, certain storage solutions utilizing multiple storage types, for example, disk and tape, may specify support for common server access. In those cases, refer to the specific storage solution documentation for the supported common access configurations and rules.

MSA1000 Maximums

The following table lists the maximum configurations for MSA1000 systems.

Table 34: MSA1000 Maximum Configurations

Platform or Operating System	Host Bus Adapters per Server	Active Controller Ports (Targets) per HBA	LUNs per HBA Target	Port Maximums HBAs per Active Controller Port
Microsoft Windows Server 2003 (32/64-bit), Windows 2000 Server SP3/SP4, Advanced Server SP2 MS Windows Server 2003 Standard Edition and Enterprise Edition (32-bit) Windows NT 4.0 SP6a Red Hat Professional v7.2, Advanced Server 2.1, SuSE SLES 7, SLES 8/United Linux 1.0 Novell NetWare 5.1, 6, 6.5 Clusters 1.01, 1.06	2	8	32	32
Tru64 UNIX 5.1A, 5.1B OpenVMS 7.3-2, 7.3-1, 7.3, 7.2-2	Server Dependent			

Heterogeneous SAN Platform Interoperability for RA4100/RA4000 Storage Systems

This section specifies the rules for shared access to a single RA4100 or RA4000 storage system. RA4100/4000 storage systems are supported for shared access with any combination of the following operating systems:

- Linux Red Hat 7.0, 7.1
- Linux SuSE 7.1
- Microsoft Windows 2000 Server, Advanced Server SP1
- Microsoft Windows NT 4.0, SP5, SP6a
- Novell NetWare 5.1

- RA4100/RA4000 systems can not be shared by more than one cluster when using Microsoft Windows NT 4.0 or Microsoft Windows 2000
- RA4100/RA4000 systems owned by a Microsoft Windows NT or Microsoft Windows 2000 cluster can not be shared with a standalone server or server

RA4100 and RA4000 Configuration Rules

- These storage systems can be configured in a SAN directly using the switch models shown in Table 17, and through the Compaq FC-AL Switch 8 cascaded to the other switch models listed. The section Specific Platform/Operating System Rules – MSA1000, RA4100, RA4000 lists the platforms and operating systems that are supported using these storage systems.
- Supports all fabric rules for SAN fabrics using the Fibre Channel switches listed in Table 17

- The Compaq FC-AL Switch 8 is supported for cascaded attachment to the SAN through a single FL-Port on B-Series switches only.
- Use single or redundant controllers with Active/Passive controllers.
- Use ACU to enable/disable LUN access to specific connections.
- For RA4100/RA4000 SAN configurations with *heavy I/O traffic*, it is necessary to increase the fabric switch buffer capacity from the default value of 16 to 27.
- Servers accessing RA4100 or RA4000 storage systems must not have access to EVA5000/EVA3000, HP XP or VA, EMA/ESA12000, EMA16000, MA/RA8000, MA6000, or MSA1000 storage systems. Zoning is required to prevent access from servers to multiple storage system types when configuring these storage systems in the same physical SAN.
- Zoning is required with multiple clusters. Each cluster must be in its own zone.

RA4100 and RA4000 Maximums

The following table lists the maximum configurations for RA4100/RA4000 storage systems.

Table 35: RA4100 and RA4000 Maximum Configurations

Platform or Operating System	Host Bus Adapters per Server	Active Controller Ports (Targets) per HBA	LUNs per HBA Target	Port Maximums HBAs per Active Controller Port
Red Hat Linux 7.0, 7.1 Suse Linux 7.1	1	1	32	32
Microsoft Windows 2000 Server, Advanced Server SP2 Windows NT 4.0 SP6a	2	1	32	32
Novell NetWare 5.1	2	1	32	32

SAN/Continuous Access EVA Integration

The HP Storageworks Continuous Access EVA solution is is approved for use within a larger Heterogeneous Open SAN provided the following additional rules are followed: All Continuous Access EVA implementations require Level 4 NSPOF SANs using two separate fabrics. Refer to Chapter 2, "Data Availability in a SAN." For additional information see the Continuous Access EVA Design Reference Guide which is available on the Web at:

http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html

The current Continuous Access solution supports a sub-set of those operating systems listed in this guide which limits the type of servers that may reside within the Continuous Access EVA management zone.

1. Shared usage of Continuous Access EVA configured storage systems by non-Continuous Access EVA configured servers

   (e.g., single HBA or an OS without multi-path support) or non-Continuous Access EVA supported operating systems is not supported.

Table 36: Heterogeneous Continuous Access EVA Operating Systems

Operating System	Version
HP-UX	V11.0 ■ HP MC/Serviceguard Clusters V11.14 and up to 8 nodes V11.11 ■ HP MC/Serviceguard Clusters either SG V11.14 or 11.15 and up to 8 nodes V11.23 ■ HP MC/Serviceguard Clusters V11.15 and up to 8 nodes V11.0, 11.11, and 11.23 ■ Cluster Object Manager VA.01.01. ■ HP StorageWorks Secure Path for HP-UX V3.0A
HP OpenVMS	V7.2-2 and 7.3-1 ■ VMSClusters appropriate to OS version
HP Tru64 UNIX	V5.1, V5.1a, and V5.1b ■ TruClusters appropriate to OS version
IBM AIX	V4.3.3, V5.1,and V5.2, HACMP appropriate to OS version
Microsoft Windows 2000 Server, Windows 2000 Advanced Server Windows 2003 32 and 64 bit	Windows 2000 (V5), Windows 2003 (V6) ■ (Windows 2000) Service Pack 3, Service Pack 4 ■ Microsoft Cluster Server (MSCS) ■ HP StorageWorks Secure Path for Windows V4.0 required (The exact version of Secure Path depends on the driver, HBA, and OS.)
Microsoft Windows NT Server	V4.0 ■ Service Pack 6a ■ Microsoft Cluster Server (MSCS) ■ HP StorageWorks Secure Path for Windows V4.0 required
Novell NetWare	V5.1Service Pack 6, V6 Service Pack 3, V6.5 V6 supports a max of 6 nodes, V6.5 supports up to 12 nodes clusters
Red Hat Linux	Advanced Server V2.1
Sun Solaris	V2.6, V7, V8, and V9 ■ HP StorageWorks Secure Path for Sun V3.0A SP1 or V3.0B required ■ VERITAS Clusters V2, 3.5, or Sun Clusters 2.2, all with maximum of 16 nodes
SuSE Linux	SLES 7, SLES 8, United Linux 1.0

2. Each Continuous Access EVA solution may contain up to 16 EVAs, where each EVA is limited to at most 256 HBAs which at 2 HBA per server, equates to 128 servers. Multiple Continuous Access EVA solutions may exist within the same SAN as long as no one solution exceeds the 16 array limit, and that limit is imposed by zoning. Any SAN running Continuous Access EVA may contain up to 28 switches and 7 hops between devices connected to B-Series switches, up to 11 switches and 3 hops with C-Series switches, or up to 24 switches and 3 hops with M-Series switches with the understanding that there are three links involved. There is the host to local storage link, the local storage to remote storage link, and the local host to remote storage link. Each of these links must not exceed 7 or 3 hops, depending on the switch family. All active/standby host-to-storage links as well as local-to-remote storage links must conform to the 7/3/3-hop limit.
3. A single array may support up to 128 DR Groups, and up to 128 Copy Sets. A single DR Group supports at least one and not more than eight copy sets.
4. The Continuous Access EVA Link supports mixed heterogeneous SAN, DRM, Continuous Access EVA, and Host Based Shadowing traffic.
5. Two Storage Management Appliance (sma) Command View element mangers are required, one active and one either active in stand by mode or in powered off passive mode. The active appliance and Command View EVA can be used for initial setup of Continuous Access EVA storage. Management of the operational Continuous Access EVA environment is done through the Continuous Access user interface, and separate product also installed on the storage management appliances. See the Continuous Access EVA Design Reference Guide and Continuous Access EVA Operations Guide for additional information.
6. Please see the Continuous Access EVA release notes for current information about the solution. The release notes are available at this URL:
http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html

SAN/DRM Integration

The HP Data Replication Manager for HSG80 (DRM) is approved for use within a larger Heterogeneous Open SAN provided the following additional rules are followed: All DRM implementations require Level 4 NSPOF SANs using two separate fabrics. Refer to Chapter 2, "Data Availability in a SAN". Several special purpose DRM configurations are also supported as defined in the DRM for HSG80 Design Guide which is available on the Web at:

DRM Technical Documentation
http://h18000.www1.hp.com/products/sanworks/drm/documentation.html

Each shared storage array must adhere to the DRM sharing rules as defined in the *DRM Design Guide*. These sharing rules may be more restrictive than those in this guide due to the requirements for DRM, for example, the operating system must support multiple-bus failover. In addition, the current DRM solution supports a sub-set of those operating systems listed in this guide.

1. Shared usage of the DRM configured storage systems by non-DRM configured servers (e.g., running in transparent failover) or non-DRM supported operating systems is not supported.
2. All servers sharing the same storage sub-system must share a compatible SCSI command mode as shown by a yes in the following table:

Table 37: Heterogeneous DRM Operating Systems

Operating System	Versions	SCSI-2	SCSI-3
HP OpenVMS	7.2-2, 7.3, 7.3-1	No	Yes
HP Tru64 UNIX	5.1, 5.1A, 5.1B	Yes	Yes
HP-UX	11.0, 11.11	Yes	Yes
IBM AIX	4.3.3, 5.1	Yes	Yes
Microsoft Windows NT	4.0	Yes	Yes
Microsoft Windows 2000 Server, Advanced Server	Server, Advanced Server, Datacenter	Yes	Yes
Novell NetWare	5.1, 6	Yes	Yes
Sun Solaris	2.6, 7, 8, 9	Yes	Yes
Red Hat LINUX Advanced Server	2.1		Yes
SuSE LINUX: SLES 8	8		Yes
SuSE LINUX: United Linux V1.0	1.0		

3. Each DRM solution instance may contain up to 96 servers and 8 storage arrays. With large fabrics, multiple solution instances may exist, as long as each is in a separate zone on a SAN or a separate zone within a VSAN (as recommended in C-Series). In other cases the actual limit will be smaller due to restrictions imposed by the intersite link. DRM supports the limit of up to 7 hops between devices connected to B-Series switches, 3 hops with C-Series switches, and 3 hops with M-Series switches with the understanding that there are three links involved. There is the host to local storage link, the local storage to remote storage link, and the local host to remote storage link. Each of these links must not exceed 7 or 3 hops, depending on the device. All active/standby host-to-storage links as well as local-to-remote storage links must conform to the 7/3-hop limit.
4. Each DRM solution instance may contain up to 12 servers per storage system per site provided both controllers of the storage system are using the “P” version of ACS configured in remote peer-to-peer replication mode. With 1 remote copy set per server, a maximum of 12 remote copy sets per pair of storage systems, and a maximum of 8 storage systems per site per instance, a single DRM instance can support up to 96 servers per site. If you increase the number of remote copy sets per server, you must reduce the total number of servers per storage system. For example, if you configure 2 remote copy sets per server, the maximum limit is 6 servers per storage system.
5. DRM over ATM configurations are supported for switches in Table 17 with switch FW 2.1.9m only, with a limit of two Fibre Channel switches per fabric, for a total of 4 switches, one at each end of each fabric (2 fabrics, times 2 switches per fabric equals 4 switches). Cascaded switches are not supported. This no-cascaded switch restriction also includes non-support for the SAN Switch Integrated/32 or SAN Switch Integrated/64 port switches due to the fact that these switch models are made up internally of 6, 16-port switches that are cascaded together.
6. The DRM Link supports mixed heterogeneous SAN, DRM, and Host Based Shadowing traffic.
7. StorageWorks Command Console (SWCC) and the Storage Management Appliance (SMA) element manger can be used for initial setup of Data Replication Manager (DRM) storage sub-systems. However, neither of these tools should be used for DRM failover and failback operations. Therefore to prevent any potential inference by MA polling of the HSG80 when running DRM scripts, it is recommended that the MA be removed from all DRM zones before running the scripts.

8. Please see the DRM release notes for current information on any hop count restrictions between devices.

SAN/DRM/OpenVMS Host Based Volume Shadowing Integration

OpenVMS servers implementing Host Based Volume Shadowing are supported integrated in a heterogeneous SAN with remote shadowset distances of up to 160 km over 1 Gbps direct fiber. The direct fiber long distance link supports mixed heterogeneous SAN, DRM, Continuous Access EVA, and OpenVMS Host Based Volume Shadowing traffic.

StorageWorks CSS 2105 Storage System Interoperability and Integration

HP provides support for heterogeneous multi-vendor online storage interoperability on a common SAN. This support includes both the StorageWorks Centralized Shared Storage 2105 (CSS 2105) and the StorageWorks Enterprise RAID Array.

The initial integration support represents the first phase or level of interoperability. This level of support provides for:

1. Coexistence of HP and IBM storage systems in a common heterogeneous Open SAN. The HP and IBM storage systems operate in separate fabric zones within the same physical SAN.
2. Data migration support between HP and IBM storage systems using a shared server running either Windows 2000/NT, IBM AIX, or Sun Solaris.
3. Multi-path failover capabilities using HP Secure Path for the HP storage and the IBM Subsystem Device Driver on a single shared server running Windows NT, IBM AIX, or Sun Solaris. Each storage system is connected to the server using independent HBA pairs.
4. Simultaneous enterprise backup support from both the HP storage and IBM storage utilizing a single shared server and the HP Enterprise Backup Solution with VERITAS NetBackup to a common tape library for Windows 2000/NT.

Refer to the Technical Note "Compaq StorageWorks Centralized Shared Storage 2105 Interoperability" for additional information. Future phases will provide additional levels of interoperability over time.

High Availability Configuration Considerations

Cabling Scheme Options

This section describes cabling scheme options for implementing high availability multi-path configurations for EVA5000/EVA3000, MA6000, MA/RA8000, EMA/ESA12000, and EMA16000 storage systems. Figure 37 and Figure 38 show cabling options when implementing a Level 4 high availability no single point of failure configuration. Figure 39 and Figure 40 show the cabling and associated zoning requirements when implementing a Level 3 high availability configuration. Refer to Chapter 2, "Levels of Availability" for a description of the availability levels.

Note: DRM requires the high availability NSPOF configuration. DRM cabling is fully described in the DRM Design Guide, available at:

http://h18000.www1.hp.com/products/sanworks/drm/documentation.html

---

Note: Continuous Access EVA cabling is supported as shown in Figure 37 and Figure 44. The cabling is also described in the Continuous Access EVA Design Reference Guide. See URL:
http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html

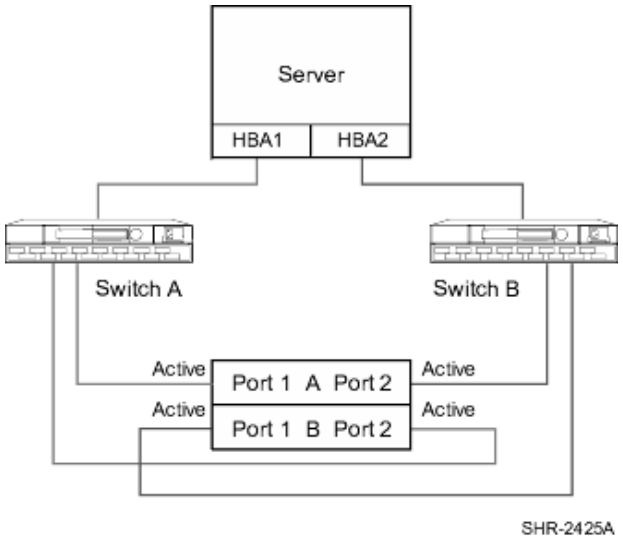


Figure 37: Cross-Cable High Availability NSPOF Configuration

Figure 37 shows the physical connections for a cross cable, high availability, no single-point of failure configuration for storage systems using two separate fabrics.

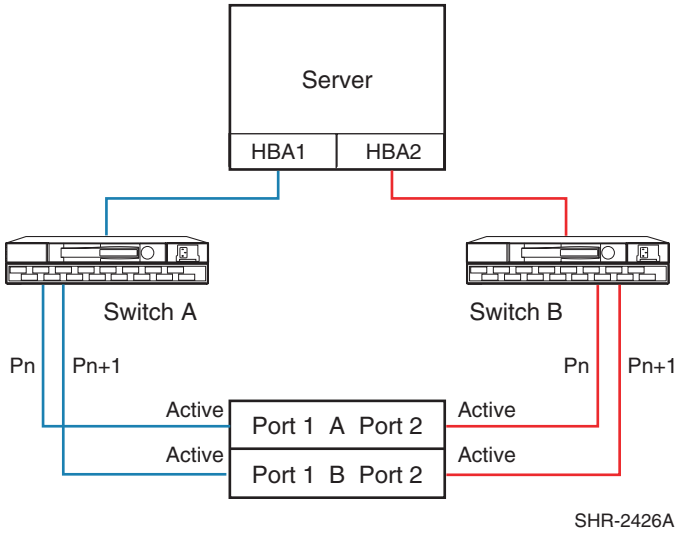


Figure 38: Straight-Cable High Availability NSPOF Configuration

Figure 38 shows the physical connections for a straight cable, high availability, no single point-of-failure configuration. The advantage of this cabling scheme is that it is the same cabling scheme used in Transparent failover mode for MA6000, MA/RA8000,

EMA/ESA12000, and EMA16000 storage systems. This allows you to migrate from Transparent failover mode to Multiple-Bus failover mode without the need to re-cable the controller connections.

Figure 39 and Figure 40 below specify the logical path zoning that may be required for cross cable and straight cable configurations when implementing a level 3 single fabric high availability configuration. The requirement to zone separate logical paths in single fabric high availability implementations is O/S and platform specific. The zoning specified enforces and effectively results in the same configuration as physically depicted in Figure 37 and Figure 38. Single fabric cross cable implementations require cross port zoning, straight cable implementations require straight port zoning. In order to provide high availability, ensure each HBA is cabled to a different switch and configured for access to specific controller ports.

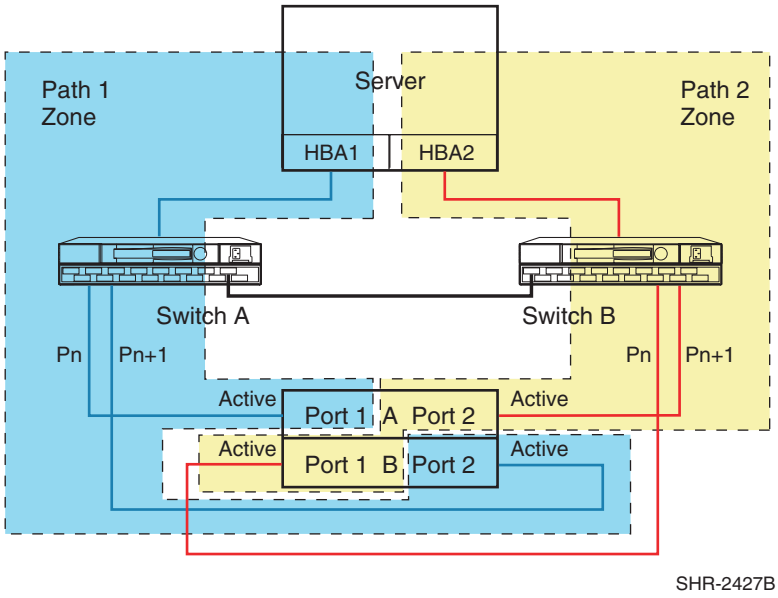


Figure 39: Cross-Cable High Availability Single Fabric Zoned Configuration

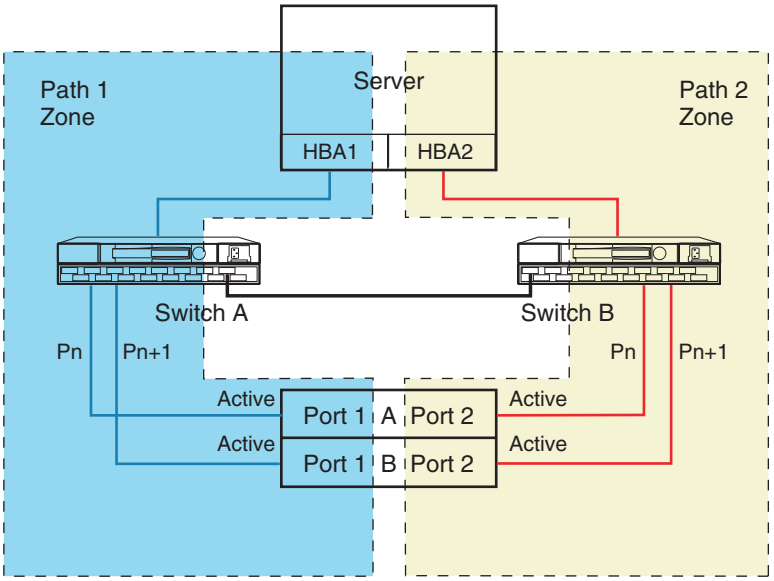


Figure 40: Straight-Cable High Availability Single Fabric Zoned Configuration

For two or more high availability server configurations, it is suggested that the first adapter in each server be connected to the first (same) Fibre Channel switch, the second two adapters to the second switch, etc. For example:

- Server 1 Fibre Channel HBA 1 to Fibre Channel Switch 1 - Switch Port 1
- Server 1 Fibre Channel HBA 2 to Fibre Channel Switch 2 - Switch Port 1
- Server 2 Fibre Channel HBA 1 to Fibre Channel Switch 1 - Switch Port 2
- Server 2 Fibre Channel HBA 2 to Fibre Channel Switch 2 - Switch Port 2

It is highly recommended that the cabling scheme shown in each Secure Path multiple-bus configuration be followed as depicted. This is not required; however, it does aid in understanding logical to physical LUN and path mapping for maintenance purposes.

Cabling Scheme Options for Dual Channel HBAs

Dual channel HBAs are typically utilized in situations where the number of server PCI slots is limited. As such, most installations are configured as shown in either Figure 41 or Figure 42. Both configurations are implemented using a single PCI slot to provide access to either the same Targets/LUNs or a different set of storage Targets/LUNs through separate ports on the HBA.

Note: Each dual channel HBA is theoretically capable of twice the performance of a single channel HBA for a given single PCI slot.

Note: Target ranges are shown for example purposes; the number of storage controller Targets and LUNs associated with each Target accessible is operating system dependent.

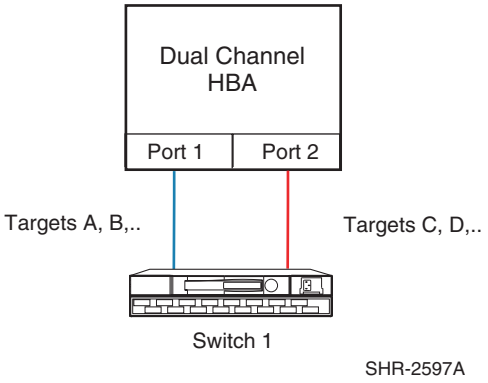


Figure 41: Single PCI Slot with Dual Channel HBA and One Switch

Figure 41 provides connectivity with both HBA paths connected to the same Fibre Channel switch.

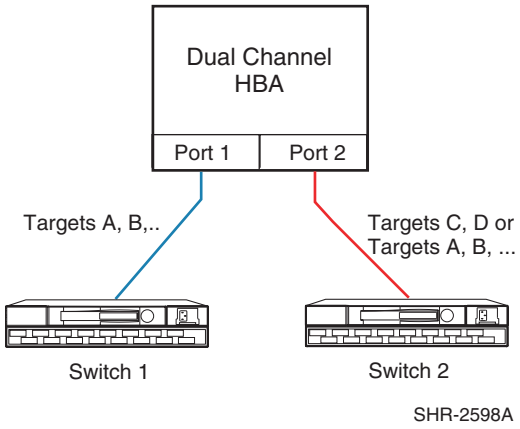


Figure 42: Single PCI Slot with Dual Channel HBA and Two Switches

Figure 42 provides increased availability over Figure 41 in the event of a single switch failure. Availability to a specific set of Targets/ LUNs can be further increased by configuring access to the Targets (A, B..) on both paths as shown.

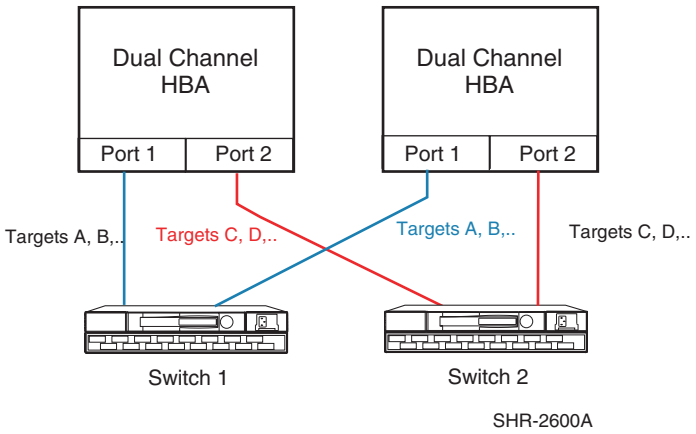


Figure 43: Two PCI Slots with Dual Channel HBAs - NSPOF

Figure 43 shows an example of how a no single point of failure solution can be implemented with two dual channel HBAs. From an availability standpoint, this equates to the use of two single channel HBAs. Refer to Chapter 2, "Levels of Availability" for further information.

Enterprise Backup Solution

5

The first step in implementing an EBS solution is to consult the *EBS Compatibility Matrix* available at:

http://h18000.www1.hp.com/products/storageworks/tapecompatibility.html

The HP StorageWorks Enterprise Backup Solutions Design Guide is the second step in implementing your Enterprise Backup Solution. This guide describes the EBS hardware configurations currently supported and how to efficiently and effectively provide shared tape library backup in a heterogeneous SAN environment.

http://h18004.www1.hp.com/products/storageworks/ebs/documentation.html

The third step in implementing your Enterprise Backup Solution is installing and configuring your backup application or backup software. Rules and recommendations for individual backup applications and software may be found in separate implementation guides.

For more information about EBS, refer to:

http://www.hp.com/go/ebs

SAN Management

6

With the advent of Storage Area Networks (SANs) and Fibre Channel technology, HP is rapidly transitioning from the traditional server, storage, and component level-based management to a SAN-level application architecture and implementation using the Storage Management Appliance (SMA.)

Just as important as the quality and feature set of the SAN's hardware is the effectiveness of the SAN management applications in tying these devices together and simplifying the complexity of the storage network. Whether using an HP standard topology, or a custom design using the StorageWorks SAN design rules, IT managers need to configure, monitor, and maintain the SAN, as well as plan for, and accommodate, growth.

The HP Open SAN management strategy is to:

- Simplify storage management using standardized web-based graphical user interfaces (GUIs) residing on easy-to-use, easy-to-implement storage management appliances.
- Centralize the management of multi-vendor Heterogeneous Open SANs in distributed and consolidated environments.
- Automate policy-based management.
- Optimize functionality by exploiting all currently available management levels such as appliances, SAN fabrics, and servers/storage.

Key to the StorageWorks SAN management strategy is the use of the Storage Management Appliance. HP SANs can be designed for local, centralized, or distributed data access. Regardless of the arrangement or location of the storage components and preferred data access method, storage environment management can be centralized using a Storage Management Appliance.

The Storage Management Appliance connects directly to the storage network through a Fibre Channel switch providing full access to all supported devices in the storage environment. Strategically located out of the SAN data path, the appliance allows data transfers to proceed independently between computers and storage devices. The appliance optimizes SAN availability and performance while streamlining manageability.

Note: For more information about using an Storage Management Appliance SAN, see Chapter 3, "Storage Management Appliance Rules and Recommendations".

Storage Management Appliance Features / Functionality

- Simple, unintrusive management of SAN elements
- High SAN performance since the appliance is located out of the data path
- High SAN availability, since data transfers occur independent of the appliance
- Support for multiple management and monitoring applications
- A web-based, centralized user interface
- No console operations for increased SAN management security
- Support for heterogeneous platforms attached to the SAN
- Higher utilization for processing applications on host servers
- Rack mountable, ease of installation and administration

OpenView Storage Management Appliance Software

HP OpenView Storage Management Appliance software is included with and resides on the Storage Management Appliance, giving you access to the storage management appliance functions. Logging into Storage Management Appliance software anywhere over the web provides a single aggregation point to launch a variety of HP's SAN management applications to monitor and manage your storage network.

Zoning the HP Storage Management Appliance in a Heterogeneous Server Environment

Whenever a storage management appliance is placed in a fabric with heterogeneous servers it is recommended that a dedicated storage management zone be created. This zone is specifically for the storage management appliance and the elements it is to monitor and manage.

For example, create a zone called SANAPP_1_ZONE that would contain the appliance host bus adapter port WWN and the port WWNs of all the HSG or HSV controllers managed by this Storage Management Appliance. Because fabric devices can be in multiple zones, this will have no effect on other zones containing the same HSG and HSV controller port WWNs.

Currently, the storage management appliance communicates with HSG or HSV controllers in-band, within the Fibre Channel fabric itself. It is not necessary or recommended to include either the switch WWNs or server HBA port WWNs in this zone. Communications to these devices are done out-of-band; outside the fabric via TCP/IP.

hp OpenView Storage Area Manager Overview

HP OpenView Storage Area Manager is comprised of a comprehensive software portfolio that simplifies and automates the management of storage resources and infrastructure. It manages tape and disk, and direct and network-attached storage, across multivendor devices and distributed environments. From its central management console, IT storage administrators effectively monitor storage and storage service availability, performance, usage, cost and growth, while optimizing resources and cost.

HP OpenView Storage Area Manager also enables users to define, monitor and measure storage service levels, helping to guarantee quality of service and increasing the value of storage investments. IT management can determine and set enterprise-wide device, capacity and performance management, usage metering, storage allocation and access control.

The Storage Area Manager product suite includes the following applications:

- Storage Node Manager, for device management
- Storage Accountant, for usage metering and billing
- Storage Allocater, for storage provisioning and access control
- Storage Builder, for capacity management
- Storage Optimizer, for performance management

You can install all applications from the Storage Area Manager CD-ROM; however, you must purchase and enter operational licenses for each application in order to use them after initial evaluation period.

The software suite's building block architecture allows each of its five software tools to operate and be available separately, so users can add functionality when needed and budgeted. Each tool focuses on a particular aspect of storage management, yet is designed to provide a seamlessly integrated view of the storage environment when used in conjunction with the other tools.

Key Benefits:

- Simple, automated operations
- Intuitive, easy-to-use tools and automated wizards drive staff efficiency and shorten learning curve
- Central console and common reporting structure to manage and monitor storage service availability, performance, usage, cost and growth
- Automated identification of wasted or stale or secondary storage frees capacity
- Usage metering and billing recovers cost and enables charge-back
- Logical, online storage provisioning for storage allocation without impacting operations
- Performance monitoring identifies bottlenecks before they impact business operations
- Automated reporting saves time and increases service quality
- Automated host access notification ensures data is safe from network intruders
- Virtualized storage access control provides highest levels of data integrity
- Continuous health status and event monitoring quickly isolates and solves problems
- Multi-vendor device and system support maximizes storage investments, and provides open choice for future storage acquisitions

Storage Area Manager Architecture

The hp OpenView Storage Area Manager hardware and software architecture is comprised of the bridge, management server, managed hosts, management clients, and the Manager of Managers (optional).

Bridge

The bridge is a Web server application that allows other applications access to Storage Area Manager's functionality, and enables Storage Area Manager's integration with other OpenView enterprise applications. The bridge consolidates information from multiple management servers for use by the application integrating with the bridge.

It is automatically installed on the management server when OpenView Storage Area Manager software is installed from the CD.

Management Server

The management server is a server application that hosts the majority of Storage Area Manager's storage management functionality. Its framework includes the Storage Area Manager database, discovery subsystem, event-handling subsystem, configuration files, and server components for each of the five software tools that comprise the product suite.

The management server software is installed from the Storage Area Manager CD on a dedicated Windows 2000 server or workstation. A single management server manages a single storage domain, which consists of storage resources that are visible to the SAN hosts associated with the management server. Storage Area Manager can manage direct-attached, SAN-attached, or network-attached storage resources.

Managed Host

The managed host contains the host agent software, which includes all components that require access to storage resources visible to the hosts. These components include discovery, status and event inquiry, and performance and capacity data collection.

The host agent software can be installed remotely from the management server or locally from the Storage Area Manager CD onto a Windows, HP-UX, Solaris, Linux, AIX, Tru64 UNIX OpenVMS, or NetWare host. Upon successful installation, the host becomes associated with and dedicated to the management server. The host agent runs as a service on Windows hosts and as a daemon on UNIX hosts.

Management Client

The management client is a graphical user interface (GUI) application that uses a common navigation and presentation framework to display the storage information stored by the management server.

The management client software is automatically installed on the management server. It also may be downloaded from the management server to remote client systems running Windows, HP-UX, Solaris, or Linux.

Manager of Managers

The Manager of Managers (MoM) is a graphical user interface (GUI) application that consolidates storage information from multiple storage domains. This allows administrators to view, from a single location, the high-level status and filtered event information of a large or geographically dispersed storage network. They also can launch the management client for one specific storage domain to view the detailed information displayed by the client.

The MoM software can be downloaded from the management server to remote Windows, HP-UX, Solaris, or Linux hosts. It is an optional piece of the Storage Area Manager architecture.

OpenView Enterprise Applications

The Storage Area Manager software suite integrates with various OpenView enterprise applications. Through the bridge, the Storage Area Manager Smart Plug-in (SPI), and the integration packages contained on the Storage Area Manager CD, its information and control can be integrated with:

- hp OpenView Reporter
- hp OpenView Operations for Windows
- hp OpenView Operations for UNIX
- hp OpenView Internet Usage Manager
- hp OpenView Service Navigator
- hp OpenView Service Desk

For more information on the integration of Storage Area Manager with these enterprise applications, refer to the Storage Area Manager documentation.

Hierarchical Multi-Domain Architecture

The Storage Area Manager software suite is designed to support hundreds of managed devices and thousands of LUNs spread across both logical and physical (direct, NAS, SAN) domains in the storage infrastructure.

Its optional Manager-of Managers (MoM) capabilities further ease the management of large distributed environments. It enables administrators to see a complete view of the distributed storage infrastructure, and allows individual administrators access to those infrastructure components for which they are responsible.

SAN Management Categories

SAN management is wide ranging, covering many aspects of the day-to-day activities used for monitoring and managing, as well as simplifying, the complexity of the storage network.

This section classifies SAN management into four major categories:

- Fabric management
- Storage management
- Data management
- SAN usage and monitoring

SAN Fabric Management

SAN fabric management can be thought of as the control of the SAN infrastructure or "traffic flow" within the SAN. This pertains to control and management of device communication or access within the SAN, such as switch zoning, or LUN level Selective Storage Presentation (SSP). This also includes managing SAN interconnect components, individually and collectively, throughout the fabric.

SAN Storage Management

Storage management allows control of the specific storage system configuration such as redundant paths, creation and management of storagesets (LUNS), setting of RAID levels, and the setting of platform specific SAN interface characteristics and parameters.

SAN Data Management

SAN data management applications help ensure that data is available and accessible. The data being stored on the SAN is part of a company's assets. It is imperative to keep this data available to system applications with minimal, if any, downtime. Techniques such as cloning, snapshots, data replication, and backups protect the data from disasters.

SAN/Storage Usage & Monitoring

SAN and storage usage and monitoring applications are necessary to provide SAN event notification and fault/failure information for service before SAN anomalies can adversely impact the enterprise. They may also provide reporting and billing information for determining the amount of storage and quality of service delivered.

SAN Management Application Deployment

Within the different categories of management tools, individual tools are implemented either on the storage management appliance, within fabric interconnect components, or within servers/storage systems. Table 38 lists the management tools by category, and identifies where the specific tools reside.

Note: Some applications may reside in more than one category.

Table 38: SAN Management Tools & Location

SAN Management Application	Appliance Based	Fabric Based	Server Based	Storage Based
SAN Fabric Management				
hp SANworks Network View	Yes	No	No	No
hp OpenView Storage Node Manager	No[1]	No	Yes	No
StorageWorks Fabric Watch	No	Yes	No	No
SAN/Fibre Channel Switch Management	No	Yes	No	No
HP StorageWorks Fabric Manager	No	Yes	Yes	No
HP StorageWorks HA-Fabric Manager	No	Yes	Yes	No
SAN Storage Management				
Storage Management Appliance Element Manager for HSG	Yes	No	No	No
Command View EVA	Yes	No	No	No
hp SANworks Network View	Yes	No	No	No
OpenView Storage Node Manager	No[1]	No	Yes	No
OpenView Storage Allocater	No[1]	No	Yes	No
StorageWorks Command Console	No	No	Yes	No
Storage System Array Controller Software (ACS) Command Line Interface (CLI)	No	No	No	Yes
Storage System Scripting Utility (SSSU)	No	No	Yes	No[2]
RA4000/4100 Array Configuration Utility (ACU)	No	No	Yes	Yes
MSA1000 (ACU, ACU-XE, ACU-XE(Offline)	No	No	Yes	Yes
Secure Path Manager	Yes	No	Yes	No
Storage Provisioner	Yes	No	No	No
SAN Data Management				
StorageWorks Business Copy (BC)	Yes[3]	No	Yes	No
OpenView Storage Virtual Replicator	No	No	Yes	No
StorageWorks Data Replication Manager (DRM)	Yes	No	No	Yes[4]
StorageWorks Command Scripter	No	No	Yes	No[5]

Table 38: SAN Management Tools & Location (Continued)

SAN Management Application	Appliance Based	Fabric Based	Server Based	Storage Based
Continuous Access EVA user interface[6]	Yes	No	No	No
SAN/Storage Usage & Monitoring				
OpenView Automation Manager	Yes	No	No	No
SANworks Network View	Yes	No	No	No
OpenView Storage Node Manager	No[1]	No	Yes	No
OpenView Storage Builder	No[1]	No	Yes	No
OpenView Storage Accountant	No[1]	No	Yes	No
OpenView Storage Optimizer	No[1]	No	Yes	No

1.hp OpenView Storage Node Manager, Allocater, Builder, Accountant and Optimizer are supported as options in the SAN Appliance
2.This product is a character cell interface to configure and control an Enterprise Virtual Array
3.BC Version 2 and later
4.DRM requires ACS Version 8.xP Software. It is best managed via a character cell command line interface.
5.This product is a front-end to the Storage System CLI
6.Requires Command View EVA, Continuous Access EVA License, VCS V3

SAN Fabric Management Tools

Storage Management Appliance Network View

HP SANworks Network View is a Storage Management Appliance application providing at-a-glance views of SAN configuration and availability. SAN devices, their Fiber Channel interconnects, and associated status are automatically discovered and represented in an intuitive topographical display. SAN device management is made easy by double clicking on a device icon. A Java based design allows remote SAN management from any web-enabled console having Internet Explorer or Netscape browsing capability. Network View serves as a SAN management consolidation point.

Software Features / Functionality

- Simplified SAN management from one application
- At a glance SAN visualization
- SAN administration from remote locations
- Automated SAN availability monitoring and notification when faults arise
- A consolidation point and launch pad for device specific device and storage management tools
- Fibre link connection mapping for established SANs or for future planning
- Scalable for future SAN growth
- A host independent solution

Storage Management Appliance Network View spans three SAN management categories by providing:

- SAN Fabric Management - Network View can view, monitor and manage FC Switches, Tape Routers as well as Inter Switch Links (ISL) right from the topology map. By either clicking on the device icon or the device folder Network View will automatically launch the device's web GUI.
- SAN Storage Management - HSG elements can also be viewed, monitored and managed from the Network View topology map. By clicking on the element icon or device entry, Network View will call up the respective Element Manager application.
- SAN monitoring - Network View can monitor the condition of the fabric hardware by displaying and reporting the condition of server HBAs, Fabric Interconnects, and HSG elements via E-mail, pager or SNMP traps. Performance can be monitored either in real time or a SAN history may be maintained to playback at anytime.

Network View Setup in a Large SAN

Network View discovers, monitors and manages various FC devices either through in-band or out-of-band communications with that device.

HSG Elements

Network View uses in-band and out-of-band communication to discover the HSG controllers or elements. Network View will automatically populate its database and topology map based on the HSG elements discovered by the appliance. Currently, HSG elements are displayed by the controller serial numbers discovered

It is recommended to change the properties of the HSG Element to a more intuitive name for display and error reporting reasons. Right-click on the element icon or device list to change properties. A suggestion would be: *location-controller type-failover mode- ACS version*

For example: RACK05TOP-G80-T-V8.6F would indicate the element resides in the top of Rack 5, and are HSG80 controllers running in Transparent Failover with ACS code V8.6F.

Fibre Channel Switches/ Fibre Channel Routers

Network View uses out-of-band communication (TCP/IP) to discover Fibre Channel Switches and Fibre Channel Routers. When Network View is launched for the first time a Configuration pop-up window will appear indicating the database is empty. You may then add a range of FC Switch/Router IP addresses for Network View to map and monitor.

You may also at any time add additional IP addresses by clicking on the Configure button on the topology map, adding the new IP addresses then Start discovery.

By default, Network View will display the DNS name of the IP address, if any, or the IP address itself. Right-clicking on the device icon or name will allow you to edit the name within the properties box that is displayed in the topology map.

A suggestion would be: *FCtopology-device-xx*

For example: RING-SWITCH-01 would indicate the first FC switch in the RING topology.

Note: Use at least 2 characters for numbers to keep the display sorted properly.

Server Host Bus Adapters

Network View does not initially discover server HBAs until a Device Manager Agent is installed on the server. During the agent install it will prompt you to input the appliance name running Network View. It is this device manager service that "pushes" the HBA information over TCP/IP to the appliance. Currently, server device managers are available on Window NT, Windows 2000, Sun Solaris, Tru64 UNIX, HP-UX, IBM AIX, OpenVMS, and NetWare.

Network View will display the DNS name of the server in the topology map and it cannot be renamed. However it is suggested to append the HBA name located under the Host name for monitoring and error reporting purposes.

A suggestion would be to prefix the existing entry with: *servername-topology*

For Example: SERVER04-RING-Emulex-LP8000-Port0 would indicate this is SERVER04's RING topology adapter.

For further information, including agent O/S versions, please read the Network View QuickSpec and release notes.

hp OpenView Storage Node Manager

HP OpenView Storage Node Manager provides a central management console from which multi-vendor storage and infrastructure resources can be centrally and automatically discovered, mapped, monitored, configured and maintained. In addition, Storage Node Manager serves as a common launch point for device applications. Storage Node Manager is part of the Storage Area Manager suite and is available as an individual product.

Key features and benefits include:

Table 39: Storage Node Manager Features and Benefits

Feature	Benefit
Centralized Management Console	Operators may troubleshoot from a single console. Adding, deleting or changing storage configurations and tracking data center environment changes are handled through a single interface.
Status and Event Monitoring	Maximize storage availability by proactively and quickly isolating and resolving events with alerts and alarms (event logs maintained for review at any time).
Auto-Discovery of Devices	Maximize availability—storage network changes are continuously and automatically identified and mapped.
Device Applications	Reduced configuration and troubleshooting time. Device applications launch from the management station
Multi-Vendor Host Support	Choice among market leaders
Graphical Device Maps	Visualize all aspects of the storage network, including redundant connections and device zones
Device Icons	Manage more efficiently through a standard set of icons.
Customizable Location Fields	Improved asset management through the clearly identified physical location of all storage devices in large, distributed (e.g., campus) environments.
Fibre Channel Zone Presentation	Efficient management. Easily identify zone members in the maps.

Fabric Watch

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

Fabric Watch can be accessed through a web GUI, a telnet interface, an SNMP-based enterprise manager, or by modifying and uploading the Fabric Watch configuration file to the switch.

Fabric Watch monitors the following elements:

- Fabric events (such as topology reconfigurations, zone changes)
- Switch environment (fans, power supplies, and temperature)
- Ports (state changes, errors, and performance)
- GBICs

With Fabric Watch, each switch continuously monitors error and performance counters against a set of defined ranges. This and other information specific to each monitored element is made available by Fabric Watch for viewing and, in some cases, modification. This set of information about each element is called a *threshold*, and the upper and lower limits of the defined ranges are called *boundaries*. If conditions break out of acceptable ranges, an *event* is considered to have occurred, and one or more alarms (reporting mechanisms) are generated if configured for the relevant threshold.

Please refer to Table 17 for hardware support.

HP StorageWorks HA-Fabric Manager

As SANs expand and become more complicated, IT administrators need an efficient tool for managing the enterprise. HP StorageWorks HA-Fabric Manager (HAFM) is a comprehensive storage resource management application used to configure and manage HP's M-Series switch product line. HAFM simplifies SAN management, optimizes storage resources, and minimizes storage networking risks.

HAFM features include:

- complete management of the SAN from a single console
- integration with leading multi-vendor applications
- high levels of access and security
- scaling from department-level SANs to enterprise networks
- savings in time, money, and personnel resources
- detailed logging, diagnostics, and proactive alerts that monitor and ensure fabric health
- streamlined troubleshooting processes
- ease to use

HP StorageWorks HA-Fabric Manager - New Features:

- Persistent Fabrics
- Improved Zoning
- User Interface Enhancements
- 2Gb/s Management Support
- New Product Managers

HAFM can be run locally on the HAFM Server platform or remotely on any network-attached user workstation in the enterprise. The Java-based deployment support gives IT administrators the flexibility to run HAFM from virtually any type or size of client device including Sun, AIX, HP-UX, Linux, Windows NT, Windows 95, Windows 98 and Windows 2000.

Please refer to Table 20 for hardware support.

HP StorageWorks Fabric Manager

HP Fabric Manager is an application that manages multiple StorageWorks SAN switches and fabrics in real time. Fabric Manager provides the essential functions for efficiently configuring, monitoring, dynamically provisioning, and managing StorageWorks SAN fabrics on a daily basis.

Fabric Manager is tightly integrated with other HP StorageWorks SAN management products, such as Web Tools and Fabric Watch. Organizations can use Fabric Manager in conjunction with other leading SAN and storage resource management applications as the drill-down element manager for single or multiple fabrics.

Highlights

Fabric Manager version 4.x enables the user to:

- Provision, monitor, and administer large numbers of switches and multiple StorageWorks SAN fabrics with greater efficiency.
- Perform management tasks across multiple devices and fabrics as a single management operation.

- Intelligently group multiple HP B-series Fabric switches or ports to facilitate aggregated management.
- Visualize and track changes to SAN configuration and state information through multiple views at multiple levels of detail.
- Launch Fabric Manager from other enterprise management applications as the element manager for the fabric or multiple fabrics.
- Track SAN assets by using detailed table views that can be exported to a spreadsheet.
- Discover details about devices logged into the fabric, including Host Bus Adapter (HBA) asset information.
- View the SAN layout through a topology map that specifies Intersite Link (ISL), switch, and device details.
- Identify, isolate, and manage SAN events across large numbers of switches and fabrics.

SAN Management: C-Series Product Line Switches

The C-Series switches can be managed in several different ways:

- via the serial port/manager console
- via telnet over IP
- with the Cisco Fabric Manager over IP or IP over Fibre Channel.

The Cisco Fabric Manager is a fabric-based, web-loaded application that provides fabric level (Fabric View) and switch (Device View) level management functions from most web-enabled clientss. Fabric Manager also provides a Summary View mode that reports on port statistics.

SAN/Fibre Channel Switch Management

The HP Fibre Channel SAN Switches are high performance, scalable switch fabrics designed for creating large SANs. The management functions let you control and monitor fabric topology, frame throughput, error statistics, fans, cooling, media type, port status, and a variety of other information to aid in system debugging and performance analysis.

The administrative and diagnostic functions of the SAN switch are accessible from IP over the RJ-45 10/100BaseT Ethernet port or any Fibre Channel port. You can use any Simple Network Management Protocol (SNMP)-based management product to access the SNMP agent. You can also use any supported web browser to use the Java Web Management Tools.

Supported management methods include:

- SNMP
- Telnet
- Web-based Management Tools launched via Network View
- Telnet command subset via switch front panel display (FC SAN Switch/16 only)

OVSAM

There is an HP OpenView Device Plug-In's (DPIs) for B-Series, C-Series, and M-Series Switches. These DPIs extend Storage Node Manager and Storage Optimizer support to discover, map, and monitor the health and performance of the HP-supported switches. These DPIs can be obtained through this URL:

http://www.openview.hp.com/products/dpi/

SAN Storage Management Tools

Command View EVA

Command View EVA is a SAN management application to configure and monitor HSV controllers. For each controller pair, Command View EVA enables you to:

- Initialize an Enterprise Virtual Array and create a pool of disk drives
- View, configure, and upload code to the controllers and disk drives
- View and configure virtual disks, and host properties
- Dynamically expand volumes for operating systems that support dynamic volume expansion
- Make temporary snapshots of volumes for backup purposes (with supported firmware, requires license)
- Make snapclones to create an exact copy of another Virtual Disk at a particular point in time (with supported firmware, uses same license as snapshots)
- View Enterprise Virtual Array event logs

VCS Features and Functionality

These features do not reflect the more restrictive requirements of solutions like Business Copy and Continuous Access EVA.

- Support for up to 240 disk drives per storage system
- Management of up to 512 virtual disks per disk pool ranging in size from 1GB to 2TB per virtual disk
- Dynamic capacity expansion and virtual disk data load leveling
- Distributed sparing of disk capacity
- Virtually Capacity-Free Snapshot (Vsnap)
- Virtually Instantaneous Snapclone
- Dual redundant controller operation for increased fault tolerance
- Multiple Bus Failover Support
- Battery Back-up
- Asynchronous Disk Swap (Hot Swap)
- Clustered Server Support
- Mirrored Write-Back Cache Support
- Read-Ahead and Adaptive Read Caching Support
- Virtual RAID Arrays (Vraid0, Vraid1, Vraid5)
- Non-disruptive software upgrade capability
- Supports connection of up to 256 hosts
- Multi-Vendor Platform Support
- Controller Password Protection for Configuration Control
- Selective Storage Presentation and SAN-based data zoning
- GUI Interface for management and monitoring

Supported management methods include:

- SSSU
- Storage Management Appliance

VCS works in a heterogeneous environment that includes Tru64 UNIX, OpenVMS, Microsoft Windows NT and Windows 2000, and Sun Solaris. This application is at the storage system level.

Command View EVA Restrictions

Current restrictions of the Command View EVA must be enforced:

- A maximum of 16 Enterprise Storage Systems can be managed by one Storage Management Appliance
- An Enterprise Storage System can be actively managed by only one Storage Management Appliance

General HSV Storage System Configuration Process

The following steps highlight the configuration process for storage systems. Refer to your storage system user guide for more information.

1. Set up the storage system according to the product user guide.
2. Ensure that you have connected the Fibre Channel from HSV controller ports to optical interfaces found on the Fabric Switch.
3. Ensure that appliance and the HSV controller port WWNs are in a Storage Management Appliance zone.

Initially, Enterprise Storage Systems are display as "UNINITIALIZED" on the Command View EVA browser window. It is recommended that, when the storage system is initialized, a intuitive name is used for display and monitoring convenience.

1. In the navigation pane, click on a controller icon.
2. In the Content Pane, click the INITIALIZE button.

   A pop-up message confirms that you are initializing the storage system. It also states that any data associated with the selected system will be lost, and then asks if you wish to proceed with the initialization procedure.

   If you have not previously entered the license key for the storage system, you will be prompted to do so.
3. Enter a name for the storage system.

   A suggestion would be:

   location-controller type- VCS version -

   For example: RACK05-V110-V2002 would indicate the element resides in Rack 5, and contains HSV110 controllers running VCS code V2002.
4. Specify the number of disks in the default group. Enter from 8 up to the total number of drives in the subsystem.
5. Click on the **Advanced Options** button and set the date and time option. It is recommended that you synchronize the time with the Storage Management Appliance time. If this practice is used with all controllers, then you will have synchronized times on all event log entries. Always use the same Storage Management Appliance to initialize all EVAs or synchronize the time of all Storage Management Appliances to the same source

   Leave the Console LUN ID set to "**0**"

Element Manager for HSG

Element Manager for HSG is a Storage Management Appliance application to configure and monitor HSG80/60 controllers. For each controller pair, Element Manager for HSG enables you to:

- View existing virtual disk, controller, physical disk, and host properties
- Make changes to these properties for different configurations
- Configure Remote Copy sets and add associations (with supported firmware)
- Dynamically expand volumes for operating systems that support dynamic volume expansion
- Make temporary snapshots of volumes for backup purposes (with supported firmware)

HSG Element Manager Restrictions

Current restrictions of the HSG Element Manager must be enforced:

- Maximum of 25 HSG Storage Systems can be managed by one Storage Management Appliance
- An HSG Storage System must not be visible to more than one Storage Management Appliance

---

Note: The HSG Element Manager is not a supported management tool for DRM environments. Contact HP consulting services for information about managing DRM.

Storage Management Appliance and HSG storage system Communication

When configuring an HSG controller in a Storage Management Appliance storage environment, you will need to enable CCL (i.e. setting the controllers to SCSI-3 or SCSI-2 with CCL Enabled) or provide a dedicated LUN (i.e. setting the controllers to SCSI-2 CCL Disabled) for the Storage Management Appliance. If you are using a dedicated LUN instead of CCL, verify that the LUN is presented to the Storage Management Appliance through each controller host port connection for the Storage Management Appliance (there are two host ports per controller). The LUN may be a partition. For more information, see your HSG controller user guide.

General HSG Storage System Configuration Process

The following steps highlight the configuration process for storage systems. Refer to your storage system user guide for more information.

1. Set up the storage system according to the product user guide.
2. Ensure that you have connected the Fibre Channel from HSG controller ports to optical interfaces found on the Fabric Switch.
3. Ensure that the appliance and the HSG controllers port WWNs are in a Storage Management Appliance zone.

Note: The following steps are only necessary if the HSG controller is configured for SCSI-2 CCL Disabled.

a. Connect to the HSG controller via the serial interface. Refer to your HSG controller manual for further information on the serial connection.

b. Start terminal session. Refer to your HSG controller manual.

c. At the prompt in the terminal session, enter the Command Line Interface (CLI) command SHOW CONNECTION.

d. Verify, via HSG connection table, that the Fibre Channel HBA of the Storage Management Appliance is online. Use CLI command SHOW CONNECTION.

e. Create Logical Unit Number (LUN) and enable access from the LUN to the Storage Management Appliance.

4. Verify that the HSG controllers are discovered. To verify HSG status, you will need to configure and launch Element Manager for HSG and click on OPTIONS. Enable controllers that are discovered.

Currently, HSG elements are displayed by the controller serial numbers discovered. It is recommended to change the properties of the HSG Element to a more intuitive name for display and error reporting reasons.

1. In the navigation pane click on a controller serial number displayed.
2. In the Content Pane edit the ALIAS field and save changes.

A suggestion would be: *location-controller type-failover mode- ACS version*

For example: RACK05TOP-G80-T-V8.6F would indicate the element resides in the top of Rack 5, and are HSG80 controllers running in Transparent Failover with ACS code V8.6F.

HSG Storage System Array Controller Software/Command Line Interpreter

HSG Array Controller Software (ACS) for Fibre Channel Arbitrated Loop and Switched Fabrics provides storage controller software capability for the StorageWorks HSG60 and HSG80 Array Controllers in Fibre Channel arbitrated loop and switched fabric environments. HSG Array Controller Software is designed to be common across multiple operating system platforms. However, there may be operational differences between platforms, and there may also be features that are not supported on every platform.

Management of storage systems based on the HSG60 or HSG80 is provided directly through the controller serial port using a terminal or a terminal emulator (such as Microsoft Windows NT HyperTerminal) using the CLI interface. The CLI provides all the commands necessary to configure controller failover modes and parameter settings, controller and host connections to the SAN, storageset creation, SAN LUN access (SSP), RAID levels, and cache settings. The CLI also provides access to the array controller utilities. The utilities are used to monitor controller functions and statistics, and to allow storage system component replacement procedures be conducted while the storage system is active.

Selective Storage Presentation

Selective Storage Presentation (SSP) provides a way to control SAN access at the storageset or LUN level. SSP allows each server or HBA's storagesets (LUNs) to be presented exclusively to those that are allowed access. Additionally, SSP allows the setting of host modes and LUN offsets for each HBA connected to the storage system. The host mode is specially tailored to the storage communication techniques of the operating system type. The LUN offset feature of SSP allows higher numbered LUNs in a storage array to be presented in a range required by specific operating systems. The SSP feature also provides a way to track the numerous Fibre Channel HBAs within servers attached to a SAN by identifying each by name and WWN.

ACS Features / Functionality

Solutions such as Data Replication Manager may impose stricter limits than those shown here.

- Host Interconnect and Protocol Services
- Microsoft Cluster Server (MSCS) Support
- Dual Redundant Controller Operation
- Testing and diagnosis of the HSG array controller
- SCSI device control
- Transparent Controller Failover Support
- Multiple-Bus Failover Support
- Asynchronous Disk Swap (Hot Swap)
- ACS system management services
- Local program support
- Mirrored Write-Back Cache support
- Read Ahead Cache support
- Disk Mirroring capability (RAID 1)
- Disk Striping capability (RAID 0, 0+1)

- RAID capability (RAID 3/5)
- Storageset Expansion
- Disk Partitioning capability

Supported management methods include:

- Terminal emulation through the HSG's serial port using the CLI
- Command Console
- Command Scripter

ACS works in a heterogeneous environment that includes Tru64 UNIX, OpenVMS, Microsoft Windows NT and Windows 2000, Novell NetWare, Sun Solaris, HP-UX, SGI IRIX, IBM AIX, Linux x86, and Linux Alpha. This application is at the storage system level.

hp OpenView Storage Allocater

The hp OpenView Storage Allocater software delivers a central, unified method for virtualized storage access control and LUN-level storage assignment, enabling you to build and manage complex Storage Area Networks (SANs) with heterogeneous servers and storage devices.

Storage Allocater is part of the Storage Area Manager suite and is also available as an individual product.

Key features and benefits include:

Table 40: hp OpenView Storage Allocater Features and Benefits

Feature	Benefit
LUN level storage assignment	Optimized storage utilization.
Storage security controls	Prevent data loss and unauthorized access
Highly scalable	Cost effective, simplified management: one software solution may be used in a range of configurations
Add/remove/assign storage without host reboots	Increased system availability.
Mirrored SAN configuration	High system availability thanks to no single point of failure.
Automated storage network with host and storage discovery device capabilities	Dramatically reduce configuration time and eliminate a major source of errors.
Intuitive Graphical User Interface (GUI)	Maximize productivity and minimize training time with familiar techniques (drag-and-drop) and controls (view filters).
Share groups for cluster configurations	Visualized storage prevents errors when setting up cluster server and shared tape device environments.
Fibre Channel topology independence	Enhanced SAN configuration flexibility.
Supports open system, heterogeneous environments	Easy-to-use, cost-effective, single tool provides storage security.
Native file system and raw disk support	Simplifies moving existing storage to SANs.
Automated rogue host detection and notification	Enhanced data/information security. Eliminate component/driver tampering.

StorageWorks Command Console

StorageWorks Command Console (SWCC) is a feature-rich, graphical user interface providing local and remote management of StorageWorks HSG60 and HSG80 array controllers. It is a user-friendly tool for monitoring, configuring, and troubleshooting HP HSG60 and HSG80 storage arrays and controllers.

SWCC can be connected to your StorageWorks controller in several ways. Once connected, the program issues commands and interprets the responses sent by the controller. The user interface displays the logical and physical layout and status of a selected subsystem in graphical form. Command Console consists of two major components: the Client and the Agent. The Client, which includes the user interface and some additional services, provides a window into your storage subsystems. The Agent is a host-resident program that is an interface between the Client and the host's storage controller to interpret and transfer information.

The Agent acts as the Client's assistant in controlling your storage subsystem. The Agent continuously monitors the subsystem and notifies the Client of changes. Commands sent from the Client are received by the Agent and are routed to the storage subsystem via the subsystem's Fibre Channel bus. Subsystem status is transmitted back to the Client from the Agent via the network connection.

Software Features / Functionality

- Easy, graphical configuration of the storage subsystem using the graphical user interface.
- Graphical view of the controller and its physical and logical storage elements.
- Status monitoring of the storage subsystem using intuitive icons.
- Fault notification by pager, electronic mail, and event log entries.
- Management of multiple host systems through a TCP/IP network connection.
- Direct serial port connection.
- Direct SCSI port connection (Windows NT and Windows 2000 Only).
- Robust security that prevents unauthorized access to configuration capabilities.
- The Client supports Microsoft Windows NT 4.0 and Windows 2000.
- The Agent supports HP-UX, Tru64 UNIX, OpenVMS, IBM AIX, SUN Solaris, Linux, Novell Netware, and Windows (NT4.0 and Windows 2000).

All G80 DRM should be placed in separate zones from SWCC.

Array Configuration Utility for RA4000/4100/MSA1000

The HP Array Configuration Utility (ACU) software (for Smart Array products, StorageWorks RAID Array 4100/4000 systems, and MSA1000 systems) makes it easy to configure and expand your disk drive arrays. This graphical tool is very intuitive: by using its Configuration Wizards, you have the ability to configure your array controller, add additional disk drives to an existing configuration, or completely reconfigure your disk drive array.

Software Features/ Functionality

- Selective Storage Presentation: allows RA4100 and MSA1000 array sets to be partitioned to multiple servers for SAN access
- Online RAID Level Migration: allows for online post-configuration change to RAID level without destroying data or volume information.
- Online Capacity Expansion: lets you add storage to an operational RA4100 or MSA1000, reducing expensive server downtime.
- Online Volume Extension: allows for the capacity growth of existing logical volumes.
- Global Online Spare: reduces the risk of data loss by facilitating automatic rebuilds after a drive failure.
- Logical Drive Capacity Extension: allows the user to increase the size of existing logical drives online under Windows NT and offline for other operating systems.
- Pre-Failure Warranty: Drives installed in an RA410 or an MSA1000 and monitored under HP Insight Manager are supported by a Pre-Failure (replacement) Warranty.

Note: Pre-Failure Warranty allows for the replacement of designated drives in an RA4100 before they actually fail when using HP Insight Manger on HP servers.

Note: Some operating systems may not support all of these features.

Secure Path Multi-Path Software

Depending on the platform or operating system, high availability functionality may or may not be embedded in the operating system I/O drivers. Tru64 UNIX and OpenVMS operating systems have the ability to create and maintain multiple paths over the SAN to the same LUN, with support for these functions embedded. For those operating systems that do not support multi-pathing, HP provides this capability using HP Secure Path.

The HP Secure Path product provides continuous data access for HP RAID storage systems accessed by operating systems that are both HP-based and not HP-based. When combined with the inherent fault-tolerant features of the RAID Array, this configuration effectively eliminates single points of failure in the storage system.

When a host bus adapter, cable, or controller in a path fails, the failure is detected and I/O is automatically re-routed to the functioning, alternate path. This process, called failover, requires no resource downtime and ensures high availability of data. Storage units that have experienced failover may be configured to failback automatically after a path is restored. Failback can also be done manually through the use of the Secure Path Manager (Windows) or via spmgr (UNIX.)

Software Features / Functionality

- Switched fabric and loop support
- Automatic path failover
- I/O load distribution
- User-selectable failback
- Supported on the Storage Management Appliance

Secure Path works in a heterogeneous environment. See Chapter 4, "Heterogeneous SAN Platform and Storage System Rules".

Secure Path Element Manager on the Storage Management Appliance

Managing Windows NT, Windows 2000, and Windows 2003 Secure Path servers throughout the enterprise is now available using the Storage Management Appliance. Secure Path Element Manager uses the easy-to-use Storage Management Appliance Web GUI interface to manage and monitor hosts and HSG60/80 and EVA3000/EVA5000 storage subsystems and integrates with the Storage Management Appliance's notification utility.

The notification utility provides centralized functionality. The web-based Notification console is used to provide a single, modular, networked software unit that has the ability to handle Event Logging, SMTP, SNMP and command line launching operations.

Secure Path Element Manager uses TCP/IP to communicate with Secure Path servers. Adding the Storage Management Appliance server name to the Client list on the Secure Path Server will allow Secure Path Element Manager to discover the Secure Path server and add it to a profile.

SAN Data Management Tools

Business Copy

Business Copy (BC) is web-based application software that manages controller-based clone and snapshot operations. Cloning is a mirroring copy function that allows you to create an exact copy of a LUN; snapshot provides an instantaneous point-in-time copy function. BC can be used to meet business continuance requirements by minimizing application downtime required for system backups and data migration activities. BC automates the creation of command files that control the cloning or snapshot operation. BC also allows you to mount the clone or snapshot on a second host on the same controller.

BC is a host-based tool that can be accessed by the user directly via a GUI or remotely via a browser. The tool then interacts with the requested application(s) to stop new I/O and flush pending I/O to disk. Once the I/O is stopped, BC instructs the storage via the in-band CLI to perform a snap or clone operation. Finally, on completion of that operation, BC restarts the application.

BC automates the creation of command files that control the cloning or snapshot operations. BC also allows users to mount the clone or snapshot to a new host. The new host can then act as a dedicated backup server or data warehouse server. All operations are performed on the clone or snapshot, minimizing performance impact on the production system.

Software Features / Functionality

- Web-based application
- Supported on the Storage Management Appliance
- Easy management of complex cloning and snapshot operations
- Supports LAN-less backup
- Simplified, centralized storage management

Business Copy works in a heterogeneous host environment that includes Tru64 UNIX, Microsoft Windows NT, Windows 2000, and Sun Solaris. This application is at the server level.

Business Copy on the Storage Management Appliance

Managing Windows NT and Windows 2000 Business Copy (BC) servers throughout the enterprise is now available using the Storage Management Appliance.

Business Copy uses TCP/IP to communicate with BC servers. Adding the Storage Management Appliance server name during the BC server agent setup will allow the BC application on the Storage Management Appliance to discover the BC server.

Virtual Replicator

The hp OpenView Storage Virtual Replicator (VR) combines a rich set of innovative capabilities that enhances and simplifies storage management for Microsoft Windows NT and Windows 2000 environments. Through virtualization, online volume growth, snapshot and management features, the software complements the standard capabilities within the operating system.

Virtual Replicator utilizes industry-standard server, storage, and network-interconnect components, protecting an organization's current and future storage investments.

Storage Virtual Replicator provides the ability to create instant, virtual snapshots of production data without having to physically copy it. A snapshot, which looks exactly like the original disk from which it was copied, takes seconds to create and allows customers to back up and restore data with minimal impact to users and applications. Customers can schedule automated snapshot backups using the integrated policy-based scheduling and scripting features.

Software Features / Functionality

- Virtualization:

  Allows companies to respond quickly to rapidly changing storage capacity requirements. With storage virtualization, multiple storage arrays can be grouped into a pool of disk space for individual or clustered systems to use. Multiple high-capacity virtual disks, up to 2 terabyte in size, can be created from a pool for users and their applications. System administrators can tailor disk space to specific requirements for maximum utilization of storage resources.

- Online volume growth:

  Enables easy, non-disruptive growth for Windows 2000 with zero downtime. Online Volume Growth allows a system administrator to grow an existing volume on a Virtual Replicator virtual disk and also on a Windows 2000 basic disk. The system will remain online, and the data on the volume will remain intact.

- Snapshots:

  Enable the instant creation of multipurpose virtual replicas of production data without the requirement of a physical copy. Snapshots function identically to ordinary physical disks with both read and write capability. Whenever a quick copy of production data is needed, snapshots can be used with minimal disruption to running applications. For example, the snapshot can be the source for backup using standard backup tools. Snapshots can remain online for restore operations, testing, and data mining.

- Management:

  Simplification through easy-to-use interfaces using Microsoft Management Console or a command line. Interactive wizards are available to guide the administrator through all management tasks and create automatic schedules of operations.

Virtual Replicator provides server-based virtualization and is supported on Microsoft Windows NT and Windows 2000 (Server and Advanced Server.) VR is cluster-aware to ensure business continuance.

Continuous Access EVA

Continuous Access EVA is a Fibre Channel storage controller-based data replication (remote mirroring) solution to support disaster tolerance requirements. Continuous Access EVA works with the HP StorageWorks Enterprise Virtual Array storage system, which contains the HSV virtualized RAID controller. The HSV controller and the Virtual Controller Software (VCS) Version 3.0 and 3.01 enhance the virtualization with remote replication technology.

Continuous Access EVA copies data online and in real time via synchronous (and in Version 3.01 asynchronous) replication to a remote EVA through a local or extended storage area network (SAN). Additionally, data replication can be bidirectional, meaning that a storage array can be both a source and a destination. A single EVA may have a replication relationship with up to two other arrays, using different DR groups for each relationship. A particular LUN can be replicated in only one direction between the two storage arrays. Write I/O is sent to the

source and then replicated by Continuous Access to the destination. Properly configured, Continuous Access EVA can be a complete disaster-tolerant storage solution that guarantees data integrity in the event of a storage system or site failure.

A basic two site Continuous Access EVA configuration is shown in Figure 44.

While Continuous Access EVA may be used to satisfy data distribution or data migration requirements, this version of the Design Guide does not provide design recommendations for those solutions.

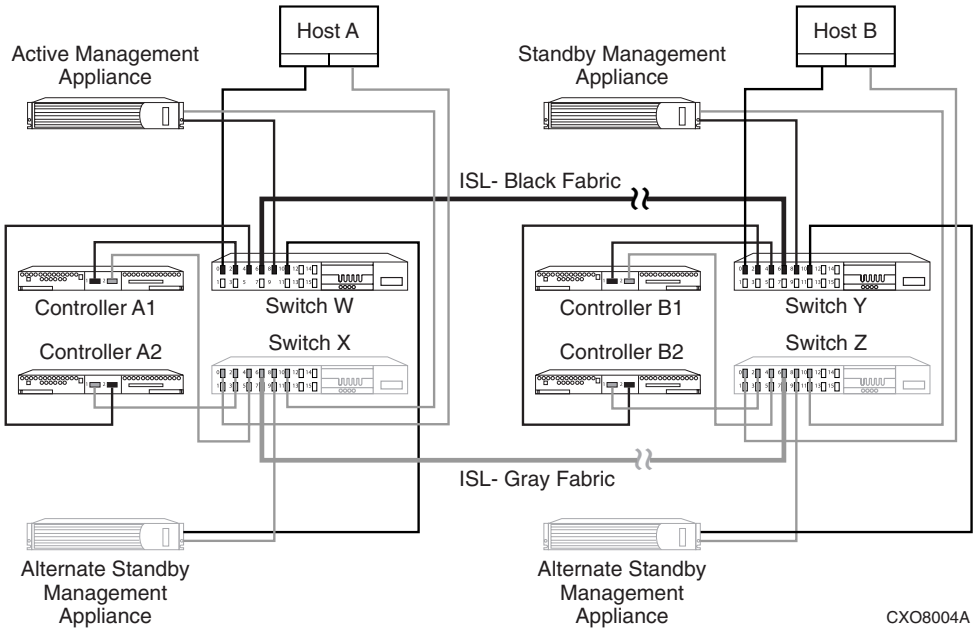


Figure 44: Continuous Access EVA basic configuration

Features

The following are prominent features of the Continuous Access EVA V1.1 solution:

- In-order synchronous or asynchronous remote replication (remote mirroring)
- Automated failover support
- Support for the following disk drives:
  - 36 GB 10K and 15K RPM
  - 72 GB 10K and 15K RPM
  - 146 GB 10K RPM
- Normal and fail-safe data protection modes of operation
- Dual redundant controller operation for increased fault tolerance
  - No single point of failure
  - Pairs of arrays share replication relationship and any one array may share a relationship with up to two arrays
  - Replicated write-back cache support
  - Read-ahead and adaptive read caching support
  - I/O continuation during normalization and merging
- Intersite link suspend and resume operations

- Multi-vendor platform support
- Dynamic capacity expansion, if supported by OS
- Merge of write history log in write order
- Failover scripting
- Multiple bus failover support
- Continuous Access user interface
- Asynchronous disk swap (hot swap)
- Controller password protection for configuration control
- GUI interface for management and monitoring
- Selective storage presentation for SAN-based data zoning
- B-Series, C-series, and M-Series switch support
- Virtual RAID arrays (Vraid0, Vraid1, and Vraid5)
- Virtual RAID (Vraid) techniques that:
  - improve performance
  - increase disk utilization efficiency
  - dynamically expand storage capacity
- Virtual disk data load leveling
- Clustered server support
- Distributed sparing of disk capacity
- Non-disruptive software upgrade capability
- LiteTouch Management
- Battery back-up
- Bi-directional replication
- Copy set size of 1 GB to 2 TB in 1 GB increments
- Up to 128 remote copy sets
- Up to 128 DR groups
- Up to eight copy sets per DR group
- Management of up to 512 virtual disks per EVA ranging in size from 1 GB to
- 2 TB per virtual disk
- Maximum of 240 FC-AL drives (with expansion cabinet) per storage system
- Maximum of 8 storage systems on the SAN management zone
- Maximum of 128 Fibre Channel adapter (FCA) connections per pair of arrays, and if a dual fabric, then 64 per fabric.c
- Maximum of 256 LUN presentations from an EVA to a single FCA.
- Up to 28 B-Series switches per fabric; seven hops are allowed (three per site and one as the intersite link)
- Up to 24 M-Series switches per fabric; three hops are allowed (one per site and one as the intersite link)
- Up to 11 C -Series switches per fabric, 3 hops are allowed, 1 per site, and one per intersite link. (only on VCS V3.0 at this time).
- Dark Fibre to 35 km at 2 Gbps or 100 km at 1 Gbps
- 2 Gbps end-to-end Fibre Channel solution

- 100 ms latency with wide area network gateways
- Virtually capacity-free snapshot (Vsnap)
- Virtually instantaneous snapclone
- Snapclone across physical disk groups
- Multiple snaps of the same data (both source and destination)
- Maximum of 8 snapshots or snapclones per DR group at the local or remote site
- The option of selectable World Wide Names (WWNs) for Vsnaps, snapshots, and snapclones

Data Replication Manager

The HSG80 Data Replication Manager (DRM) Software is the software component of the HSG80 array controller used in switched fabric environments for remote data replication. Data Replication Manager Software is a storage-based disaster tolerance and workload migration solution that provides the ability to copy data, in real time, to a remote location, up to 100 km away using direct Fibre Channel or further using either FC over ATM or FC over IP links. This is done without any host involvement. The HSG80's dual host port design, when used in DRM configurations, allows for long distance mirroring in a switched No Single Point of Failure (NSPOF) Fibre Channel topology.

The DRM software executes in the HSG80 array controller and processes I/O requests from the hosts, performing the local and remote device-level operations required to satisfy the requests. This is done through the use of a pair of initiator and target controllers sharing a switched NSPOF Fibre Channel fabric. Host generated Reads are performed on the local copy of the data. Host generated Writes to the local storage are copied by DRM from the local controller directly to the remote controller automatically. This capability provides the ability to maintain the same data at both locations, providing disaster tolerance protection.

Software Features / Functionality

- Online, real-time data replication to a local or remote site
- Data replication over a Fibre Channel SAN
- Cloning at Initiator and Target sites
- Snapshot support at Target site
- Cascaded switches support
- Full Fibre Channel-to-ATM connectivity with line speeds of T1 through OC3
- Full Fibre Channel-to-IP (FCIP) connectivity with line speeds of T1 through 1 GbE
- Replicate up to 100 km(~63 miles) with Very Long Distance GBIC
- Asynchronous and synchronous transfer modes
- Write History Logging and "Mini-Merge" reconstruction
- Stretched Clusters capabilities for Microsoft Windows NT and OpenVMS
- Association sets
- Non-RCS LUN support
- Switch Zoning support
- Wavelength Division Multiplexing

Data Replication Manager works in a heterogeneous host environment that includes HP OpenVMS, HP Tru64 UNIX, HP-UX, IBM AIX, Microsoft Windows NT, Windows 2000, Novell NetWare, and Sun Solaris. The application is at the storage system level.

See the DRM Design Guide which is available online for additional details.

Command Scripter

Command Scripter is application software that provides command-level control of HP StorageWorks systems equipped with HSG60, HSG80, HSZ70, and HSZ80 Array Controllers. With Command Scripter, you can create, edit, and run script files that contain StorageWorks Command Line Interpreter (CLI) commands. This allows automation of frequently performed StorageWorks operations.

Two interfaces are included in Command Scripter: a command line interface for local, direct connection to StorageWorks controllers and a web-based interface, which requires StorageWorks Command Console (SWCC)) for centralized, remote connection via browser.

Software Features / Functionality

- Web-based interface for centralized, remote connection to StorageWorks array controllers
- Command line interface for local, direct connection to array controllers
- Select agent host and StorageWorks subsystem
- Create and edit CLI script files
- Run saved CLI script files
- Execute a single CLI command
- Display CLI command history

Command Scripter works in a heterogeneous host environment that includes Tru64 UNIX, OpenVMS, Microsoft Windows NT, Windows 2000, Sun Solaris, HP-UX and AIX (command line interface only), and AIX (command line interface only). This application is at the server level.

Storage System Scripting Utility

The Storage System Scripting Utility (SSSU) is the character cell interface for a user. Host based application that needs to access the Command View EVA should use the EMClientAPI. That API will transport SOAP/XML requests over the wire to the element manager, handling security and communication. The EMClientAPI provides an efficient machine interface to the Command View EVA, specifically designed for host-based applications.

SAN Storage Usage & Monitoring Tools

Automation Manager

Automation Manager provides a tool with which a storage administrator can automate the management of a storage area network. Automation Manager runs, controls, and manages predefined policies that storage administrators can configure for their environment. Predefined policies are provided with the product as Perl scripts. In addition, you can create and import your own management scripts.

Automation Manager also provides the following utilities to assist in managing storage operations:

Reports – View and print status reports about storage operations.

Agents – View and download an agent to hosts on which scripts resides. Agents enable Automation Manager to communicate with and run batch jobs on hosts systems.

Notification – Set up different notification types for Automation Manager events.The notification utility provides centralized functionality. The web-based Notification console is used to provide a single, modular, networked software unit that has the ability to handle Event Logging, SMTP, SNMP and command line launching operations.

hp OpenView Storage Builder

The hp OpenView Storage Builder is a storage inventory and resource planning tool for direct attached, SAN attached and network attached storage, and enables you to monitor, manage storage capacity and plan for future storage demands.

Storage Builder is part of the Storage Area Manager suite and is available as a separate product.

Key features and benefits include:

Table 41: hp OpenView Storage Builder Features and Benefits

Feature	Benefit
Centralized view of allocated vs. unallocated storage, and used vs. unused storage-by application, host, storage device, LUN, partition, volume, directory and user	Understand how much storage is assigned, being used, available for deployment, and how to balance capacity across systems/users. Make better use of storage resources. Lower total cost of ownership.
Automated thresholds warning system: set thresholds on hosts, partitions, volumes, directories and user	Receive early warning of capacity shortfalls that could cause system outage or user inconvenience. Capacity quotas on a per-user basis ensure storage growth is in line with company goals.
Group hosts, interconnects, bridges, NAS devices and storage components to reflect departments or physical locations, then create screens, reports and thresholds for these storage groups	Better identification of major users and heavily used devices. Establish norms and quotas to ensure storage growth is in line with company goals.
Identification of junk or stale files selectable by extension, such as MP3 or games, that waste valuable storage space	Free up primary storage capacity for use in meeting business goals.
Screens and reports that rank hosts by the amount of storage accessed each day	Achieve better asset utilization, higher availability and centralized management.
Historical trending of storage capacity data through screens and reports. Future extrapolation of historical data	Anticipate storage capacity shortfalls. Plan for and justify just-in-time purchases of additional storage capacity. Improve storage resource management efficiency and utilization rates, which lowers total cost of ownership.
Tabular and graphic reports showing allocated vs. unallocated storage, as well as consumed vs. free storage	Clearly communicate facts, trends and analysis concerning storage resources to staff and upper management.
Volume management	Provide better visibility into the host to LUN utilization mapping.
Capacity information can seamlessly be integrated into HP OpenView Internet Usage Manager (IUM)	Allow for centralized usage analysis, billing and charge-back.
Applications are automatically discovered and elements of the applications are reported and mapped to the storage devices	Provide better visibility of how the applications are utilizing the storage devices in order reduce costs associated with application capacity.

hp OpenView Storage Accountant

The hp OpenView Storage Accountant provides a toolset to measure, or meter, storage assigned to users (customers/organizations) for financial analysis, budgeting and charge-back.

Storage Accountant is part of the Storage Area Manager suite and is available as an individual product.

Key features and benefits include:

Table 42: hp OpenView Storage Accountant Features and Benefits

Feature	Benefit
Create and manage customer accounts and organizations	Better customer service. Analyze storage service usage on customer/organization basis. Define greater levels of granularity within one customer, organization.
Define and apply service levels	Reduce costs by providing the required type of storage based on usage analysis.
Assignment of storage to accounts	Measure assigned storage for tracking consumption, budgeting and financial analysis.
Automated billing Detailed usage and billing views and reporting	Recover costs of providing storage services. Manage relationships.
CSV, HTML and XML output	Export charge-back information to third-party applications for billing and financial analysis.
Audit log maintenance	Track events related to customers, service levels and storage consumption.
Seamless integration with HP OpenView Internet Usage Manager (IUM)	Centralize usage analysis and billing/charge-back.

hp OpenView Storage Optimizer

The hp OpenView Storage Optimizer provides performance monitoring of all components of the Storage Area Network (SAN), including hosts, storage devices, and infrastructure.

Storage Optimizer is part of the Storage Area Manager suite and is available as an individual product.

Key features and benefits include:

Table 43: hp OpenView Storage Optimizer Features and Benefits

Feature	Benefit
Monitors key metrics of SAN performance, drilling down to individual node level (host, switch or storage array)	Ensures service levels and availability of business processes are met.
Management of storage resources via a single centralized station	Centralize storage management on a SAN. Company-wide cost savings in a tight job market.
Multiple data presentation formats-GUIs, CLUIs and interval summation reports	Receive information in a user-preferred format.
Automated baselining and over-baseline notification for performance metrics	High availability and reliability. Proactively ensure that SAN SLAs are met.
Graph historical performance metrics and extrapolate historical data	Proactively identify SAN infrastructure trends/anomalies. Evaluate the impact of upgrades. Identify future performance demands. Improve system efficiency.

Network Attached Storage

7

This chapter covers the following major topics:

- NAS / SAN Integration Overview
- StorageWorks NAS 4000s / 9000s Features
- StorageWorks NAS b3000v2 Features
- StorageWorks NAS e7000v2 Features
- StorageWorks NAS 8000 Features
- StorageWorks NAS SAN Configuration and Zoning Rules
- StorageWorks NAS SAN Fabric Rules
- StorageWorks NAS SAN Storage Rules

NAS / SAN Integration Overview

Customers typically base their decisions on SAN or NAS implementations by selecting file or block formats and by determining the hardware and software components they need. But with NAS integration in a heterogeneous SAN environment using the StorageWorks NAS devices, the decision to use either NAS or SAN systems becomes irrelevant.

With NAS/SAN integration, the customer benefits are significant and include the following:

Table 44: NAS/SAN Integration Features and Benefits

Feature	Impact	Benefit
The decision to use NAS or SAN systems is irrelevant because customer should use both.	Fully integrated, converged storage architectures.	Ease of choice. Eliminates technical trade-offs. Easy to implement and grow.
Supports multiple operating systems.	Allows centralized data and increases flexible storage capacity and efficiency. Data can be shared across multiple operating systems regardless of the device or operating system.	Provides strategic power in the marketplace and consolidates data. Saves money by providing better disk utilization.
Storage networks integrate with existing hardware	Less interruption to production systems and easier to manage.	Reduces Total Cost of Ownership (TCO).
Enterprise-wide file sharing reduces file duplication.	The right information to the right person at the right time in the right format.	Data sharing, which reduces storage capacity requirements.
Reliable and efficient access to data and application information 24x7.	Improves both local and wide- area data retrieval.	Improved data availability across the enterprise.
Seamless integration of storage devices and architecture.	New applications integrate reliably to ensure new data does not overload your system.	Faster time to market. Lower maintenance costs.
Data storage in centrally managed locations rather than across multiple application servers.	Facilitates administration, backup, and security.	Centralized deployment of specialized resources and skill sets.
Storage resources shared among a much larger number of processing systems and users.	Improved efficiency and simplified management.	Better asset allocation.
Data is highly accessible.	Business continues without interruption.	Provides strategic power in the marketplace.

StorageWorks NAS Features

StorageWorks NAS 4000s / 9000s Features

The StorageWorks Network Attached Storage (NAS) 4000s and 9000s fuses NAS and SAN, offering customers the greatest scalability and flexibility, providing cost effective management for their storage resources. This latest innovation from HP provides enhanced performance along with simplified, centralized storage and system management, ultimately saving customers resources, time, and money, lowering their Total Cost of Ownership (TCO). The StorageWorks NAS delivers the fusion of NAS and SAN in a common, networked storage pool that provides customers with the flexibility to choose file (NAS) or block (SAN)-level access to best suit the needs of their applications.

- Windows Storage Server 2003 Support
- Multi-protocol File Serving (Windows, UNIX/Linux, NetWare, AppleTalk)
- Users, groups share creation/management
- Quotas
- Manageability
- Backup support
- Anti-virus support
- Storage virtualization
- Snapshot capabilities
- High Availability
- Cluster support
- Redundant hardware components
- Data replication Support
- Integrated Lights Out (iLO) connectivity
- Featuring HP SAN connectivity
- 10/100 Ethernet (TCP Offload Engine - TOE, Optional)
- Gigabit Ethernet (TCP Offload Engine - TOE, Optional)
- Fibre Channel storage connectivity using the XP*, VA*, EVA, MA/RA/ESA/EMA, and MSA storage arrays
- Services; warranty uplifts
- Installation and configuration service
- CarePAQ Priority Services supplying 24x7 support with a maximum response ranging down to 2 hours for hardware and 30 minutes for software

Support for these Arrays will be include in December 2003.

StorageWorks NAS 4000s/9000s Hardware

The StorageWorks NAS is qualified in a heterogeneous open SAN as both a stand-alone or clustered server and follows the same Windows 2003 SAN hardware rules found in this guide.

Refer to the *StorageWorks NAS 4000s/9000s QuickSpec* document for additional information, including the latest IP network controller hardware support:

StorageWorks NAS b3000v2 Features

The StorageWorks NAS b3000v2 is the entry-point into NAS/SAN fusion solutions with enterprise-level availability, scalability and performance in a turnkey package that includes:

- Multi-protocol File Serving (Windows, UNIX/Linux, NetWare, AppleTalk)
- Users, groups share creation/management
- Quotas
- Manageability
- Backup support
- Anti-virus support
- Storage virtualization
- Snapshot capabilities
- Availability
- Cluster support
- Redundant hardware components
- Data replication Support
- Integrated Lights Out (iLO)
- Fibre Channel storage connectivity with MSA1000, EVA3000, EVA5000, and VA storage
- 1Gb and/or 2Gb HP SAN connectivity
- 10/100 Ethernet (TCP Offload Engine - TOE, Optional)
- Gigabit Ethernet (TCP Offload Engine - TOE, Optional)
- Services; warranty uplifts
- Installation and configuration service

StorageWorks NAS b3000v2 Hardware

The StorageWorks NAS b3000v2 is qualified in a heterogeneous open SAN as both a stand-alone or clustered server and follows the same Windows 2000 SAN hardware rules found in this guide.

Note: Refer to the StorageWorks NAS B3000v2 QuickSpec document for additional information, including the latest IP network controller hardware support:

http://h18006.www1.hp.com/products/quickspecs/11339_div/11339_div.html

---

StorageWorks NAS e7000v2 Features

The StorageWorks Network Attached Storage (NAS) e7000v2 fuses NAS and SAN, offering customers the greatest scalability and flexibility, providing cost effective management for their storage resources. This latest innovation from HP provides enhanced performance along with simplified, centralized storage and system management, ultimately saving customers resources, time and money, lowering their Total Cost of Ownership (TCO). The StorageWorks NAS e7000v2 delivers the fusion of NAS and SAN in a common, networked storage pool that provides customers with the flexibility to choose file (NAS) or block (SAN)-level access to best suit the needs of their applications.

- Multi-protocol File Serving (Windows, UNIX/Linux, NetWare, AppleTalk)
- Users, groups share creation/management
- Quotas
- Manageability
- Backup support
- Anti-virus support
- Storage virtualization
- Snapshot capabilities
- High Availability
- Cluster support
- Redundant hardware components
- Data replication Support
- Integrated Lights Out (iLO) connectivity
- Featuring HP SAN connectivity
- 10/100 Ethernet (TCP Offload Engine - TOE, Optional)
- Gigabit Ethernet (TCP Offload Engine - TOE, Optional)
- Fibre Channel storage connectivity using the XP, VA, EVA, MA/RA/ESA/EMA, and MSA storage arrays
- Services; warranty uplifts
- Installation and configuration service
- CarePAQ Priority Services supplying 24x7 support with a maximum response ranging down to 2 hours for hardware and 30 minutes for software

StorageWorks NAS e7000v2 Hardware

The StorageWorks NAS e7000v2 is qualified in a heterogeneous open SAN as both a stand-alone or clustered server and follows the same Windows 2000 SAN hardware rules found in this guide.

Refer to the *StorageWorks NAS Executor E7000v2 QuickSpec* document for additional information, including the latest IP network controller hardware support:

http://h18006.www1.hp.com/products/quickspecs/11004_div/11004_div.html

StorageWorks NAS 8000 Features

HP StorageWorks NAS 8000 solutions provide easily managed network-attached storage (NAS) solutions in dedicated storage and SAN configurations for customers that require file-sharing flexibility. With an HP operating system optimized for file serving, NAS 8000 solutions attach directly to Ethernet networks, and deliver- low maintenance and high uptime. Cluster technology is available for environments requiring mission-critical access to data.

The NAS 8000 solutions support Windows, UNIX, and Linux. Network administration, user access, and storage configurations are all easily managed through the Command View NAS or command line interfaces. The NAS Data Path Manager software enables management and control of the data paths.

- Multi-protocol File Serving (Windows, UNIX/Linux)
- Users, groups share creation/management
- Quotas
- Manageability
- Backup support
- Anti-virus support
- Snapshot capabilities
- High Availability
- Cluster support
- Redundant hardware components
- Integrated Lights Out (iLO) Connectivity
- 10/100 Ethernet
- Gigabit Ethernet
- Fibre Channel storage connectivity using the XP, VA, EVA 5000, EMA & MA arrays
- Services; warranty uplifts
- Installation and configuration service

StorageWorks NAS 8000 Hardware

The StorageWorks NAS 8000 is qualified in a heterogeneous open SAN as both a stand-alone or clustered server and follows the same Linux SAN hardware rules found in this guide.

Refer to the *StorageWorks NAS 8000 QuickSpec* document for additional information, including the latest IP network controller hardware support:

http://www.hp.com/products1/storage/products/nas/8000/specifications.html

Also refer to the *HP StorageWorks NAS 8000 SAN Storage Configuration Guide* technical whitepaper available at:

http://welcome.hp.com/country/us/eng/prodserv/storage.html

StorageWorks NAS SAN Configuration and Zoning Rules

NAS Product	Source for Rules
StorageWorks NAS 4000s StorageWorks NAS 9000s StorageWorks NAS b3000 v2 StorageWorks NAS e7000 v2	Windows 2003 SAN Configuration and Zoning information
StorageWorks NAS 8000	Linux SAN Configuration and Zoning information

StorageWorks NAS SAN Fabric Rules

The StorageWorks NAS 4000s, NAS 9000s, NAS b3000v2, NAS e7000v2, and the NAS 8000 are supported in SAN fabrics consisting exclusively of switch models listed for the B-Series product line or exclusively of switch models listed for the M-Series product line.

StorageWorks NAS SAN Storage Rules

For additional information on supported storage system firmware versions, contact your HP field representative.

StorageWorks NAS 4000s Storage Rules

The StorageWorks NAS 4000s supports MSA, EVA, MA/RA/ESA/EMA, VA, and XP arrays. Versions of firmware supported are consistent with those supported under Windows 2003. See the individual storage array documentation or contact your HP representative for firmware support levels.

Note: XP and VA support will officially be released in December 2003.

StorageWorks NAS 9000s Storage Rules

The StorageWorks NAS e7000v2 supports XP, VA, MSA, EVA, and MA/RA/ESA/EMA arrays. See the individual storage array documentation or contact your HP representative for firmware support levels.

Note: XP and VA support will officially be released in December 2003.

StorageWorks NAS b3000v2 Storage Rules

The StorageWorks NAS b3000v2 supports MSA, EVA3000, EVA5000, and VA arrays. See the individual storage array documentation or contact your HP representative for firmware support levels.

Note: Full support of latest array firmware requires the update of Secure Path to 4.0c and the A16 driver for the Emulex HBA.

StorageWorks NAS e7000v2 Storage Rules

The StorageWorks NAS e7000v2 supports XP, VA, MSA, EVA, and MA/RA/ESA/EMA arrays. See the individual storage array documentation or contact your HP representative for firmware support levels.

Note: Full support of latest array firmware requires the update of Secure path to 4.0c and the A16 driver for the Emulex HBA.

StorageWorks NAS 8000 Storage Rules

The StorageWorks NAS 8000 supports SAN storage using the RA8000, MA8000, ESA12000, EMA12000, Enterprise Virtual Array 5000, HP Virtual Array 7xxx series, and XP series disk arrays. Recommended firmware versions are as follows:

- XP FW is 21.05.06 (for Tru64 FW is 21.04.32)
- VA 7x00 FW is HP18
- VA 7x10 FW is A100
- EVA5000 v2 FW is v2.002
- EVA5000 v3 FW is v3.000
- MA/RA/ESA/EMA FW is V87F-0

The StorageWorks NAS 8000 supports SAN storage using the Enterprise Virtual Array 5000.

The StorageWorks NAS 8000 can access storage on a variety of devices within a SAN device, including the HP Virtual Array 71x0 and 74x0 series storage, and HP XP series disk arrays using SecureManager VA or SecureManager XP.

SAN Extension

8

With the advent of extension technologies specifically developed for the transport of data it is now possible to consolidate, simplify, manage and integrate storage Fibre Channel SAN fabrics within the enterprise to further exploit its networking investments and lower the cost to manage global storage.

A SAN extension is considered an Inter Switch Link (ISL) connection between two Fibre Channel switches greater than 500 meters for 1 Gbps Fibre Channel switch pair or greater than 300 meters for a 2 Gbps Fibre Channel switch pair. Whether it's called SAN Extension, SAN Bridging or SAN Mirroring, HP seamlessly integrates these new technologies into the benefits of today's Fibre Channel SAN.

This chapter describes the current HP supported technologies and products available that provide SAN Extension in non-Continuous Access or non-DRM topologies. If disaster recovery protection extension is necessary, please read the section SAN/Continuous Access EVA Integration or SAN/DRM Integration in Chapter 4, and refer to the *HP StorageWorks Continuous Access And Data Replication Manager SAN Extensions* available at:

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

This chapter covers the following major topics:

- Why Extend the SAN?
- Supported SAN Extension Technologies
- Fibre Channel Long Distance Technologies
- TCP/IP Data Protocol Technologies
- IP Network Considerations
- HP StorageWorks SR2122-2 IP Storage Router

Why Extend the SAN?

The growing need for storage data that is permeating the business community, coupled with the available bandwidth afforded by IP networks or WDM, for example, are making SAN extension an increasingly attractive option to grow the storage network. With SAN extension, end users can connect to data centers at opposite ends of a campus, metropolitan, and wide-area environment. The challenge is to do so at full-wire speed, with the same reliability and availability as the storage traffic within each data center.

Supported SAN Extension Technologies

Currently, HP supports the following technologies for Fibre Channel ISL SAN extension.

- Fibre Channel Long Distance Technologies
  - — Long Wave Transceivers
  - — Wavelength Division Multiplexing (WDM)
- TCP/IP Data Protocol Technologies
  - — Fibre Channel over Internet Protocol (FCIP) using the SR2122-2 IP Storage Router and C-Series MDS IP Storage Services Module

Supported SAN Bridging Technology

- iSCSI to Fibre Channel Bridging using the SR2122-2 IP Storage Router

---

Note: Not all technologies are supported by all HP Fibre Channel switch product lines. Please read each technology description for further details.

Fibre Channel Long Distance Technologies

Long Wave Transceivers

Fibre Channel switches use two types or styles of fiber-optic transceivers that come in both short wave and long wave varieties. The 1-Gbps transceivers use “SC” style connectors that are known as Giga-Bit Interface Converters, or GBICs for short. The 2 Gbps transceivers use the “LC” style connectors that are known as Small Form Factor Pluggable transceivers, or SFP. Long wave GBIC or SFP transceivers are required to go beyond the 500 meter limit for 1 Gbps and the 300 meter limit for 2 Gbps links respectively. There are long-wave optical transceivers that are capable of transmitting up to 100 kilometers.

Currently HP supports the following long wave transceivers

- 10 kilometer GBIC
- 100 kilometer GBIC
- 10 kilometer SFP
- 35 kilometer SFP

Long wave transceivers are supported on HP B-Series, HP C-Series, and HP M-Series product lines. C-Series products currently only support 10 kilometer SFPs.

Wavelength Division Multiplexing

Wavelength Division Multiplexing devices can be used to extend the distance between two Fibre Channel switches. These devices are transparent to the switches themselves and do not count as an additional hop. The only consideration that should be made to accommodate these devices is to have enough buffer-to-buffer credits in order to maintain line speed performance. Wavelength Division Multiplexing is supported for both 1 Gbps and 2 Gbps. This technology is ideally suited for metro data center deployments. When designing SAN extension across an optical ring, buffer-to-buffer credits becomes a very important consideration. In many WDM ring designs, the recovery path due to a link failure can be significantly longer distance than the primary path due to routing the traffic in the opposite direction around the ring. It is important to consider the distance over primary and recovery paths to ensure enough buffer-to-buffer credits exist for both so as not to impede performance during a ring fault event.

Refer to the individual switch product line WDM sections in this chapter for additional information about WDM support.

Note: SAN extension using WDM is supported on all WDM devices listed in the CA/DRM SAN Extension Reference Guide. Refer to ftp://ftp.compaq.com/pub/supportinformation/techpubs/user_reference_guides/aa-ru5cb-te.pdf.

Maintaining Performance beyond 5 or 10 kilometers

A primary consideration with extended fabrics is maintaining the performance of the Inter Switch Link - connection(s) between a pair of switches. The flow control mechanism for a Fibre Channel connection is buffer-to-buffer credits. The number of credits a port has is equal to the number of frames a port can transmit before getting an acknowledgement that the frame was received.

At the speed of light in a fiber-optic cable, it takes a full second for light to travel 200,000 kilometers or 5 microseconds per kilometer. If you calculate the time it takes a frame to travel 100 kilometers and for the "RRDY" (frame acknowledgement) to travel back the same 100 kilometers at 1 Gbps you need about 60 buffer-to-buffer credits to keep the link running at full speed. The rule-of thumb in Fibre Channel is that to sustain 1 Gbps of bandwidth for full 2148B frames approximately one buffer-to-buffer credit is required for every 2 km of distance between two interfaces on a link. For a 2 Gbps link, one buffer-to-buffer credit is required for every 1 km of distance between two interfaces on a link. For smaller frame sizes, the number of buffer-to-buffer credits that are required increases.

There are different limits on the extended link parameters as well as the maximum number allowed across all HP switch product lines. In addition, the commands to configure the buffer-to-buffer credits for each switch product line also vary. The following sections detail these limits and the procedures for configuring extended links for each of the HP switch product lines.

HP B-Series product line

Extended Fabric Limits using WDM

WDM is supported on both 1 Gbps and 2 Gbps switch models.

The maximum number of hops allowed in an B-Series product line Fabric is 7, with a maximum total distance of 160 kilometers across the SAN between any two devices.

Extended Fabric Compatibility Support

HP has three series of switches in the B-Series product line as listed below; these switches can be divided into two classes based on the internal ASIC technology used in the switch. The two classes are switches limited to 1 Gbps and those that are 2 Gbps capable.

- StorageWorks 1 Gbps SAN switch series with version 2.x installed,
- StorageWorks 2 Gbps SAN switch series with version 3.x installed, or
- HP StorageWorks SAN switch 2/32 and Core switch 2/64 switches with version 4.x installed.

An extended fabric link (a link >5 km at 2 Gbps or >10 km at 1 Gbps) can only exist between two switches of the same technology, meaning a B-Series 1 Gbps only switch can only have an extended fabric link to another B-Series 1 Gbps only switch. Likewise a B-Series 2 Gbps capable switch can only have an extended fabric link to another B-Series 2 Gbps capable switch regardless of the link speed.

ISL connections up to 10 km are supported between 1Gbps only and 2Gbps capable switches at the "L0" portcfglongdistance setting only.

“portcfglongdistance” Settings

Extended Fabric optimizes the internal buffering algorithm for StorageWorks switches, which results in line speed performance of close to full Fibre Channel speed. The “portcfglongdistance” setting is used to configure the port with the appropriate amount of buffers based on the speed and distance of the extended link.

The possible settings are:

- L0: 1 Gbps links up to 10 kilometers or 2 Gbps links up to 5 kilometers
  No Extended Fabric license required
- LE: 2 Gbps links between 5 and 10 kilometers
  No Extended Fabric license required
- L0.5: Extended links greater than 10 kilometer but not more than 25 kilometers.
  Extended Fabric license required
- L1: Extended Links greater than 10 kilometer but not more than 50 kilometers
  Extended Fabric license required
- L2: Extended Links greater than 50 kilometer but not more than 100 kilometers
  Extended Fabric license required

These port settings modify the number of Buffer-To-Buffer credits a particular port is allocated and there are limited numbers of these credits available. Buffer-To-Buffer credits are allocated to a group of 4 ports or what is referred to as a "Quad". A quad consists of ports 0 through 3, 4 through 7, 8 through 11, 12 through 15 and so on.

The following table lists the configuration limits for a "Quad".

Table 45: Long Distance Port Matrix

Fabric OS	Speed	Port A	Port B	Port C	Port D
HP StorageWorks FOS versions: 2.x	1 Gbps	L2	E/L1	LE/L0.5/Fx	Disabled
	1 Gbps	L2	L0.5	L0.5/LE/Fx	Disabled
	1 Gbps	L2	L0.5	LE/Fx	LE
	1 Gbps	L2	LE/Fx	LE/Fx	LE/Fx
	1 Gbps	E/L1/L0.5/ LE/Fx	E/L1/LE/L0.5/ Fx	E/L1/LE/L0.5/ Fx	E/L1/LE/L0.5/ Fx
	1 Gbps	LD	LD	LD	LD
HP StorageWorks FOS versions: 3.0, 3.0.1, 3.0.2, 4.0, 4.0.2	1 Gbps	L2	E/L1	Fx	Disabled
	1 Gbps	L2	Fx	Fx	Fx
	1 Gbps	E/Fx/L1	E/Fx/L1	E/Fx/L1	E/Fx/L1
HP StorageWorks FOS versions: 3.0, 3.0.1, 3.0.2, 4.0, 4.0.2	2 Gbps	L2	Disabled	Disabled	Disabled
	2 Gbps	L1	L1	Disabled	Disabled
	2 Gbps	L1	E	E/LE/Fx	Disabled
	2 Gbps	L1	LE/Fx	LE/Fx	Fx
	2 Gbps	E/LE/Fx	E/LE/Fx	E/LE/Fx	E/LE/Fx
HP StorageWorks FOS Version: 3.1 and 4.1	1 Gbps	L2	E/L1	LE/L0.5/Fx	Disabled
	1 Gbps	L2	L0.5	LE/L0.5/Fx	Disabled
	1 Gbps	L2	L0.5	LE/Fx	LE
	1 Gbps	L2	LE/Fx	LE/Fx	LE/Fx
	1 Gbps	E/L1/L0.5/ LE/Fx	E/L1/L0.5/LE/ Fx	E/L1/L0.5/LE/ Fx	E/L1/L0.5/LE/ Fx
	1 Gbps	LD	LD	LD	LD

Table 45: Long Distance Port Matrix (Continued)

Fabric OS	Speed	Port A	Port B	Port C	Port D
HP StorageWorks FOS Version: 3.1 and 4.1	2 Gbps	L2	E	Fx	Disabled
	2 Gbps	L2	LE/Fx	LE/Fx	Disabled
	2 Gbps	L2	L0.5	Disabled	Disabled
	2 Gbps	L1	L1	Disabled	Disabled
	2 Gbps	L1	E	E/LE/Fx	Disabled
	2 Gbps	L1	LE/Fx	LE/Fx	Fx
	2 Gbps	L1	L0.5	LE/Fx	Disabled
	2 Gbps	L0.5	L0.5	L0.5	Disabled
	2 Gbps	L0.5	E/L0.5/LE/Fx	E/LE/Fx	Disabled
	2 Gbps	L0.5	E/L0.5/LE/Fx	LE/Fx	LE/Fx
	2 Gbps	L0.5	E/LE/Fx	E/LE/Fx	LE/Fx
	2 Gbps	E/LE/Fx	E/LE/Fx	E/LE/Fx	E/LE/Fx
	2 Gbps	LD	LD	LD	LD

Fx = Fabric port L0, LE, L0.5, L1, L2 = Inter Switch Links

Fabric Long Distance Bit Setting

The Fabric Long Distance Bit needs to be set on all switches in the fabric when any pair of StorageWorks 1 Gbps SAN series switches has an extended link greater than 10 kilometers (portcfglongdistance = L0.5, L1, or L2). This bit sets fabric wide parameters so that all switches know how to use the legacy method to calculate the number of buffer-to-buffer credits.

Whenever a pair or pairs of StorageWorks 2 Gbps SAN series or an HP StorageWorks core switch 2/64 switches have a port configured for LE, L0.5, L1, or L2 then the Fabric Long Distance Bit must be off. In other words you cannot have an extended link of greater than 10 kilometers between a pair of StorageWorks 1 Gbps SAN series switches and an extended link greater than 5 kilometers between a pair of StorageWorks 2 Gbps SAN series or an HP StorageWorks core switch 2/64 switches in the same fabric.

You can have extended links of up to 10 kilometers (portcfglongdistance = L0) between a pair of StorageWorks 1 Gbps SAN series switches and any length extended link between a pairs of StorageWorks 2 Gbps SAN series or an HP StorageWorks core switch 2/64 switches in the same fabric. Likewise you can have an extended link over 10 kilometers between StorageWorks 1 Gbps SAN series switches as long as there are no Inter Switch Link (ISL) connections greater than 5 kilometers between a pairs of StorageWorks 2 Gbps SAN series or an HP StorageWorks core switch 2/64 switches in the same fabric.

HP C-Series Product Line

Extended Fabric Limits using WDM

WDM is supported on all C-Series switches at both 1 Gbps and 2 Gbps speeds.

The maximum number of hops allowed in C-Series product line fabric is 3, with a maximum total distance of 160 kilometer across the SAN between any two devices.

For C-Series Fibre Channel switches, HP offers a Coarse Wave Division Multiplexing (CWDM) solution. CWDM is a technology involving similar concepts as Dense Wave Division Mulitplexing (DWDM) but is less expensive, less expandable (8 channels max) and works over a shorter distance of 100Km. CWDM allows up to eight 1Gbps or 2Gbps channels (or colors) to share a single fiber pair. Each channel uses a different color or wavelength transceiver. These channels are networked with a variety of wavelength specific add-drop multiplexers to enable an assortment of ring or point-to-point topologies. A typical CWDM SFP can reach up to ~100 km in a point-point topology or around 40 km in a ring topology.

Refer to Cisco switch product documentation on the HP Storage web page for more information.

Extended Fabric Compatibility Support

All C-Series switches are compatible from a functionality perspective. The long distance Fibre Channel connection can be formed between two C-Series directors, Two C-Series MDS 9200 Series fabric switches, or a combination of a 9500 Series director and a 9200 Series fabric switch. All C-Series products support up to 255 buffer-to-buffer credits for extended distance configurations.

In C-Series, each port on the 16-port line card supports 255 buffer-to-buffer credits that are available on a per-port basis for an ISL when using either a single link or a link aggregated via Port Channel. A Port Channel forms a logical ISL and can bundle up to 16 x 2Gbps links to form a single 32 Gbps link. All links within the Port Channel must be the same speed.

HP M-Series Product Line

Extended Fabric Limits using WDM

WDM is supported on both 1 Gbps and 2 Gbps switch models.

The maximum number of hops allowed in a M-Series product line Fabric is 3, with a maximum total distance of 160 kilometers across the SAN between any two devices.

HP StorageWorks edge switch 2/24 Limits

The HP StorageWorks edge switch 2/24 has a fixed buffer-to-buffer credit setting and are limited in which ports can support links beyond the 500 meter limit for 1 Gbps and 300 meter limit for 2 Gbps links.

Ports 0 through 3 are capable of supporting distances up to 20 kilometers at 1 Gbps and up to 10 kilometers at 2 Gbps per second.

Ports 4 through 23 do not have enough buffer-to-buffer credits to support long wave SFP transceivers and are limited to the short wavelength SFP transceiver limits of 500 meters at 1 Gbps or 300 meters at 2 Gbps.

10-100km Port setting

In order to maintain line speed performance of close to full Fibre Channel speed for extended lines over 10 kilometers it is necessary to configure the applicable ports for 10-100km setting. Using the High Availability Fabric Manager (HAFM) select the configure ports menu option and then click on the 10-100 km box for the applicable ports. This will increase the number of buffer-to-buffer credits from 16 to 60 for the selected port.

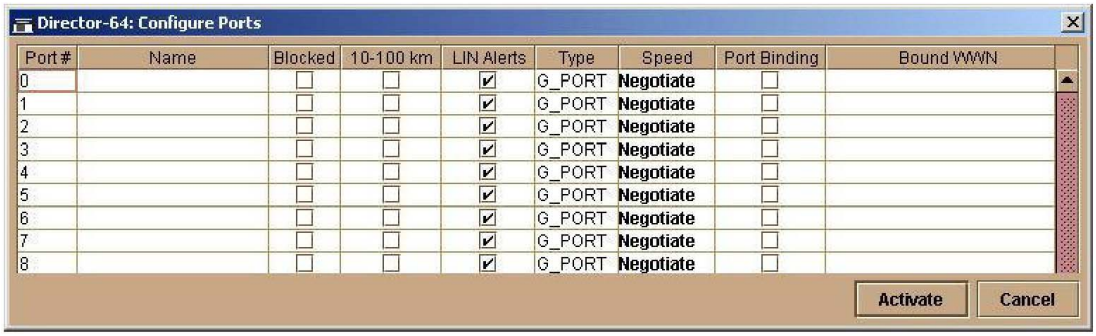


Figure 45: HAFM Configure Ports for 10-100 km setting

TCP/IP Data Protocol Technologies

Fibre Channel over Internet Protocol (FCIP)

FCIP is a protocol that encapsulates Fibre Channel frames into IP packets and tunnels them through an existing IP network infrastructure to transparently connect two or more SAN fabrics together. The IP tunnel acts as a dedicated link to transmit the Fibre Channel data stream over the IP network, while maintaining full compatibility with the Fibre Channel SAN.

FCIP Gateways perform Fibre Channel encapsulation process into IP Packets and reverse that process at the other end.

FC Switches connect to the FCIP gateways through an E_Port for SAN fabric extension to remote locations.

A tunnel connection is set up through the existing IP network routers and switches across LAN/WAN/MAN.

This example shows a configuration that connects FC SANs using an Internet Protocol (IP) intersite link.

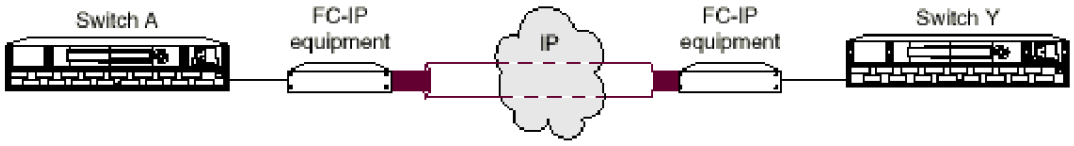


Figure 46: Connecting Fibre Channel SANs with an IP link

Using Internet Protocol over an IP-based network, FCIP can link sites over any extended distance. Local SANs are connected through an IP network to create an extended SAN. An FC-IP gateway is used at each end of the intersite link. Each FC-IP gateway box encapsulates received FC frames into IP packets for transmission over the IP network. Similarly, the FC-IP box extracts the original FC frame from received IP packets and retransmits them to the destination FC node. The FC-IP boxes also handle IP-level error recovery.

FCIP Products supported for Heterogeneous SAN Extension

The HP StorageWorks SR2122-2 IP Storage Router provides heterogeneous SAN FCIP extension support on HP Series B-Series and M-Series Fibre Channel switches.

The Cisco MDS 9000 IP Storage Services Module is supported with C-Series product line switches

The SAN Valley SL700/SL1000 IP-SAN Gateways are supported with B-Series and M-Series product line switch models for heterogeneous SAN FCIP extension. Please read the manufacturers documentation for further configuration details.

IP Network Considerations

Considerations Relevant to Using the Existing IP Network

The ability to use your existing network with FC-IP depends on the type of storage I/O you plan to do and the traffic already existing on your current network. The key consideration is whether you have enough unused/available bandwidth from your network to continue the current network load, accommodate future growth, and handle FCIP SAN load demands.

Table 46: IP Network Issues to Consider

Storage I/O Type	Use Existing IP Network?	Factors
Mirrored I/O or continuous I/O throughput over the FCIP intersite link.	A separate network is recommended.	For peak performance for your current network, and for peak Storage I/O performance a separate network is recommended.
Data Migration or Adhoc Data Updates	The use of your existing network may be possible.	Data migration is a one-time movement of data for upgrade or maintenance purposes. Adhoc Data Updates is more of a 'burst' of data from one site to another for remote backups, database content delivery, etc. It is possible to use your existing network, however the network performance may be significantly affected.

Network Speeds

In general, the FC-IP equipment supports Ethernet speeds of 10/100 Mb/s, and 1 Gbps (Gigabit Ethernet). The network connection should be selected to match the amount of data to be transferred.

The speed of light through fibre is approximately 200,000 kilometers per second or 5 microseconds to travel one kilometer.

Network Distance Considerations

The HSG80 controller uses SCSI protocol to manage the storage devices. Before a SCSI I/O can be transmitted, it must be encapsulated into Fibre Channel frames. Because of SCSI protocol, a minimum of 4 trips over the long-distance link is required.

These trips conceptually:

1. Tell the remote site you want to transmit data.
2. Wait for the acknowledgment from the remote site.
3. Send the data to the remote site.
4. Wait for the acknowledgment from the remote site.

When sending data over fiber, the one-way transmission time is approximately 5 microseconds per kilometer. Since a minimum of four trips is required for each SCSI data transfer, this translates to a total transmission delay per command of 20 microseconds per kilometer, or about 32.2 microseconds per mile. For example, if a remote site is located 150 miles away from the local site, the total time will be 4,830 microseconds (4.83 milliseconds) for every data transfer. Since a typical I/O operation on a non-DRM configuration with write-back cache takes approximately 500 microseconds, long distances can have a significant effect on performance.

Note: The above calculations for a link of 150 miles do not include any latency induced by the FC-to-IP conversions, or latency of the routers and switches in the network.

Additional I/Os, either from additional LUNs on the same controller or from a different controller, will require additional bandwidth. Care must be taken to understand this principle. Adding bandwidth to a given link at a given distance will not increase the time it takes to complete an I/O operation. It will, however, allow you to add additional I/Os from different LUNs, thereby consuming the available bandwidth.

Conversely, if enough bandwidth is not given to a link, then the number of I/Os per second will decrease, possibly to the point of failure

---

Note: The time it takes an I/O to complete an operation is more complex than the above example, and there are additional factors involved with this calculation. This discussion is an attempt to help you understand the importance that distance latency has on the time it takes to complete an I/O operation.

Network Distance/Latency Example Calculations

1. **1.0 MB Link**

   Link Bandwidth: 1.0 MB/s

   Write size: 8 KB

   Available bandwidth divided by size of I/O equals maximum I/Os per second:

   $$\frac{\text{1.0 MB/s}}{\text{8 KB per I/O}} = \textbf{125 I/Os per second}$$

2. **50 Miles of Latency**

   Distance: 50 miles (80 kilometers)

   Latency: 8 µs/mile (5 µs/kilometer)

   Write size: 8 KB

   Latency for 1 I/O per mile: 4 trips * 8 µs/mile = 32 µs per mile

   Latency for 1 I/O at 50 miles: 50 miles * 32 µs/mile = 1.6 ms per I/O

   Reciprocal of total latency indicates maximum I/Os:

   $$\frac{1.0}{\text{1.6 ms per I/O}} = \textbf{625 I/Os per second}$$

   I/O's multiplied by size of I/O = bandwidth used:

   625 I/O per second * 8 KB per I/O = **5 MB/s**

3. **150 Miles of Latency**

   Distance: 150 miles (241 kilometers)

   Latency: 8 µs/mile (5 µs/kilometer)

   Write size: 8 KB

   Latency for 1 I/O per mile: 4 trips * 8 µs/mile = 32 µs per mile

   Latency for 1 I/O at 150 miles: 150 miles * 32 µs/mile = 4.8 ms per I/O

   Reciprocal of total latency indicates maximum I/Os:

   $$\frac{\text{1.0}}{\text{4.8 ms per I/O}} = \textbf{208 I/Os per second}$$

   I/Os multiplied by size of I/O = bandwidth used:

   208 I/O per second * 8 KB per I/O = **1.6 MB/s**

In summary, when an IP Network is used in a situation where the local and remote sites are located many miles apart, the speed of light through fiber may cause unacceptable delays in the completion of an I/O transaction. Increasing the amount of available bandwidth cannot solve this problem. Careful consideration must be given to these factors when matching your needs and wants to a particular application.

IP Network Best Practices

Currently most IP networks do not manage bandwidth to each individual connection. As traffic increases due to other demands on the network, bandwidth can be robbed from the FCIP Intersite Link The following techniques can be used to minimize this effect:

- Create virtual private networks (VPNs) with Quality of Service (QoS) through premise routers for the FCIP circuit.
- Create separate physical networks.
- Guarantee the bandwidth using a third-party router/QoS vendor.

As mentioned, distance has a dramatic effect on the amount of work that can be done across a link. Therefore, site planning should include:

- Using the shortest possible distance between remote sites.
- Minimizing the amount data transferred over the FCIP link.
- Designing a plan to add additional storage I/O that will not impact normal data traffic.
- Consider additional controller pairs to effectively use available bandwidth.

IP Storage Services Module

Cisco MDS 9000 Family IP storage (IPS) services modules extend the reach of Fibre Channel SANs by using open-standard, IP-based technology. The switch connects separated SAN islands using Fibre Channel over IP (FCIP). It integrates seamlessly into the Cisco MDS 9000 Family, and supports the full range of features available on other switching modules, including VSANs, security, and traffic management.

The IPS module can be used in any Cisco MDS 9000 Family switch and has eight Gigabit Ethernet ports.

- FCIP-FCIP transports Fibre Channel frames transparently over an IP network between two Cisco MDS 9000 Family switches or other FCIP standards-compliant devices. Figure 47 depicts the FCIP scenarios in which the IPS module is used.
- Simplifies data protection and business continuance strategies by enabling backup, remote replication, and disaster recovery over WAN distances using open-standard FCIP tunneling.
- Improves utilization of WAN resources for backup and replication by tunneling up to 3 virtual Inter Switch Links (ISLs) on a single Gigabit Ethernet port.
- Reduces SAN complexity by eliminating the need to deploy and manage a separate remote connectivity platform.
- Preserves Cisco MDS9000 Family enhanced capabilities including VSANs, advanced traffic management, and security across remote connections.

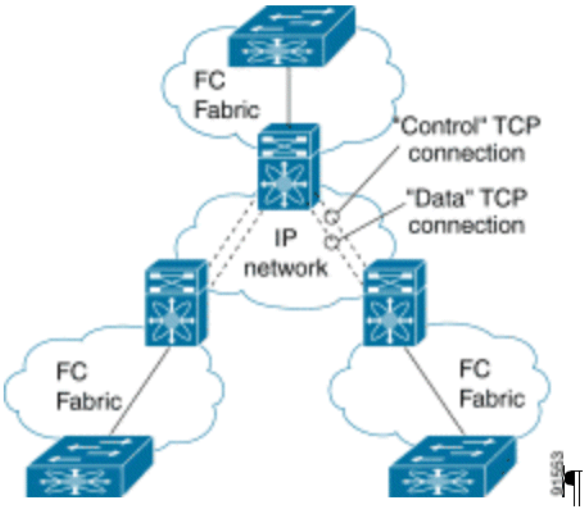


Figure 47: FCIP Scenarios

Table 47: Supported SFPs

Optics	Media	Distance
1-Gbps—SX, LC SFP	50/125 micron multimode	500 m
1-Gbps—SX, LC SFP	62.5/125 micron multimode	200 m
1-Gbps—LX/LH, LC SFP	9/10 micron singlemode	10 km

HP StorageWorks SR2122-2 IP Storage Router

The HP StorageWorks SR2122-2 IP Storage Router offers FCIP SAN extension functionality and iSCSI to Fibre Channel Bridge capability within a single chassis.

The HP StorageWorks SR2122-2 IP Storage Router can be configured to run either in Single-Mode (FCIP or iSCSI Routing only) or in Multi-mode (FCIP and iSCSI Routing concurrently).

IP SR2122 Storage Router Documentation

Further SAN configuration documentation, including:

- HP StorageWorks IP Storage Router 2122-2 Command Line Interface Reference Guide
- HP StorageWorks IP Storage Router 2122-2 User Guide
- HP StorageWorks IP Storage Router 2122-2 Getting Started Guide

is available via the HP website at:

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

HP StorageWorks SR2122-2 IP Storage Router - FCIP Overview

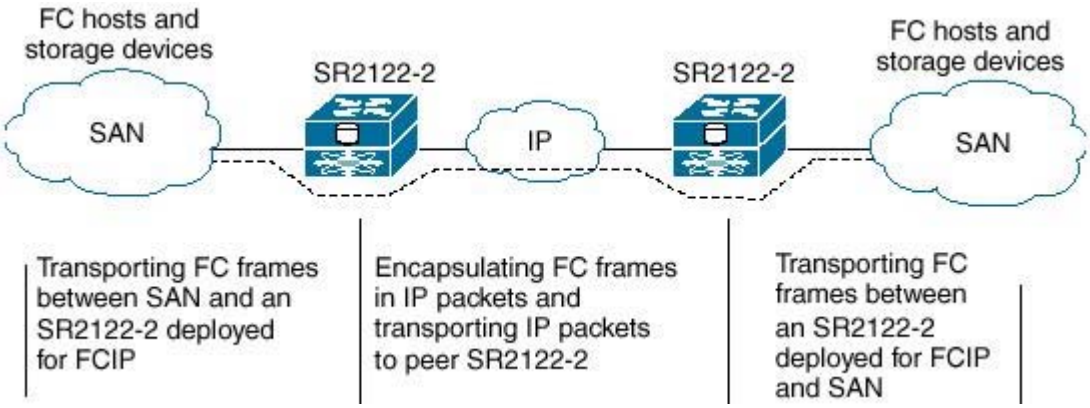
Fibre Channel over IP (FCIP) enables SR2122-2 Storage Routers to provide connectivity between FC hosts and FC storage devices over an IP network. To deploy FCIP, two SR2122-2 Storage Routers are required. Each system is configured for FCIP and connected to a SAN. An FC host or FC device needs no additional hardware or software to access storage devices via an SR2122-2 Storage Router deployed for FCIP.

Note: Refer to Table 24 for a list of devices that are supported for FCIP heterogeneous SAN extension.

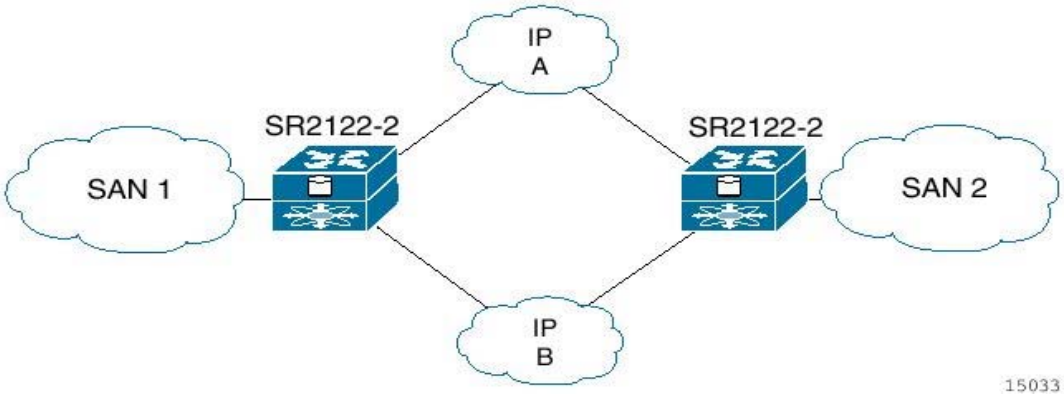
With FCIP, peer systems transport FC frames over an IP network. From the perspective of the SANs the storage devices accessed through the peer systems appear to be part of one unified SAN.

Once configured, FCIP instances, or connections, on each system become active and establish their connectivity via the IP network. The storage devices in one SAN access the storage devices in the connected SAN using FC frames, which are encapsulated in IP packets by the FCIP instance, and transmitted to the peer system. The peer FCIP instance strips the IP packet data and passes only the FC frames over the FC interfaces to the storage devices.

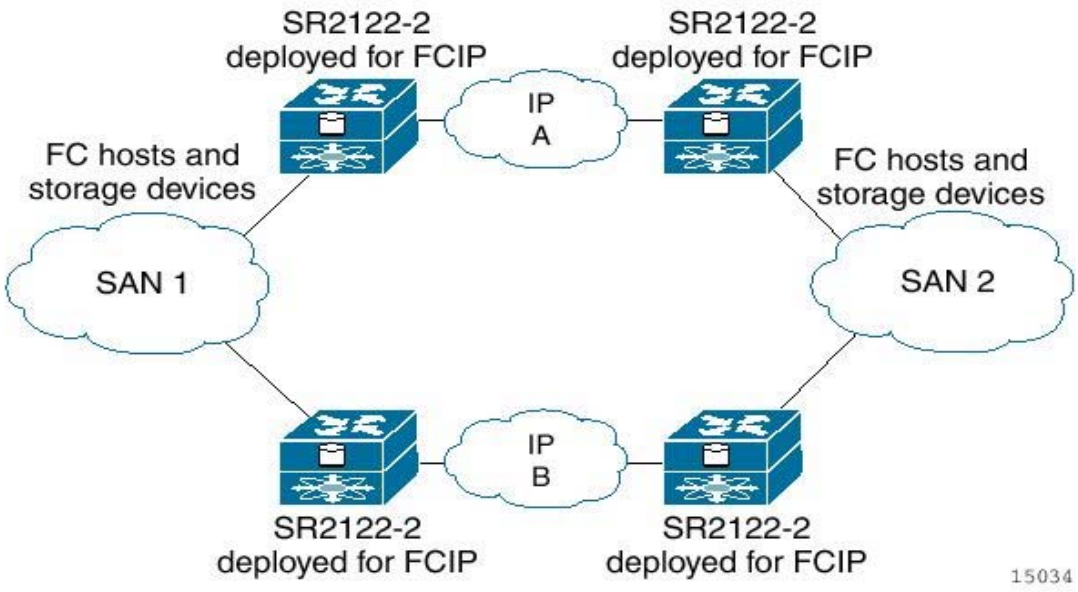
The peer systems are connected to each other through an IP network.



In this example a FC host or FC device connects to one or more Fibre Channel interfaces of each peer SR2122-2 Storage Router deployed for FCIP. Each SR2122-2 connects to the IP network through one of its Gigabit Ethernet interfaces. Through the IP network each FCIP instance accesses its peer, thereby connecting the SANs.



In this example configuration, an FC host or FC device connects to one or more Fibre Channel interfaces of each peer SR2122-2 Storage Router deployed for FCIP, and each SR2122-2 connects to two separate IP networks through each of its Gigabit Ethernet interfaces. Through the IP network, each FCIP instance accesses the peer storage router deployed for FCIP, connecting the SANs. In this configuration, IP A and IP B are redundant paths, so that the loss of connectivity via either path does not cause a loss of connectivity between the SANs.



This example shows an even more reliable FCIP configuration, in which pairs of SR2122-2 Storage Routers provide full redundancy. In this configuration, loss of an SR2122-2 or loss of connectivity through one of the IP networks can be tolerated with no loss of connectivity between the SANs.

Note: For multiple paths between SANs, multiple pairs of systems deployed for FCIP need to be connected to the FC hosts or FC devices. It is assumed that the multipath management is being done by an entity outside the SR2122-2 (for example, by management applications on the FC host or storage devices).

HP StorageWorks SR2122-2 IP Storage Router - iSCSI Overview

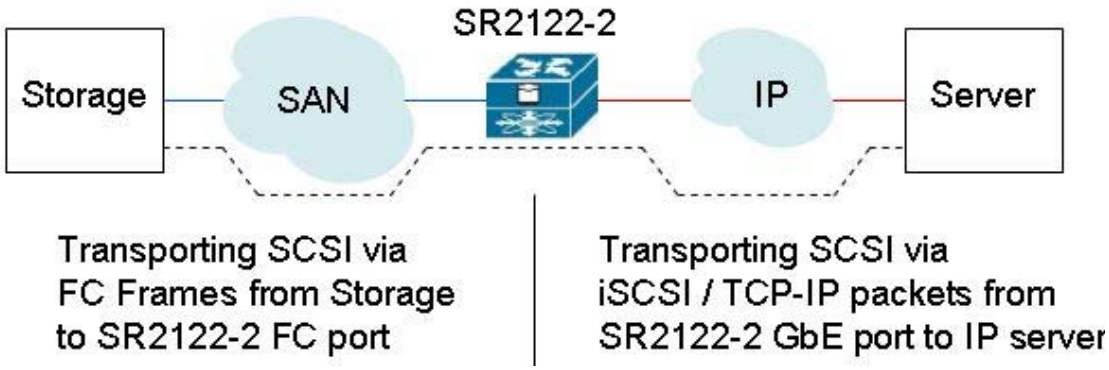
The SCSI transport protocol iSCSI maps block-oriented (CDB) storage data over TCP/IP networks. The iSCSI protocol enables universal access to storage devices and storage-area networks (SANs) over standard Ethernet-based TCP/IP networks.

These networks may be dedicated networks or may be shared with traditional Ethernet applications. IP LAN/WAN routers and switches can be used to extend the IP storage network to the wide area of applications such as synchronous and asynchronous remote disk copy or tape backup and restore.

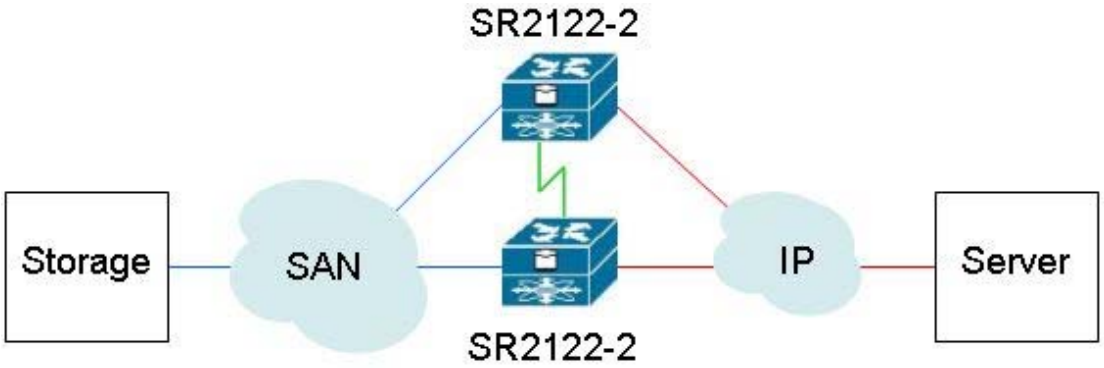
Note: Although the iSCSI protocol is written as a complete data transport from host to storage, this section will only discuss the current HP supported topology of iSCSI hosts to Fibre Channel storage using the HP SR2122-2 IP Storage Router.

SCSI routing provides IP hosts with access to FC storage devices as if the storage devices were directly attached to the hosts, with access to devices being managed primarily in the storage router. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. The iSCSI targets are created and mapped to physical storage devices attached to the storage router. The SR2122-2 presents the iSCSI targets to IP hosts (iSCSI initiators) as if the physical storage devices were directly attached to the hosts.

With SCSI routing, storage devices are not aware of each IP host; the storage devices are aware of the storage router and respond to it as if it were one FC host.



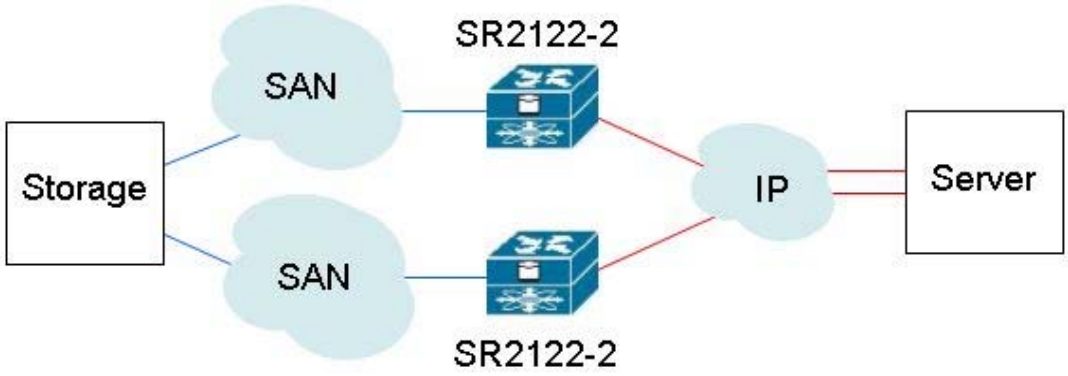
In this example FC storage connects to the Fibre Channel interface of the SR2122-2 Storage Router deployed for iSCSI . The SR2122-2 connects to the IP network through one of its Gigabit Ethernet interfaces. The server accesses the storage served from the router through the IP network.



In this example configuration, two storage routers are connected (clustered) together to allow the storage routers to back each other up in case of failure.

Note: A storage router can participate in a cluster only if it is deployed for SCSI routing.

In a cluster, storage routers continually exchange High Availabilty information to propagate configuration data to each other and to detect failures in the cluster. The storage routers exchange HA information through a separate network connected to the HA interface of each storage router.



This example shows an even more reliable iSCSI configuration in which pairs of SR2122-2 Storage Routers and SANs provide full redundancy. In this configuration, loss of a SR2122-2 or loss of connectivity through one of the SANs can be tolerated with no loss of connectivity between the storage and server.

Note: For multiple paths between SANs, it is assumed that the multipath management is being done by an entity outside the SR2122-2 (for example, by management applications on the FC host such as HP Secure Path).

SR2122-2 Hardware and Software Support

This section lists the hardware, devices, and operating systems that are compatible with this SR2122-2 IP Storage Router.

Storage Array Hardware Support

The following hp Storage Array products are supported:

- MSA1000
- RA/MA8000
- ESA/EMA12000
- EMA16000
- Enterprise Virtual Array
- VA7100
- VA7400/7410
- XP128/1024

Fibre Channel Switch Hardware Support

The SR2122-2 Storage Router is supported with the HP B-Series, C-Series and M-Series product line switches listed in Chapter 3.

Network Interface Controller (NIC) Hardware Support

The following Proliant Server Network Interface Controllers are supported:

- NC6136 Gigabit Server Adapter
- NC7131 Gigabit Server Adapter
- NC7770 PCI-X Gigabit Server Adapter

The following Blade Server Network Interface Controller is supported:

- NC7781 Gigabit Server Adapter

Operating System Software Support

- Microsoft Windows 2000 SP2 with either Microsoft hotfix Q302895 or Q248720 and Microsoft hotfix Q318271, SP3
- Microsoft Windows 2003
- MSCS support (HP iSCSI driver only)
- Red Hat Advanced Server 2.1
- Secure Path (Windows 2000, Windows 2003 only)

Compaq Network Teaming Software Support

- Compaq Network Teaming (Windows 2000, Windows 2003 only)

SR2122 Management Software Support

The following HP management software is supported:

- Compaq Insight Manager 7
- hp OpenView Storage Area Manager (SAM)

iSCSI Initiator Software Support

- HP
- Microsoft (MSCS, Secure Path not supported)

SR2122-2 iSCSI Configuration Rules

SR2122 Router Rules

Table 48: SR2122-2 Router Rules

Router Rule	Maximum
Maximum scsirouter instances per SR2122-2 Router (and per SR2122-2 Router Cluster)	12
Maximum iSCSI host connections per SR2122-2 SCSI Router instance	32
Maximum active logical units (LUNs) per SR2122-2 Router	30
Maximum active targets per SR2212-2 Router	30

- The SR2122-2's 2nd fibre Channel port (FC2) is not supported as a redundant iSCSI SAN port for FC1. FC2 can, however, be configured as a FCIP port
- Direct connect of the SR2122-2 FC ports to any HP storage array is not supported.
- The SR2122-2 Management port must be in a different subnet than the SCSI Router Instances.
- The SR2122-2 fibre channel ports appear as host bus adapters to the FC switches and to all storage arrays.

ISCSI Host Rules

Table 49: ISCSI Host Rules

iSCSI Host Rule	Operating System	Maximum
Maximum targets accessed per iSCSI host	Windows 2000, Windows 2003	30
	Red Hat Linux, HP-UX	4
Maximum active LUNs per target	Windows 2000, Windows 2003, Linux, HP-UX	30

Operating System Rules

- Linux Clustering is not supported.
- hp Secure Path for MSA1000, RA/MA8000, EMA/ESA12000 and for Enterprise Virtual Array for Linux are not supported.
- hp Auto Path for VA/XP for Windows 2000 and Linux are not supported.
- hp Secure Manager on XP and VA is not supported.
- Windows MSCS and Windows Secure Path not supported with the Microsoft iSCSI Initiator

Storage Array Rules

- The HSG80 is supported in both SCSI-3 Transparent Failover Mode and Multiple-Bus Failover Mode.
- Without hp Secure Path the RA8000/MA8000 and the Enterprise Virtual Array is supported with the SR2122 accessing only one controller port. This will disable controller failover protection.
- The MSA1000 is supported with the SR2122-2 accessing only one MSA controller port. This will disable controller failover protection.

Fibre Channel Switch/Fabric Rules

- The SR2122-2 is supported on the HP B-Series, C-Series and M-Series Switches.
- The SR2122-2 should only be zoned with the storage devices that it will access. Zoning theSR2122-2 with other servers is not supported.

Management Software Rules

- hp OpenView Storage Area Manager (SAM) support is limited to property support only. It will identify the device, and by clicking on it, one can launch the device embedded web server interface or telnet. A device specific plug-in for the SR2122 is available on the
- SAM Website.
- CIM 7 Supports the SR2122's SNMP management capabilities.
- Management of the storage arrays through the SR2122 is not supported. Please use the recommended application/element manager to configure the storage array.

SR2122-2 FCIP Configuration Rules

SR2122 Router Rules

- IP network speeds less than 10 Mb/sec are not supported.

- When the SR2122-2 is configured with HP data replication products, two separate long distance links must be implemented.
- If the router is to be configured for both FCIP and iSCSI, then the FCIP and iSCSI traffic is not supported through the same SR2122-2 GbE port.

Sample SR2122-2 Configurations

This section provides a brief overview of three recommended host/storage configuration using the HP SR2122-2 IP Storage Router:

- FCIP Only
- FCIP with Local iSCSI Hosts
- FCIP with Remote iSCSI Hosts

Further SAN configuration documentation, including the

- HP StorageWorks IP Storage Router 2122-2 Command Line Interface Reference Guide
- HP StorageWorks IP Storage Router 2122-2 User Guide
- HP StorageWorks IP Storage Router 2122-2 Getting Started Guide

is available via the HP website at:

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

SR2122-2 Sample Configuration - FCIP Only

Two SAN islands may be joined into a single large, geographically dispersed SAN using the HP SR2122-2s as Fibre Channel to IP gateways to translate between Fibre Channel protocol and FCIP protocol.

FCIP protocol transmitted over a WAN network is used to extend the connection between the two SAN islands beyond the nominal 10 km maximum length for direct Fibre Channel.

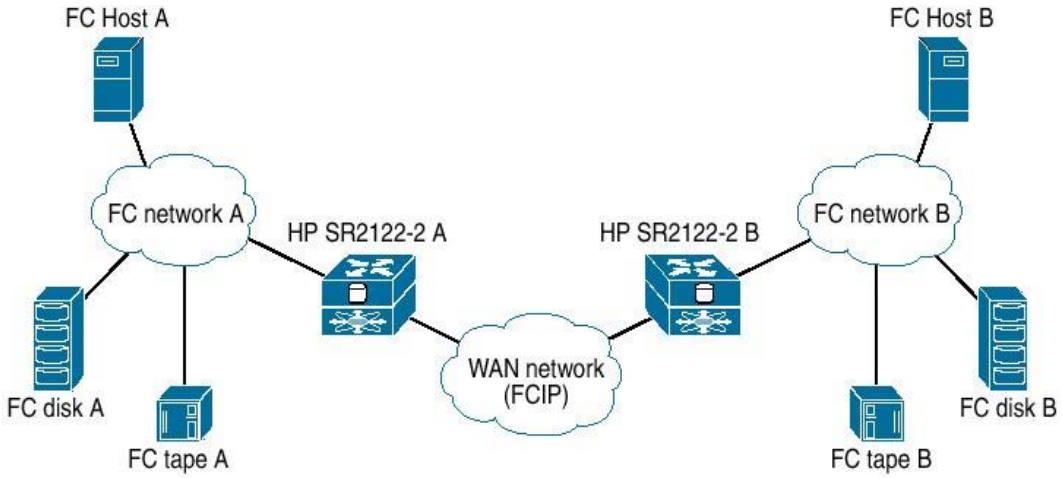


Figure 48: FCIP only

Disk LUNs at either site A or site B may be assigned either to local hosts or to remote hosts.

This basic configuration may also be used when Data Replication Manager or Continuous Access is employed to replicate disk data between the two sites. Since these data replication products use redundant Fibre Channel fabrics, two separate long distance links must be implemented. Although the two Fibre Channel fabrics could be routed through only two SR2122-2s, to avoid a single point of failure, a total of four SR2122-2 units should be included in this configuration.

As shown in Figure 48, a single Fibre Channel connection is required between the SR2122-2 and the Fibre Channel network at each site. The second Fibre Channel port on the SR2122-2 is not used. The iSCSI protocol is not used in this configuration.

SR2122-2 Sample Configuration - FCIP with Local iSCSI Hosts

One or more host servers may be connected to the extended SAN through a local IP network at site A using the iSCSI protocol. This connection uses the second Gigabit Ethernet port on the site A SR2122-2.

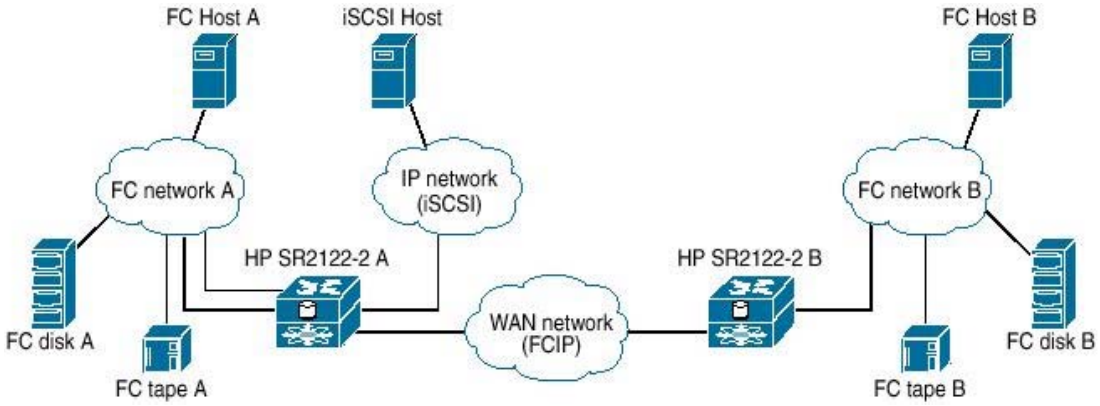


Figure 49: FCIP with Local iSCSI Hosts

For this configuration, two connections from the SR2122-2 to the Fibre Channel network at site A are required. One SR2122-2 Gigabit Ethernet (Fibre Channel) port is assigned to the FCIP connection and the second is designated for the iSCSI connection.

Disk LUNs at site A may be assigned to the iSCSI hosts. The SR2122-2 translates the iSCSI I/O commands into Fibre Channel protocol commands. The iSCSI hosts at site A are also able to access the disk LUNs at site B. The iSCSI protocol I/O commands are converted to FCIP protocol in the site A SR2122-2 and transmitted to site B using FCIP. The iSCSI host applications must be able to tolerate the total latency incurred through the multiple protocol conversions plus the overall network delay to access disk LUNs at site B. A further expansion of this configuration would be to mirror the site A iSCSI configuration to include iSCSI hosts at site B. This would provide access to site B disk LUNs, as well as site A disk LUNs, through the SR2122-2 at site B.

SR2122-2 Sample Configuration - FCIP with Remote iSCSI Hosts

The FCIP configuration with local iSCSI hosts may be extended by locating the iSCSI hosts apart from either site A or site B. This configuration requires that the iSCSI IP network be connect to the large SAN through a WAN network as shown below.

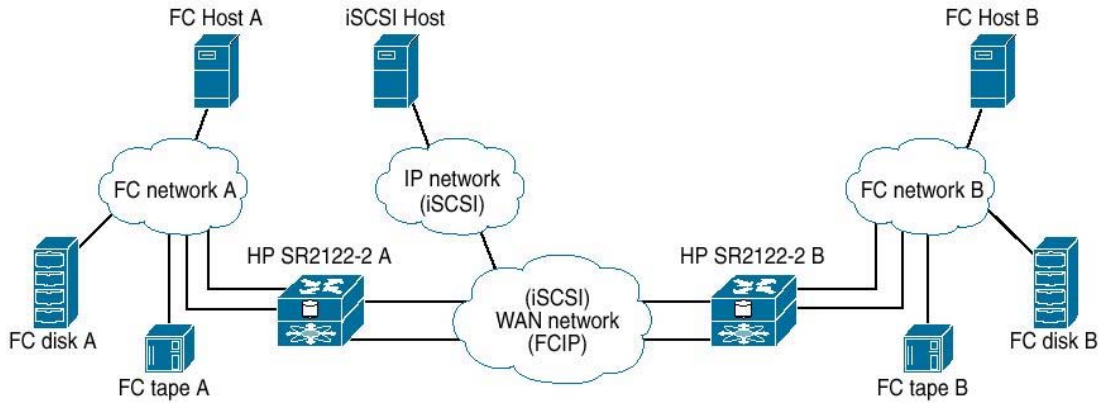


Figure 50: FCIP with Remote iSCSI Hosts

This configuration allows the iSCSI hosts to access disk LUNs at either site A or site B, providing maximum configuration flexibility.

Note: Within the WAN network the iSCSI protocol traffic is kept isolated from the FCIP protocol traffic and connects to the SR2122-2s through the second Gigabit Ethernet port on each gateway.

The SR2122-2 has the capability to rate-limit or "pace" the FCIP protocol traffic that it handles. This is accomplished using standard Fibre Channel flow control mechanisms that allows the user to limit the amount of FCIP traffic through the SR2122-2 so that it does not exceed the bandwidth allotted for this connection through the WAN network.

However, the iSCSI protocol traffic has no corresponding flow control mechanism. If the iSCSI protocol traffic and the FCIP protocol traffic are combined on a single network and if the combined traffic exceeds the available network bandwidth, the iSCSI protocol traffic can theoretically consume some or all of the bandwidth allotted to the FCIP connection. If that happens, both iSCSI and FCIP I/O commands are subject to failure due to dropped packets in the WAN network.

By isolating the iSCSI protocol from the FCIP protocol using separate network connections, it is possible to prevent a failure in the FCIP portion of the system due to over-subscription of the WAN connection.

Sample Configurations

For maximum supported SAN and Storage configurations, see Chapter 3 and Chapter 4.

For maximum supported IP configurations please consult with your network administrator

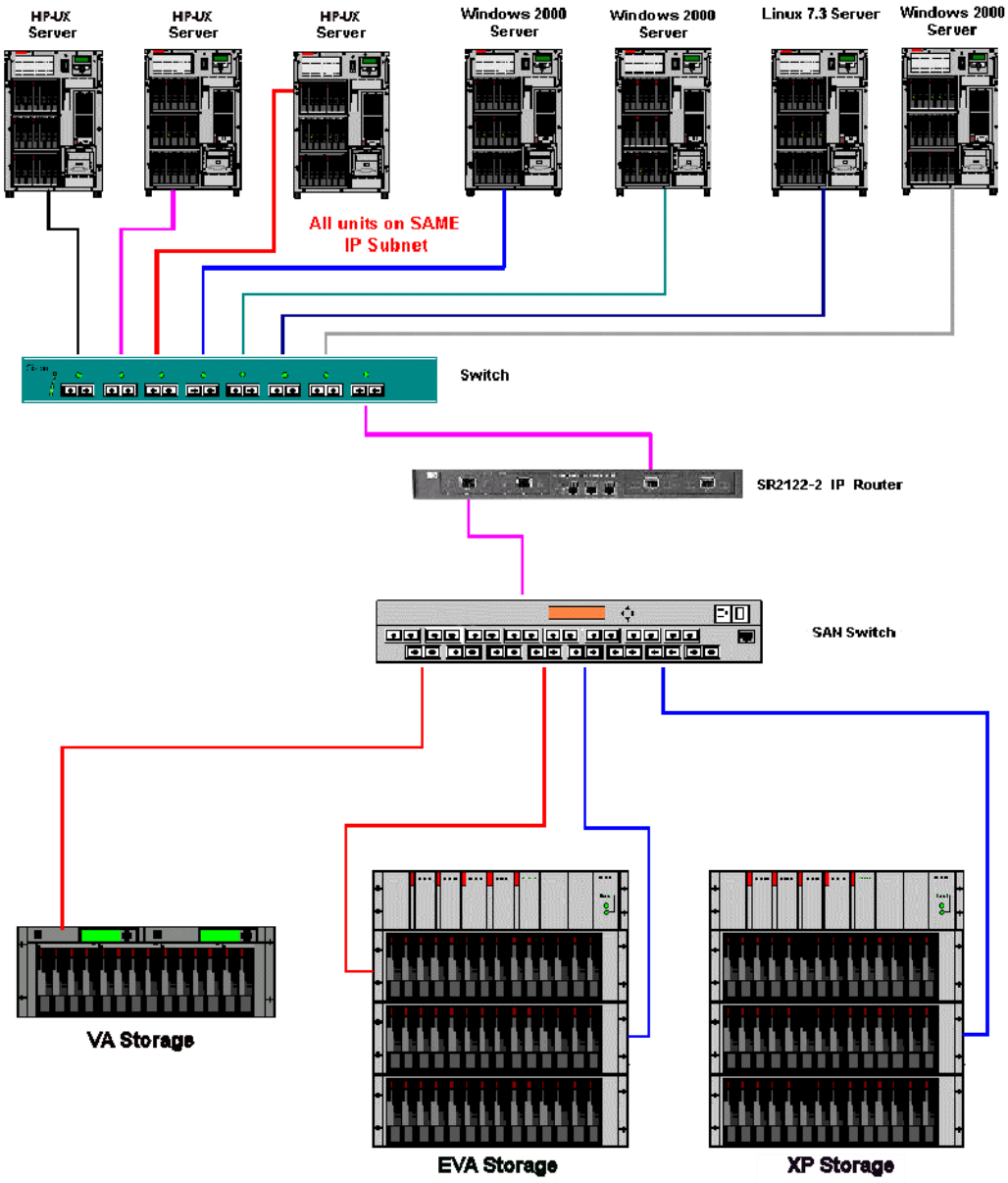


Figure 51: Example of Multiple OS Systems in a Non-Redundant Path Configuration

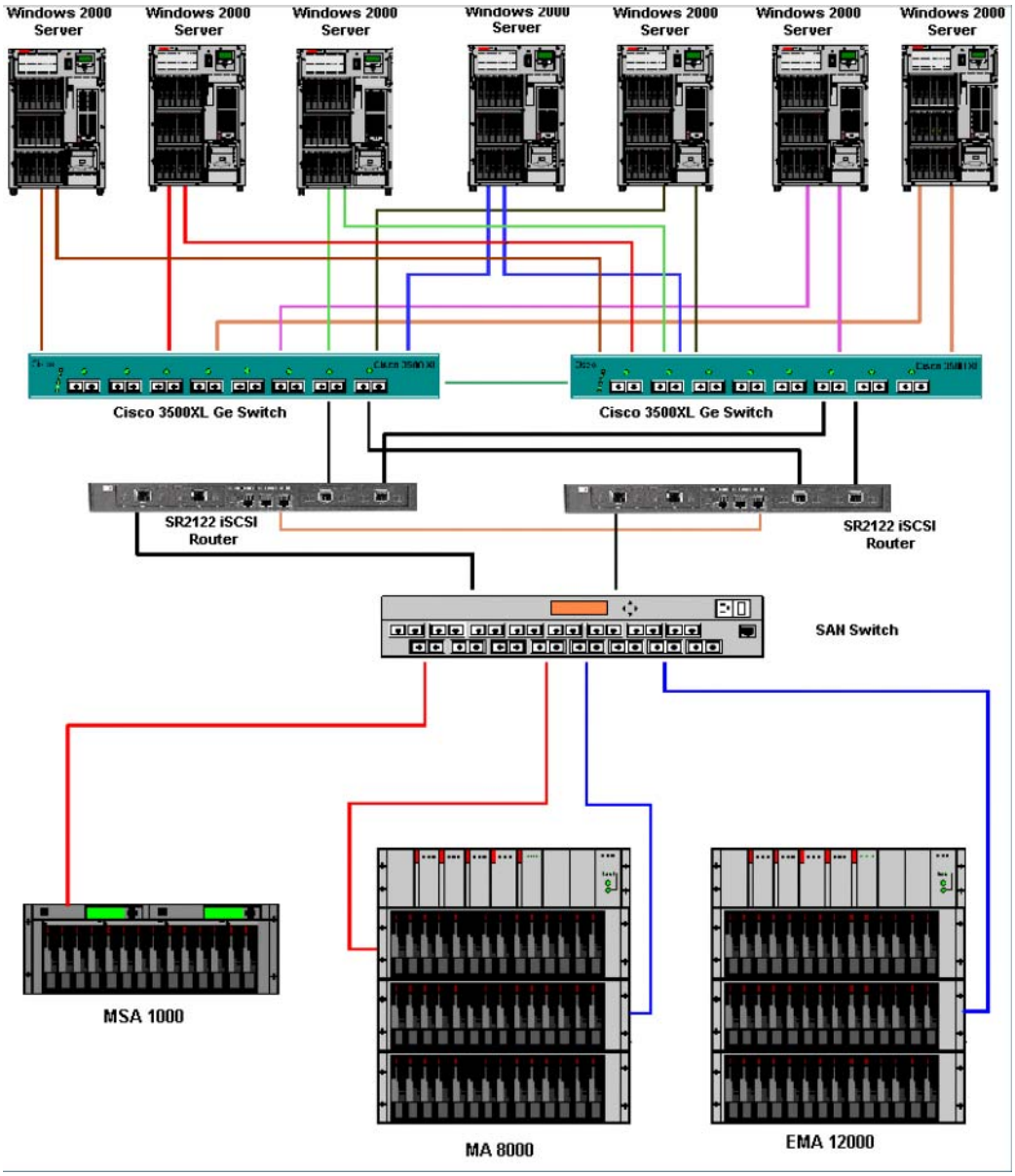


Figure 52: Windows 2000 Servers with NIC Teaming: 2 Node SR2122-2 Cluster

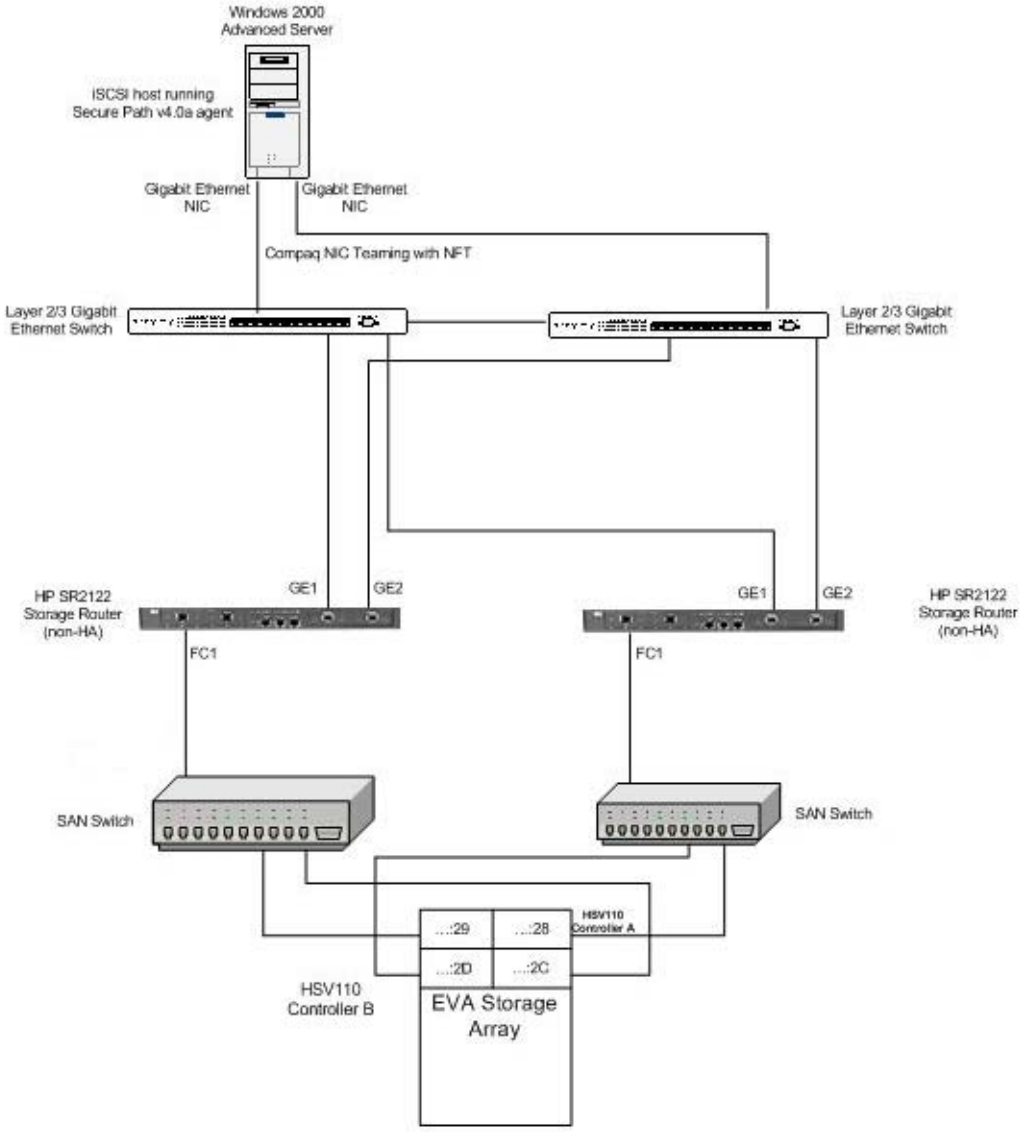


Figure 53: Secure Path Configuration

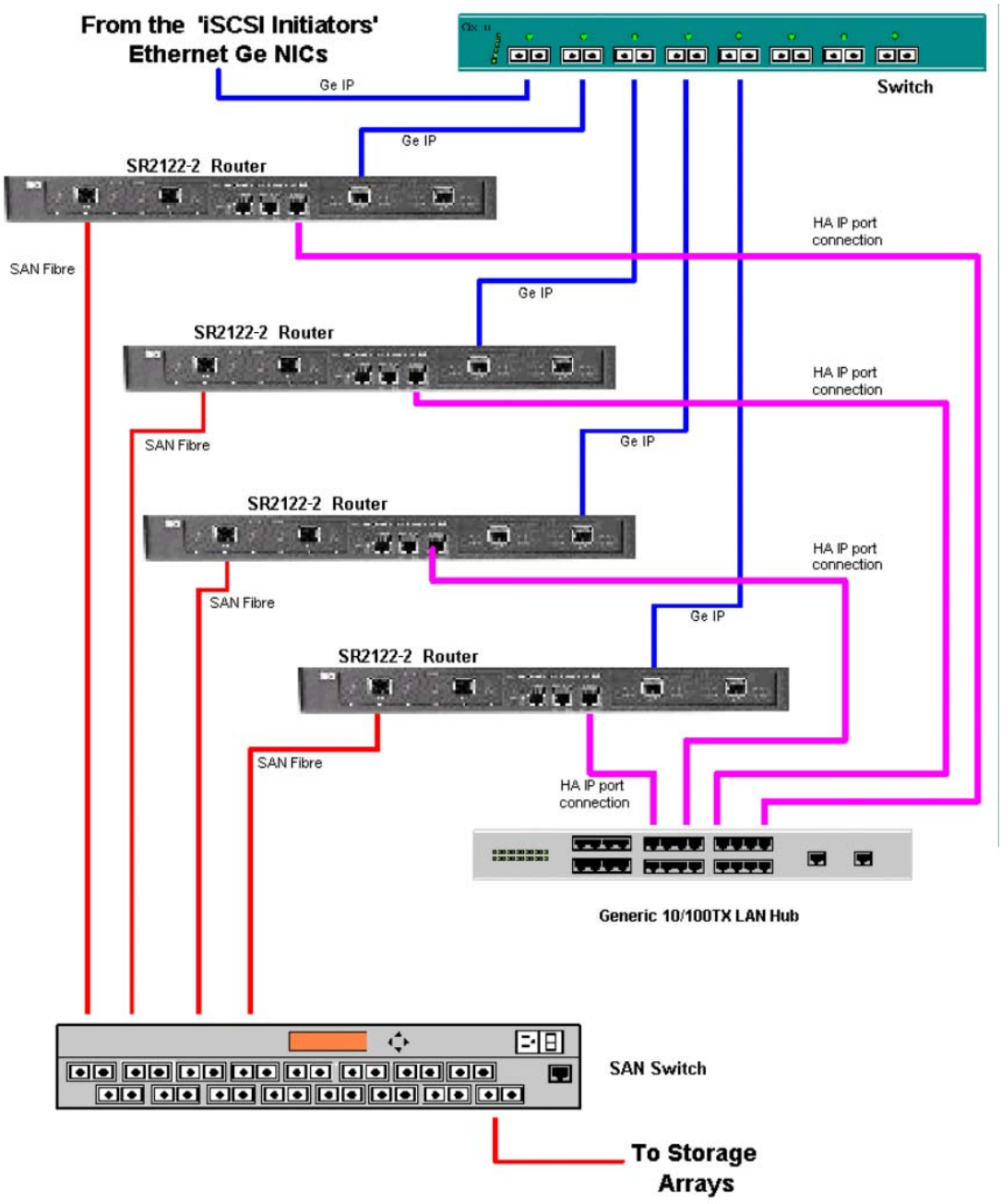


Figure 54: Maximum SR2122-2 Cluster Configuration Using HA Ports

SAN Security

9

Information security is a fundamental issue that must be dealt with while managing any data center. HP understands the importance and complexity of establishing and maintaining a secure information storage environment. HP storage products are designed to make it easy to protect the availability, integrity, and confidentiality of the customer data that they hold.

HP is working with other storage vendors in the Storage Networking Industry Association to develop enhanced SAN security technology. Refer to: http://www.snia.org/tech_activities/storage_security for additional information.

HP is also working with the Fibre Channel standards community to develop storage network security protocols. Refer to http://www.t11.org for information on the Fibre Channel Security Protocols (FC-SP) project.

This chapter describes storage aspects of information security in a StorageWorks SAN environment. Major topics covered in this chapter include:

- Basic Security Model
- Summary of SAN Security Practices
- Security Features of HP StorageWorks SAN Components
- Storage System
- Storage Security in an Enterprise Environment
- Storage Security in a Service Provider Environment
- Storage Security in a Secure Environment

Basic Security Model

The ideal mass storage system provides fast storage and retrieval of information for a number of servers.

This one line summary leaves unspoken a number of additional expectations: It is expected that data written to the storage system today will be available tomorrow. It is expected that the data will be the same when it's read as it was when it was written. And it's expected that the data is not available to any server or any person not specifically authorized to have access. These three possibilities are covered under the general headings of availability, integrity, and confidentiality.

These additional expectations form the basis for defining the availability and security of the data in the mass storage system. For example, the data should be available even if a hardware or software component in the storage system fails: RAID and remote mirroring technology are methods used to maximize data availability.

Three types of attacks, corresponding to the three aspects of information security, can be made on a computer system. Data can be made unavailable for access. Data can be deleted or modified without permission. Data can be examined without permission. Any computer security system must deal with these types of attacks.[1]

The security of a computer system is the responsibility of a Security Manager. This person defines the operational rules and procedures that are required to maintain the desired security level. To achieve the desired security level in an HP SAN system, the operational rules and procedures should incorporate the guidelines discussed in this chapter.

The basic approach to making a system secure is to define one or more security domains. A security domain is a logical grouping of related components in the storage system, along with a set of rules that specify the amount of communication that is allowed between the components. Devices such as servers and storage systems that are within a given security domain are allowed to communicate with each other. The security manager defines the communication–if any–that is allowed between domains. The security system works by controlling every possible communication path between the security domains, so that data cannot be moved between domains without authorization.

The boundaries of the security domains are barriers that control access to the components. The boundaries also control communication between domains through the network or storage bus connections. Any potential path between security domains must be reviewed to make sure that only approved access is permitted. This can be an extremely complex undertaking.

1. An excellent introduction to computer security may be found in "Computer Security Basics", by Deborah Russell and G.T. Gangemi Sr, published by O'Reilly. A more detailed discussion of network security methods and protocols my be found in "Network Security Essentials," by William Stallings, published by Prentice-Hall.

Summary of SAN Security Practices

HP StorageWorks SAN hardware and software components incorporate features that can be used to implement a secure data storage system. The following table shows the appropriate use of these security features in various environments. The Enterprise Storage System environment is a typical mid-sized to large IT installation used in a business. The Service Provider Storage System environment is a large installation where several customers share a single IT infrastructure. These environments are discussed in more detail in later sections of this chapter.

Table 50: How to Use SAN Security Features

SAN Storage Security Feature	Enterprise Storage System	Service Provider Storage System
Physical security of SAN environment.	Suggested. All personnel are employees, but it is always better to keep sensitive systems away from informal access.	Essential. Personnel are competitors, so the systems must be kept in a secure environment.
Use of zones.	Optional. Use port or WWN zoning as required to manage Operating System conflicts.	Optional. Use port zoning as required to manage Operating System conflicts.
Use of Selective Storage Presentation (SSP.)	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.
Controlled access to storage system management using serial line interface.	Suggested. Limit physical access to machine room.	Optional. Storage systems are physically secure in this environment.
Controlled access to storage system management using in-band interface.	Optional.	Optional.
Restricted use of multiple switches.	Optional. No additional risk is added.	Optional. No additional risk is added.
Restricted use of multiple storage systems.	Optional.	Essential. Each customer must be located on a different storage controller pair.
Restricted use of Storage Management Appliance.	Optional. Appliance applications are password protected.	Recommended. Appliance applications are password protected, but a shared infrastructure is sensitive to competing interests.
Use of logical unit visibility control on Modular Data Router tape controller.	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.
Event logging enabled.	Essential. Needed to track possible intrusion attempts.	Essential. Needed to track possible intrusion attempts.

Data Path and Management Path Security

HP divides the responsibility for SAN security into two parts. Data Path Security refers to the protection of the communication path used to move user data through the SAN. Management Path Security refers to the protection of the communication path used to move management information through the SAN.

This is a functional distinction, because in some cases the same physical connection is used for both user data and for management information. For example, the Storage Management Appliance communicates with an HSV storage controller using the Fibre Channel connection that is also used to send user I/O traffic.

Table 51 shows the Data Path Security and the Management Path Security features available in HP SAN products.

Table 51: HP SAN Products Data Path and Management Path Security Features

Data Path Security	Management Path Security
Selective Storage Presentation	Passwords on user interfaces
Zoning by port and WWN	Security of sign-on to Element Manager
Port binding	Secure communication between storage management appliance and storage array
Fabric binding	Control of IP access to device management ports
Switch binding	
Communication packet encryption (future)	
Data encryption on storage media (future)	

The HP storage security model is implemented as three distinct areas. The overall security of the storage system is an integral part of the total solution security, and is deployed within the context of a comprehensive understanding of the system, developed and delivered by HP Professional Services. The software components of the storage system provide Management Path Security by controlling operator access rights and by securing the SAN management communication paths. The hardware components of the SAN provide Data Path Security by controlling storage array access and by governing the SAN fabric configuration control mechanisms.

Personnel and Operating Practises

The most important security feature in any environment is the attitude and operating practises of the personnel. The system managers and operators must have a positive view of security, and must be able to balance the need for data security with the need for reasonable user access.

Responsibility for maintaining SAN security should be assigned to a Security Manager, and this person should have the authority to enforce reasonable security guidelines. The Security Manager is responsible for making the trade-off between required user access capability and access restrictions required to maintain the required level of security.

HP professional services can assist in developing a suitable operating protocol for your SAN environment. The HP Security Services Portfolio includes a comprehensive end-to-end lifecycle range of services for designing, building, integrating, managing, and evolving sound solutions. The Security Healthcheck Services provide quick, comprehensive security vulnerability and risk assessments of your installation, including the storage systems and related storage network infrastructure. Refer to http://www.hp.com/hps/security for additional information on HP Security Services.

Professional Services for SAN Security

The establishment of a comprehensive security environment for a large computer system is a complex task. In addition, a failure or breach of the security system may result in the loss of important business information. For these reasons, HP requires that licensed security options must be installed as part of a professional services contract.

The HP SAN Security Services product includes a security review and planning feature and an ongoing security auditing process. The initial security review and planning steps are done before the security products are installed, and result in a report summarizing the security environment and requirements of the proposed installation. The security products are installed when required. The ongoing audit process includes a periodic review of the environment, management and operational practises, and any security logs or other data that is recorded by the system.

Risk of security problems is minimized by using the HP professional services for SAN security.

Security Features of HP StorageWorks SAN Components

The components of an HP StorageWorks SAN are shown in the figure below.

Hardware components include the Host Bus Adapter (HBA) residing in each Application Server, the Fibre Channel Switches that make up the SAN fabric (or fabrics in a multiple fabric SAN), the Disk Storage Systems (including their RAID controllers, cache memory, disks, and related management components), the Tape Storage Systems (including their Network Storage Router gateways), the SAN Management Server, the Storage Management Appliance, and various communication cables.

Software components include the server operating systems, the StorageWorks Command Console software, the SAN Management Software, Web Browser and Terminal Emulator interfaces to the Fibre Channel Switch and Storage System management tools, and the MDR management interface.

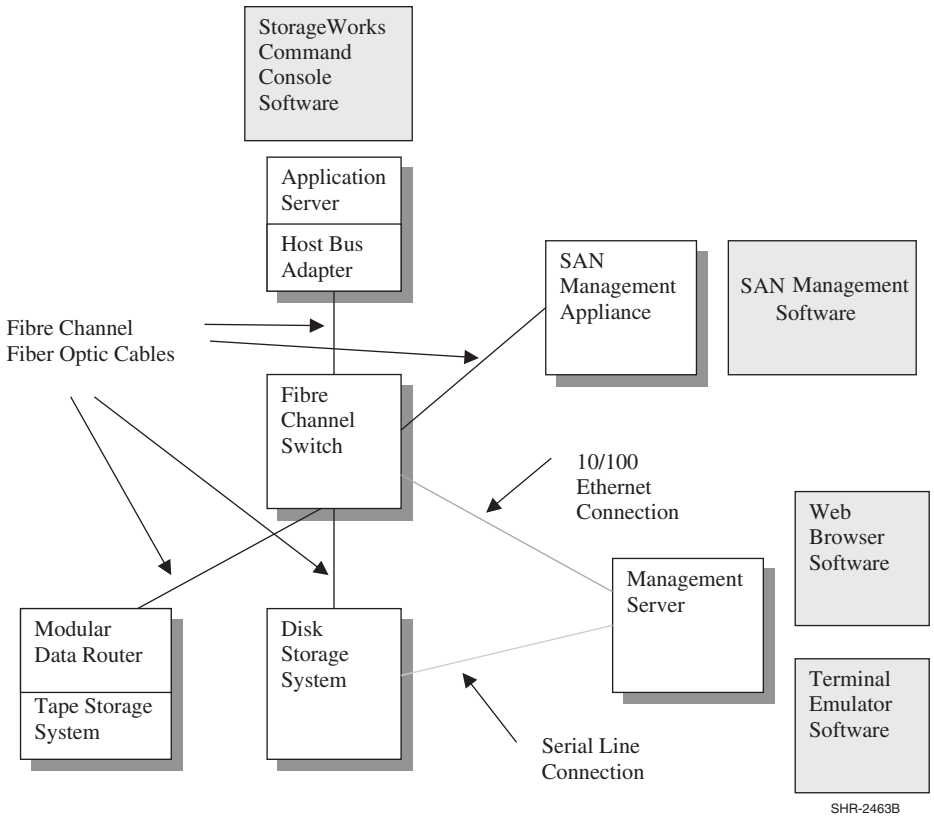


Figure 55: SAN Components

The current and future security features of each SAN component are listed below. SAN security is a rapidly developing technology, and the information in this chapter reflects the status of the technology as of the date of publication.

Fibre Channel Fiber Optic Cables

Fiber optic cables used for Fibre Channel communication do not emit electromagnetic radiation. This reduces the risk of security intrusion by means of remote sensing. However, it is not particularly difficult to make a physical tap into an active fiber optic cable. To maximize communication security, the cables should be kept within a secure area.

If a Fibre Channel cable is disconnected, the loss of signal is detected by the connecting devices and is logged in the devices' event logs. Verify that event logging is enabled on all connecting devices that have this feature.

10/100 Ethernet

Because of the difficulty of securing a distributed system, many IP LAN installations suffer from a low overall level of security. The storage security manager should verify that good passwords are in use on all the SAN components that are connected to a LAN, including the application servers, the Storage Management Appliance, the management server, and the Fibre Channel switches.

Serial Line

Serial line interfaces are used to connect a terminal (with its associated keyboard and display) to a server or other SAN component. Serial line connections are made using RS-232 physical interface. The EIA-423 protocol is used, and the connection runs at a low speed (typically 9600 baud). The serial line protocol itself does not have any provision for access security.

The security manager should verify that good passwords are in use on all the SAN components that have serial line connections, or that these connection points are in a secure area.

Host Bus Adapter

The host bus adapter (HBA) is the basic interface between the SAN and each server. The microcode in an HBA can be changed by using a utility program. In the case of Windows NT, a microcode load can be done on an active system, and the server does not need to be re-booted to resume normal I/O activity. A new host bus adapter may be installed in an operational server.

In Fibre Channel, there is no equivalent functionality to the "promiscuous" mode of operation that historically could be used on 10 Mbps CSMA/CD Ethernet networks. The security risk associated with HBAs in a Fibre Channel environment is low because the switches filter all traffic. Only traffic intended for a given server is communicated between the switch and that server's HBAs.

If the operating system driver is changed, then the system must be rebooted. This minimizes the likelihood of undetected changes to driver software.

Fibre Channel Switch

Fibre Channel switches are connected together to form a SAN fabric. The switches are the foundation of the SAN system. HP offers three families of switch products, the B-Series Fabric Line, the M-Series Line, and the C-Series Line, each with a unique set of features and capabilities. The security features differ between the three families, as described in the sections below. Refer to the product documentation for additional information that is specific to these products.

Standard Security Features of M-Series Product Line Switches

The following security features are included with all members of the M-Series product line family of Fibre Channel switches.

Switch Zones

The switches in a fabric cooperate to enforce data access zones. Servers are identified either by the switch port to which they are connected, or by their unique World Wide Names (WWN). These two methods are called "port zoning" and "WWN zoning", respectively.

The advantage of port zoning is that it is easy to configure, while the disadvantage is that if a server is moved from one port to another, the zone configuration must be changed to reflect the new connection topology. The advantage of WWN zoning is that it is independent of port, so servers may be moved from one port to another without changing the zone settings. The disadvantage is that an HBA in a server could, at least theoretically, take on the WWN of another HBA and thus gain unauthorized access to the wrong zone.

The purpose of zones is to manage the interaction of servers in a SAN, preventing interference between the operating system drivers. In heterogeneous configurations the drivers may interfere with each other, and in homogeneous operating system environments the capacity of certain driver data tables may be exceeded. Zoning is used to manage these operational factors. The security manager should verify that event logging is enabled to record unintended and unauthorized changes to the SAN configuration.

Passwords

All user interfaces to switches in the M-Series Line are protected by passwords. HP strongly recommends customers change the passwords on all switches.

Management System Communication

The Ethernet connection between the switch and the management station is protected by a secure protocol.

Optional Security Features of M-Series Product Line Switches

The following security features may be activated on all members of the M-Series product line family of Fibre Channel switches by the use of a license key. This key is supplied in the HP SANtegrity Binding product. Refer to the HP SANtegrity Binding product description for additional information on these features.

Fabric binding

When Fabric Binding is activated, only switches and directors that are identified in the Fabric Membership List are authorized to join the fabric.

Switch binding

When Switch Binding is enabled, only devices that are identified in the Switch Membership List are allowed to connect to the fabric.

Enterprise fabric mode

When Enterprise Fabric Mode is active, the security system automatically activates the following capabilities on all switches in the fabric and does not allow any to be deactivated:

- Fabric Binding (includes Insistent Domain ID)
- Switch Binding
- Domain RSCN's
- Rerouting Delay

Standard Security Features of B-Series Line Switches

The following security features are included with all members of the B-Series Line family of Fibre Channel switches.

Switch Zones

The switches in a fabric cooperate to enforce data access zones. Servers are identified either by the switch port to which they are connected, or by their WWN. These two methods are called "port zoning" and "WWN zoning", respectively.

The advantage of port zoning is that it is easy to configure, while the disadvantage is that if a server is moved from one port to another, the zone configuration must be changed to reflect the new connection topology. The advantage of WWN zoning is that it is independent of port, so servers may be moved from one port to another without changing the zone settings. The disadvantage is that an HBA in a server could, at least theoretically, take on the WWN of another HBA and thus gain unauthorized access to the wrong zone.

The purpose of zones is to manage the interaction of servers in a SAN, preventing interference between the operating system drivers. In heterogeneous configurations the drivers may interfere with each other, and in homogeneous operating system environments the capacity of certain driver data tables may be exceeded. Zoning is used to manage these operational factors. The security manager should verify that event logging is enabled to record unintended and unauthorized changes to the SAN configuration.

If more than 64 zones are defined in a single SAN, there may be cases where the port zoning table overflows. In this case the switches revert to WWN zoning. Refer to the user guide for the switch you're using for additional information on this topic.

Passwords

All user interfaces to switches in the B-Series product line are protected by passwords. The default passwords are available to the public, so it is extremely important to change them when the switches are installed.

Optional Security Features of B-Series Product Line Switches

Enhanced Brocade Fabric Manager 4.0

Brocade Fabric Manager provides a comprehensive SAN configuration control utility. Fabric Manager enables customers to configure and manage multiple B-Series product line switches from a single console. Features available with Fabric Manager 4.0 include SAN-at-a-Glance overviews with a topology map, call home support to send automatic notifications of system failure, enable remote support and isolate faults, and enhanced port management support, including port grouping.

Refer to www.brocade.com for additional information on Brocade Fabric Manager 4.0.

Secure Fabric OS

HP StorageWorks Secure Fabric OS protects your SAN by using the strongest, enterprise-class security methods available, including digital certificates and digital signatures, multiple levels of password protection, strong password encryption, and Public Key Infrastructure (PKI)-based authentication, and 128-bit encryption of the switch's private key used for digital signatures.

Features include Fabric Configuration Servers ("trusted" switches), Management Access Controls, Device Connection Controls (Access Control Lists), Switch Connection Controls, and Secure Management Communications. The trusted switches provide a central location for controlling SAN security. Device ACLs and Switch Connection Controls prevent unauthorized devices and switches from connecting to the secure fabric. All inter-switch management communication as well as communication to the management console is secured using encrypted passwords.

For additional information on configuring your HP StorageWorks SAN using the HP StorageWorks Secure Fabric OS, refer to

http://www.hp.com/country/us/eng/prodserv/storage.html

To access the technical documentation at this site:

- Locate the **Networked Storage** section of the web page.
- Under Networked Storage, go to the **by type** subsection.
- Click **SAN Infrastructure**. The SAN Infrastructure page displays.
- Locate the **fibre channel switches** section.
- Go to the **infrastructure** subsection.

Storage System

Products in the HP HSG80-based and Enterprise Virtual Array series of storage systems incorporate security controls on all the interfaces to the storage system.

Each storage system consists of a pair of HSG80 or HSV storage controllers, along with assorted supporting hardware.[2] The storage system is connected to one or more servers, and presents logical disks to those servers. Each logical disk has a logical unit number (LUN).

The Selective Storage Presentation (SSP) feature allows visibility of logical units to be restricted to a subset of the servers connected to the storage system.

Physical Access Control

The storage system is typically housed in a standard HP rack with locking front and rear doors. The locks for these cabinets all use the same key, so the security aspect of the locks is only sufficient to deter the most casual intrusion. The locks can be changed to provide additional physical security if desired.

Controller Management

Basic control of the storage system is performed using various buttons and lights on the front and rear panels of the RAID controller shelf. These controls allow the controllers to be halted or restarted. The HSG80 controller microcode is stored on PCMCIA cards that are inserted into these panels. Physical access controls to the controller shelf must be maintained to prevent unauthorized manipulation of these controls and to prevent unauthorized replacement of the controller microcode.

One option for initial setup of the storage system as well as for ongoing operation is to use a serial line connection to each HSG80 RAID controller. This connection is typically made between a controller and a terminal emulator program running on a nearby computer. All storage system management operations can be done using this interface. Physical access to the controller shelf must be maintained to avoid unauthorized use of this interface.

2. Refer to the HSG80 and HSV controller documentation for a complete description of the features of the HP family of storage systems.

Another option for the initial setup and ongoing operation of the storage system is to use the in-band Fibre Channel management system. This system sends SCSI commands to logical units on the storage system to control the logical unit definitions and the SSP settings. A server may send these commands to any logical unit to which SSP allows it access.

Data Access Control

The Selective Storage Presentation feature of the storage system is the method used to control access to user data. Access is allowed to each logical unit by one or more servers.

The SSP settings may be controlled by any server having access to any logical unit on the storage system. This includes the SWCC agent, the SSSU tool, and the Storage Management Appliance, and could include a purpose-built intrusion application running on a server connected to the SAN. If a computing environment has multiple security domains then the domains must not coexist on a single storage system.

For example, consider the configuration shown in the following figure. Server A and Server B have access to logical unit D and logical unit E respectively. Server A and logical unit D are in one security domain, and Server B and logical unit E are in a separate security domain. Since both have access to Storage System C, then Server A may change the SSP settings to prevent Server B from accessing any logical units on the storage system.

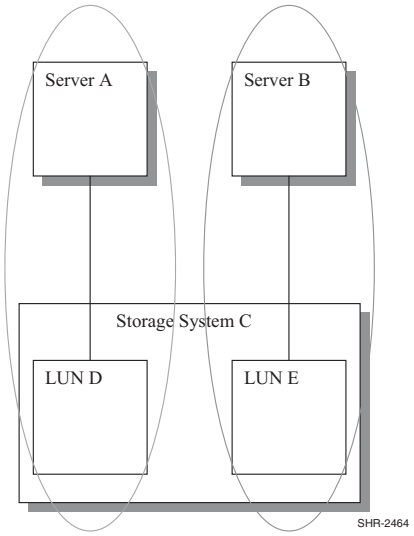


Figure 56: Multiple Security Domains on One Storage System

A future version of the HSG Array Controller Software will include a security enhancement that restricts management access to the controller. With this feature, the ability to make configuration changes to an HSG controller is restricted to those servers who are specifically authorized. This will allow multiple servers in multiple security domains to be connected to a single controller (or controller pair).

LUN security in the XP based Disk Storage Systems

Secure Manager XP provides security at LUN level, which is not available through switch zoning. LUN security can be enabled on a per port basis and allows permitted WWNs of hosts to be added to host group or groups on the selected ports.

LUN security in the VA-based Disk Storage Systems

Secure Manager VA is an optional software for the VA arrays that provides extra security at LUN level. This is accomplished by mapping LUNs against pre-configured host HBA WWNs thus creating a secure host table internally. The array will not permit access to the LUNs if the WWN of the host HBA is not present in the table. The total number of hosts or HBAs allowed per VA controller varies depending on the model. Refer to the respective user manuals for details.

EVA Management Access Control

A management agent can control many storage systems, and many management agents can control a storage system. Without password protection, any management agent on the fabric can access any storage system on the fabric. A password is used to increase the security within your storage subsystem. Specifically, password protection:

- Allows a management agent to control only certain storage systems.
- Allows only certain management agents to control a storage system.

All management functions for Enterprise Virtual Array storage subsystems are done via the Storage Management Appliance (sma). Two levels of security are implemented for the Enterprise Virtual Array to control unauthorized access to the storage subsystem.

The first level controls access to the MA itself. User access to the MA is controlled by a username and password method that uses the WEBM security model. Without the correct username and password, an unauthorized user cannot access the MA.

Secondly, the storage subsystem has an optional password protection to control which MA can manage which storage subsystems. The password is established by entering a password into the operator control panel (OCP) of one of the controllers. Use Command View for HSV Management Agent options to enter the password used by that MA to access particular Storage Subsystems.

In addition to the optional storage subsystem zoning on the fabric, this should prevent someone from putting an unauthorized MA on the fabric and attempting to manage a EVA storage subsystem.

StorageWorks Command Console Management Software

StorageWorks Command Console (SWCC) is a client-server storage management software product that supports in-band management of HP EVA and HSG80-based storage systems. An agent program runs on a server and communicates with any storage system attached to that server. The SWCC client program runs on a second, remote server to provide the GUI. The two servers communicate by using a TCP/IP connection between the two servers.

The Command Scripter tool also uses the SWCC agent to communicate with storage systems.

User access to the SWCC agent is controlled by a username and password. Any SWCC client accessing the agent to perform management tasks will be asked for this password. The communications between the management station and the host servers connected to the storage controllers is protected by single-use key encryption. In addition, remote configuration can be optionally disabled.

Communication between the agent and the controller is done by using SCSI commands on the Fibre Channel connection between the server and the controller. The agent communicates with a logical unit on the controller.

Storage System Scripting Utility

Storage System Scripting Utility (SSSU) is a character cell interface that allows a user to configure and control Storage Controllers generically on a Storage Area Network (SAN). Simple or initial configuration requests can be handled easily and expediently through this simple character cell interface, such as the initial creation of LUNs presented to the host. SSSU meets this requirement with an interface that allows the user to issue simple, terse commands.

SSSU uses the Storage Management Appliance (sma) to communicate with EVA storage systems. User access to the MA is controlled by the username and password method that uses the WEBM security model.

Storage Management Appliance

HP offers an optional integrated SAN management system that uses an appliance connected to the Fibre Channel fabric. The Storage Management Appliance hosts web-based Open SAN Storage Management software. This software provides a wide variety of management tools.

Access to the Open SAN Management applications is controlled by a username and password method that uses the WEBM security model.

Storage Security in an Enterprise Environment

In a business enterprise, computer systems may be shared between two or more departments. The systems are managed and operated by an Information Systems organization, which has enterprise-wide responsibility for the computing environment. All the people in the enterprise work towards a common business goal, but the day-to-day interests of the departments may vary widely depending on the business climate, time of year, or product development issues. Each department has specific computing requirements that must be met by the IS organization.

There may be wide differences in the need for data security. For example, a typical accounting department has strict security guidelines, while the marketing department may be willing to tolerate more risk.

The IS organization may try to achieve efficiency by placing the computer equipment in a single central location. A considerable amount of computer and storage hardware is required for an enterprise of moderate size. This discussion assumes that the storage for all the departments is located in a single SAN storage system. Servers are distributed throughout the facility.

The IS organization must implement a computing system that meets the security and capacity requirements of all the departments to which it provides service, and the IS security manager must implement a security plan that is suitable for the needs of the enterprise.

To meet the security requirements, many security managers specify a centralized machine room located in a secure area. This substantially reduces the security risk for the storage system, because the ordinary users of the system do not have physical access to the machines.

Security Expectations

This is an environment with a requirement for a high level of storage system security. Protection is needed against unauthorized accidental and malicious data access attempts. The required security level is set by the department with the most strict security needs.

SAN Component Security Attributes

The following features are used to provide security in this environment.

Traditional user account security is in effect in the servers. This protects each user account against accidental access by an unauthorized user. Disk quotas are enabled for each account. This prevents a user from consuming all of the storage capacity allocated to the server.

The HBAs pass user I/O requests to a Fibre Channel switch. Communication is done using Fibre Channel fiber optic cables. These cables pass from the servers into the secure area that holds the storage systems.

The SAN switches are shared by all the users and servers in all departments in the system, and are located in the secure area. Configuration management of the switches is done by the system manager using the web management interface. The interface is protected by password to prevent unauthorized changes to the switch configuration.

Data is stored in several StorageWorks storage systems. Access to each logical unit is controlled by the Selective Storage Presentation feature of the array controller.

Response to Attacks

Two attack scenarios are possible in this situation. Accidental inappropriate data access requests might be made by any user, and malicious attempts to make an inappropriate data access requests might be made by a user.[3]

Inappropriate read and write requests by system users are routinely handled by the operating system. Disk mounting requires a privileged account, and directories are protected by access control lists. The benign server environment puts little stress on the security capabilities of the storage system.

Since the storage systems are located in a secure area, the risk of inappropriate access to the array controllers is limited. There is some risk that the fiber optic cables might be tapped, but this requires a technical approach that is unlikely in this scenario.

Denial of service attacks initiated by system users, whether accidental or purposeful, are not fully protected against. A user could write a program that issues a useless but very high I/O load and consume most of the I/O operation capability of the storage system.

Checklist

For a SAN storage system that requires a moderate level of security, and where the storage systems and Fibre Channel switches are located in a secure area, the following steps are required.

- Good employment practices to minimize malicious attacks.
- Computer system security awareness training for all personnel.
- Routine user account management at the server.
- Disk quotas enabled for all users.
- Locate storage systems and Fibre Channel switches in a secure area.
- Passwords enabled on all switch configuration ports.
- Selective Storage Presentation for all logical units.
- Disable SES management interface to Fibre Channel switches.
- Routine periodic security audits.

The HP StorageWorks Secure Fabric OS is recommended for SANs based on B-Series product line switches.

3. We've ruled out serious attempts to break into the storage system, but unsophisticated attempts to read someone else's data are possible in any computer system environment.

Storage Security in a Service Provider Environment

Some organizations provide computing services to their customers on a lease or contract basis. The services may include general-purpose office applications such as Microsoft Exchange or file and print services, or they may be specialized. One example of the latter is the Storage Service Provider, which provides storage capacity to some other organization. In all service provider situations, the service provider is the HP customer, and the service provider has second level customers of its own who purchase the service.

These second level customers are the users of the systems.

These users may be competitors of each other, and it is essential that they be protected against security breaches—accidental or intentional—by other users in the computer system. The security plan must take into account the possibility of aggressive attacks.[4] This is probably the most difficult environment for a storage system security manager.

Physical access to the storage system is controlled by placing it in a secure area. The servers are in separate secure areas, segregated by user so that each user has a unique secure server area.

Security Expectations

The requirement is for high security. Each user wants a separate security domain because there is no trust between competitors. Protection against accidental or intentional unauthorized access to data must be provided, and protection against unauthorized changes to the configuration of the storage system is also required. Sophisticated attacks are not expected, but intentional attacks may occur.

At the same time, services providers are very sensitive to cost. There is a desire to share equipment between users to minimize hardware and management cost. This must be balanced against the security requirements.

SAN Component Security Attributes

The following features are used to provide security in this environment.

Traditional account security is in effect in the servers. This protects each user from accidental unauthorized access. Disk quotas are enabled for each account. This prevents I/O from one account from consuming all of the storage capacity allocated to the server.

If one user attempts an intentional attack on another user's data, it may be expected that this would be done from a privileged account on a server. Account security does not protect against this sort of attack, but the exposure from a privileged account is to the data of other accounts on that system, not other users—because they are on their own servers.

The HBAs pass I/O requests to a Fibre Channel SAN switch. Communication is done using fiber optic cables. These cables pass from the servers into the secure area that holds the storage systems.

The Fibre Channel switches are shared by all of the service provider's customers, and are located in the secure area. Configuration management of the switches is done by the service provider's system manager using the serial line interface.

Data is stored in several StorageWorks storage systems. Access to each logical unit is controlled by the Selective Storage Presentation feature of the array controller.

4. Denial of Service attacks are not considered to be a problem, because the comparatively small number of users on a SAN makes it easy to identify and eliminate this sort of aggressor.

A user may attempt to access a competitor's data. To protect against this possibility, it is important to provide a separate storage system for each of the service provider's customers. While the risk associated with sharing a single storage controller between customers is small,[5] distributing them onto private storage controllers eliminates the risk.

Response to Attacks

Two attack scenarios are possible in this situation. Accidental inappropriate data access requests might be made by any user, and malicious attempts to make an inappropriate data access requests might be made by a user.

Inappropriate read and write requests by system users are routinely handled by the operating system. Disk mounting requires a privileged account, and directories are protected by access control lists.

The storage systems are located in a secure area, but there is some risk of intentional attacks. This is prevented by providing a separate storage controller for each user.

There is some risk that the fiber optic cables might be tapped. While this risk is minimal, the Fibre Channel switch logs must be examined regularly and the configuration change alarms on the switches enabled. These will notify the security manager if this sort of activity occurs.

Depending on the service provider environment, it may be possible for a sophisticated attack on the SAN to take place. This could involve equipment such as frame grabbers or phantom switches. It is extremely difficult to protect against a sophisticated attack against any network system, and Fibre Channel is inherently exposed because the data is sent as clear text. If this level of risk is expected, refer to the following section.

Denial of service attacks initiated by system users, whether accidental or purposeful, are not fully protected against. A user could write a program that issues a useless but very high I/O load and consume most of the I/O operation capability of the storage system.

Checklist

For a SAN storage system that requires a high level of security, and where the storage systems and Fibre Channel switches are located in a secure area, the following steps are required.

- Good employment practices to minimize malicious attacks.
- Computer system security awareness training for all personnel.
- Routine user account management at the server.
- Disk quotas enabled for all users.
- Locate storage systems and Fibre Channel switches in a secure area.
- Passwords enabled on all switch configuration ports.
- Selective Storage Presentation for all logical units.
- Disable SES management interface to Fibre Channel switches.
- Disable SNMP management interface to Fibre Channel switches.
- Disable web browser management interface to Fibre Channel switches.
- Each user (that is, each customer of the service provider) must have a separate array controller.
- Routine periodic security audits.

5. It requires special knowledge and equipment to successfully complete an unauthorized access to data on an array controller.

The HP StorageWorks Secure Fabric OS is strongly recommended in B-Series product line SANs used in service provider environments. The enhanced security provided by this product eliminates the risk associated with having ports from a single SAN exposed to multiple second level customers.

Storage Security in a Secure Environment

Some system environments require extremely high levels of security. These are cases of national security or where the data is so sensitive that the owner is willing to make substantial functionality trade-offs to maintain the desired security level. These systems are safe in the face of the worst cases of overt attempts to break into the system by any means possible.

Security Expectations

It is expected that the system will have no exposure to security intrusions. This corresponds to the highest levels of information security.[6] Network systems generally are not able to be audited for compliance with the highest levels of security, because network software is too complex for a comprehensive evaluation. To obtain the highest possible levels of information security, the entire system must be enclosed in a secure environment.

SAN Component Security Attributes

To provide security in this environment, the system is enclosed in a secure area.

Checklist

For a SAN storage system that requires the highest level of security, enclose the entire system in a secure area.

- Perform routine periodic security audits.
- Follow other appropriate actions based on the required system security level.
- Place machines in a secure area.

6. Computer system security ratings are set by NIST/NSA in the US and ITSEC in Europe, and “Common Criteria” is a newly-adopted US standard. Within these classifying bodies, a product can be evaluated at various security levels. Currently, most operating systems are classified at ITSEC's E3 rating or Common Criteria's CAPP protection profile EAL4. The OpenVMS SEVMS product has a E3/B1 rating. Tru64 UNIX has an E2/C2 rating. See http://csrc.nist.gov/cc/.

Continuous Access Storage Appliance

10

The HP OpenView Continuous Access Storage Appliance (CASA) solves a wide range of problems that may be encountered in enterprise storage environments. This chapter provides an overview of CASA as well as information about how to integrate CASA solutions into general HP StorageWorks Fibre Channel SAN installations. The following topics are discussed in this chapter:

- Overview of CASA
- How CASA Works
- CASA Features
- CASA Management
- Security Implications of CASA
- Supported Systems and Software
- Configuration Rules
- CASA Services
- Additional Information Sources

Note: The information in this chapter is specific to version 5.6.1 of CASA.

Overview of CASA

CASA provides data replication on SANs consisting of heterogeneous mixes of servers and RAID array storage devices. By making all available storage capacity accessible by all servers—with appropriate access controls as required—CASA helps you optimize the use of the server and storage systems in your installation. Data may be placed on the storage device that makes the most sense, regardless of server driver, host bus adapter, or operating system.

CASA supports data mirrors and point-in-time snapshots. These may be done between heterogeneous storage devices. By providing the opportunity for flexible data placement, CASA allows you to distribute redundant copies of data on the storage device most appropriate for each specific type of copy.

CASA can be used to migrate data between heterogeneous storage devices. By removing limits to where data is stored, CASA facilitates the retirement of legacy equipment and the addition of new equipment. If your data availability specifications change, CASA helps you adapt existing data to different availability configurations. As your data center requirements change to meet new business conditions, CASA provides the adaptable data placement and migration tools to optimize your new SAN configuration.

CASA provides an incremental approach to storage virtualization, because it works in conjunction with traditional SAN solutions. If only a subset of your data requires replication or migration, then adding CASA to your existing SAN won't disturb the rest of the data.

The features and supported configurations described here reflect CASA SANOS software version 5.6.1.

Figure 57 is an overview of a typical CASA configuration.

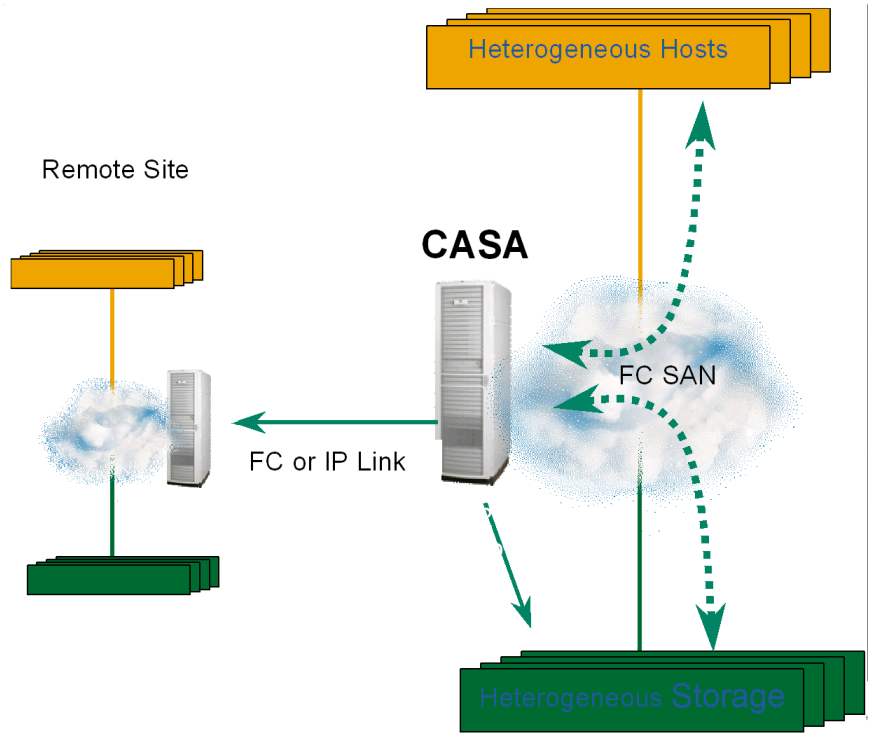


Figure 57: Typical CASA Deployment

How CASA Works

The Continuous Access Storage Appliance consists of the following components:

- Physical application servers and physical storage arrays
- A CASA appliance with two internal nodes and shared metadata storage
- The CASA utility software
- Management tools used to manage the operating characteristics of the CASA
- Optional racks to hold the appliance, servers, storage, and related equipment

Application servers are connected to CASA using traditional Fibre Channel (FC) Host Bus Adapters (HBAs), cables, and switches. RAID storage arrays are connected using FC cables and switches as required for the specific configuration. The detailed requirements for these components are discussed in this chapter.

Figure 58 shows a schematic of the internal architecture of the CASA. The target ports present virtual disks to the physical servers, while the initiator ports present virtual servers to the physical storage arrays. Shared storage is used within the appliance to store metadata information about the virtual devices. Gigabit Ethernet ports are used to connect the nodes in the appliance.

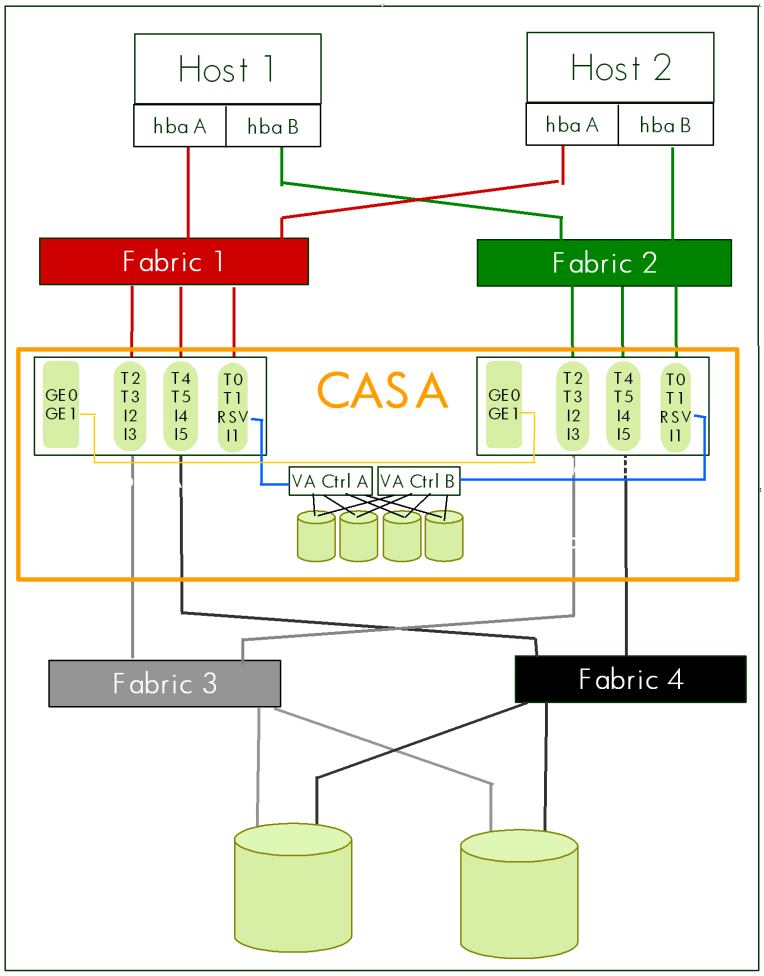


Figure 58: CASA Internal Architecture

The CASA software implements two kinds of virtual devices:

- The appliance presents virtual target logical units (LUNs) to the application servers.
- The appliance presents virtual initiators to the storage arrays.

The servers "see" the virtual storage devices provided by the appliance, but not the physical storage arrays in your SAN. Similarly, the storage arrays "see" the virtual servers provided by the appliance, but not the physical servers in your SAN.

This isolation of the physical servers from the physical arrays provides the opportunity for tremendous flexibility in the deployment of the servers and storage in the SAN, and is a core element of the storage infrastructure that supports the HP Adaptive Enterprise environment.

Changes to the array configuration can be made without the knowledge of the servers, and changes in the server configuration can be made without the knowledge of the arrays. For example, failures in disk arrays can be made completely transparent to the servers. The failure recovery mechanism in the array works with the virtual server in the appliance to manage the failure, but the appliance masks this activity from the servers on the SAN. Certain appliance failures are visible to the servers—in the same way that array failures are visible to the servers in a traditional SAN—but because all of the storage provided to the server is from the appliance, there is only one storage failure model that the server needs to handle. This means that a server may connect to storage capacity provided by a heterogeneous mix of storage array types, while only implementing a single storage failure handling model. This failure handling model is the one provided by the appliance.

Appliance Ports and Paths

Each CASA appliance is fully redundant, and includes two peer nodes, each with:

- 6 target ports (host-connect)
- 5 initiator ports (storage-connect)
- 1 dedicated initiator for shared metadata storage
- 3 Gigabit Ethernet ports

The CASA appliance has a total of 12 target ports and 10 initiator ports.

Shared metadata (data about the data) is stored on fully redundant dual controller local storage.

The CASA appliance has redundant paths:

- From hosts to CASA
- From CASA to storage

CASA Features

Using the method described above, the CASA provides the following capabilities:

Storage Pooling

Under the control of CASA, physical SAN storage is collected into a virtual capacity pool. Unused storage capacity (“stranded capacity”) can be allocated from the virtual capacity pool and then assigned to where it is needed. Mirroring and related replication technology can be applied to the pool in a flexible fashion, without disrupting the servers’ view of the virtual devices. This capability optimizes the utilization of existing storage capacity.

Local Data Replication

1. Data replication. Data in a given LUN may be mirrored to up to nine other LUNs. This adds to the reliability of the data stored in the physical arrays by protecting against array failure. Mirroring can be used to add flexibility to your backup process by allowing multiple copies of the data to be available at one time.
2. Data snapshot. The Vsnap feature creates a space efficient point-in-time image of a LUN. This capability can be used to create additional static copies (up to nine) of databases or other information. Typically, Vsnap uses only a fraction of the space that would be required for a full mirror of the LUN.

Remote Data Replication

1. For CASA Fibre Channel replication (FCP mirrors) or for Synchronous IP replication, CASA's must be within a campus configuration, typically within 40 kilometers.
2. A cascaded configuration supports 2 CASAs only.
3. Remote data replication. Mirror copies may be made (up to nine copies) between multiple CASAs, providing disaster tolerance and the ability to recover quickly from a site failure.
4. Remote cross mirroring between two appliances. The virtual storage capacity pool is distributed across the two sites, and servers at each site may have local and remote mirrors. This provides a fully disaster tolerant configuration that can withstand the failure of either site. For more information on this CASA application, refer to http://www.hp.com/products1/storage/products/virtualization_appliances/network/sv3000/infolibrary/CASA_CAMs.pdf
5. Synchronous and asynchronous mirroring. Both types of remote mirroring are supported. In the synchronous case, I/O operations issued by a server are not reported as complete until the remotely replicated operation has completed. In the asynchronous case, I/O operations are reported as complete when the local operation completes, which improves performance in cases where distance-related latency is undesirable. Both cases provide guaranteed write ordering technology, so that a disaster recovery operation will have a coherent data image with which to continue operation.
6. "N to 1" replication (for IP replication only.) Up to three sites can be mirrored back to a single central site. This may be used to support centralized backup of multiple sites. This feature allows the use of asynchronous replication to all of the the cascaded sites: No snapshot is required to handle multiple sites.

Figure 59 shows a cascaded configuration.

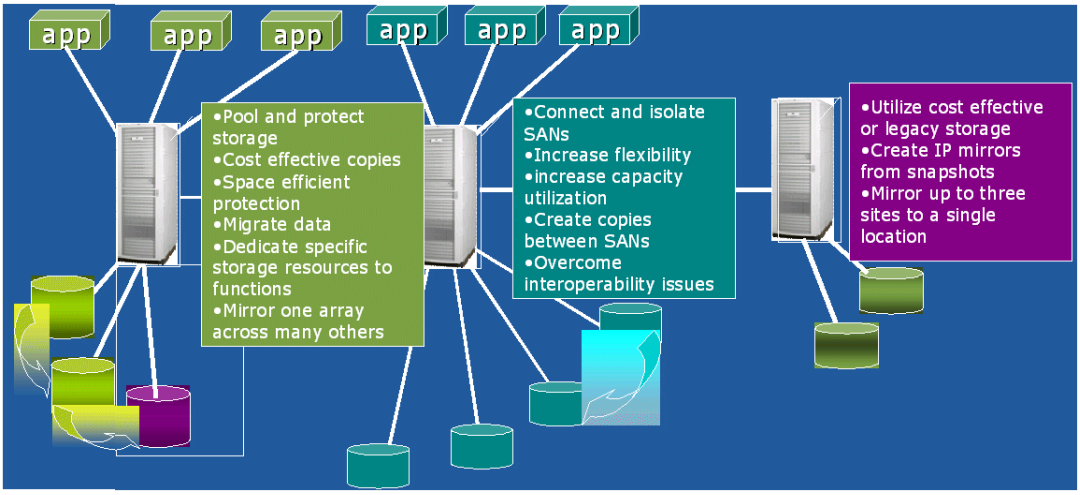


Figure 59: Cascaded CASA Configuration with Three Sites

IP/FCP Mirroring

The CASA appliance contains a pair of redundant nodes. These nodes work in tandem as peers to provide a high level of availability to the CASA system. "IP/FCP mirroring" is used to maintain coherence between the two nodes. A journal is maintained on a shared metadata disk array built into the CASA, making the appliance fully redundant. If one node fails, the other node has full access to the shared journals and can fully recover the data.

Mirroring availability continues under a variety of failure conditions:

- Local storage failure
- Remote storage failure
- Either IP link failure
- Either CASA node failure
- In the case of either IP link failure, SCSI requests are routed to the peer node
- If one node loses access to storage, SCSI requests are routed to the peer node

Heterogeneous Storage

In all of these cases, heterogeneous mixes of storage arrays are supported. CASA contains HBAs, HBA firmware, driver software, and path failover software appropriate for use with all supported combinations of storage array devices. Since the device characteristics are hidden from the application servers, heterogeneous mixtures of storage array devices may be used without requiring any changes or special configuration options in the application servers.

This powerful feature adds considerable flexibility to the HP StorageWorks SAN. Benefits include:

- Existing arrays may be mixed with new arrays to support data migration.
- Low cost arrays may be mixed with enterprise-class arrays to optimize cost.
- Migration from one type of array to another may be done without impact to the servers.
- Configuration changes required to support new storage requirements may be done without interfering with production work.

Many other important applications for this feature may be imagined without difficulty.

CASA Management

CASA environments are managed using the CASA Management Service (CMS), a centralized web-based user interface. The management service is used to configure and control all aspects of the CASA system. All CASA features are presented in a common fashion to make it easy to control both local and remote devices and the distributed virtual capacity pool. CMS implements a secure management interface for all CASA-related functions.

CASA Graphical User Interface

The CASA graphical user interface (GUI) supports remote management of CASA appliances. It provides navigation between multiple CASA nodes and appliances without having to login, and provides optional access to the command line interface (CLI) if needed. The GUI incorporates settable user privileges to provide selective access to management operations.

CASA Command Line Interface

The CASA command line interface (CLI) provides remote console based management of CASA appliances. It uses a UNIX shell-like interface that has scripting capability, the ability to process multiple requests from a single file, and flexible navigation between CASA nodes and appliances. The scripting capability allows a CASA to be managed by third party clients.

CMS Server

The CMS server software runs on the CASA, and is responsible for handling user management requests from management clients, either the GUI or the CLI.

The GUI or CLI sends an XML request to the management server, which in turn performs the required validation and translates the request to a command that is understood by the appliance. The XML handler is capable of processing management requests for the appliance backend engine and for B-Series switches.

The appliance processes the request, and then sends and appropriate response to the management server, which in turn creates an XML response message and sends it back to the requesting client.

Prior to forwarding any request to the appliance backend engine, the management server first authorizes the request with the security service, as discussed in the CASA security section, below.

Integration of CMS with OpenView SAM

OpenView Storage Area Manager (OpenView SAM) is used to handle SNMP traps generated by CASA. OpenView SAM 3.0 Suite DPIs are available for integration with Storage Node Manager, Storage Builder, Storage Optimizer, and Storage Accountant. These provide centralized discovery, mapping, performance planning and management, and billing capabilities.

Additional Information About CASA Management

Refer to the *HP OpenView Continuous Access Storage Appliance System Administrator's Guide* for additional information about managing the CASA system.

Security Implications of CASA

Traditional networked storage systems deliver a high level of security. In many cases this security is built into the SAN, because typical SANs are constrained to fairly small physical areas (such as a single machine room, single building, or single campus) and because SAN infrastructure components (such as Fibre Channel switches) incorporate various security control methods. In those cases where a SAN is extended beyond these limits, additional techniques (like encryption of data passed on extended links) must be used to maintain a suitable level of security.

Security Features

CASA systems achieve a level of security similar to that of traditional SAN systems by the use of strong access controls and redundancy.

- Passwords protect against intrusions through the management interface.
- Every CASA system is designed using a no-single-point-of-failure topology with redundant components and redundant meta-data storage.
- LUNs are mapped to hosts by unique worldwide name (WWN) to protect data from access by unauthorized servers. New hosts on the network have no access until LUNs are explicitly mapped.
- Hosts can have exclusive storage for independent applications or shared storage to enable failover for clustered applications
- Mapping is network-based, so no host software is required.

The security component provided by the CASA Management Service (CMS) provides ticket-based authentication and authorization for services on a CASA appliance. This is used by CMS to control access to the CASA appliance, B-Series switches, and its own administrative interface. It also provides an audit trail of authentication and authorization operations, as well as of its own administrative operations.

Security Services provided:

- Identification and Authentication:
  - Challenge-Response Mechanism. Password is never transmitted over the wire.
  - Encryption Based on Shared Knowledge of the Password and User ID.
  - 128 bit Encryption utilizing Blowfish
  - Result: Ticket is Granted
  - Tickets have a tunable timeout—Default is 8 hours.
  - Originator IP Address is contained within the encrypted portion of the Ticket.
  - Ticket must be passed with every request.
- Authorization:
  - Authorization request contains: Ticket, Originating Host, Comma separated list of requested operations
  - The requestor must have privileges required for ALL operations to allow any to be performed.
- User and Role Administration:
  - Add/Mod/Delete/Query Users
  - Add/Mod/Delete/Query Roles
  - List Roles for a User
  - List Privileges for a User

Architectural Advantages of this approach include:

- XML is a standard language that allows an open, human-readable protocol.
- The security service is usable by clients written in any language that can output XML on a socket connection.
- Implementation in Java enables platform independence.
- XML-based socket level protocol

The strong security features of CMS provide a high level of protection against intrusion through the management interfaces. In addition, if someone were to obtain unauthorized access to the appliance itself, a valid account and password are required to use the GUI or CLI even from the local machine.

Refer to Chapter 9, "SAN Security" for additional information.

Supported Systems and Software

CASA 5.6.1 supports the following Fibre Channel SAN switches, storage arrays, and server operating systems. Contact your Hewlett-Packard representative for information on specific supported models and version numbers.

Supported Fibre Channel SAN Switches

CASA supports the full line of HP StorageWorks SAN switches, as shown in the following tables.

Table 52: HP StorageWorks B-Series Product Line Switches

HP StorageWorks Switch Name		Firmware Version	Number of Ports
HP StorageWorks MSA SAN switch 2/8		3.1.1c	8
HP StorageWorks SAN Switch 2/8 EL, 2/8 Power Pak			8
HP StorageWorks SAN Switch 2/16, 2/16 EL, 2/16 Power Pak			16
HP StorageWorks SAN Switch 2/32, 2/32 Power Pak		4.1.2b	32
HP StorageWorks Core Switch 2/64, 2/64 Power Pak			64 (2 switches per chassis, for a total of 128 ports per chassis)
HP Switch Name	**Compaq StorageWorks Switch Name**		**Number of Ports**
HP Brocade 2400 (HP reseller)	Compaq StorageWorks SAN Switch 8	2.6.1c	8
N/A	Compaq StorageWorks SAN Switch 8-EL		8
HP Brocade 2800 (HP reseller)	Compaq StorageWorks SAN Switch 16		16
N/A	Compaq StorageWorks SAN Switch 16-EL		16
HP Surestore FC Switch 6164 (64 ISL Ports)	Compaq StorageWorks SAN Switch Integrated/32 (64 ISL Ports)		32 (counts as 6 switches and 2 hops when applying configuration rules)
HP Surestore FC Switch 6164 (32 ISL Ports)	Compaq StorageWorks SAN Switch Integrated/64 (32 ISL Ports)		64 (counts as 6 switches and 2 hops when applying configuration rules)
HP Surestore FC 1Gb/2Gb Entry Switch 8B	N/A	3.1.1c	8
N/A	Compaq StorageWorks SAN Switch 2/8-EL		8
N/A	Compaq StorageWorks SAN Switch 2/16-EL		16
HP Surestore FC 1Gb/2Gb Switch 8B	N/A		8
HP Surestore FC 1Gb/2Gb Switch 16B	Compaq StorageWorks SAN Switch 2/16		16

Table 53: HP StorageWorks M-Series Product Line Switches

HP StorageWorks Switch Name		Firmware Version	Number of Ports
HP StorageWorks edge switch 2/12		05.05.00-12	4 to 12
HP StorageWorks edge switch 2/16		05.01.00-24	16
HP StorageWorks edge switch 2/24			8 to 24
HP StorageWorks edge switch 2/32			16 to 32
HP StorageWorks director 2/64			32 to 64
HP StorageWorks director 2/140			64 to 140
HP Switch Name	**Compaq Switch Name**		**Number of Ports**
N/A	McDATA ES-3016 (Compaq reseller)	05.01.00-24	16
N/A	McDATA ES-3032 (Compaq reseller)		32
McDATA ED-5000 (McDATA reseller)		04.00.00-16	32
HP Director FC-64	Compaq StorageWorks SAN Director 64	05.01.00-24	64

In addition to the switches listed in Table 52 and Table 53, CASA is also supported with the following Fibre Channel switch models (vendor branded):

Table 54: Brocade and McData Fibre Channel Switch Support for CASA-only SAN

Switch Brand	Switch Model	Firmware	Hub
Brocade	2400	2.6.1c	No
	2800	2.6.1c	No
	3200	3.1.1c	No
	3800	3.1.1c	No
	3900	4.1.2b	No
	12000	4.1.2b	No
McData	6064 (1 Gb directors)	04.01-02-4	No
	6140 (2 Gb directors)	05.01.00-24	No
	3216	05.01.00-24	No
	3232	05.01.00-24	No

Note: Table 54 lists switch vendor branded switch models supported by CASA only. For general non-CASA SAN configurations, refer to Chapter 3 for a list of supported HP-branded switch models.

Supported RAID Storage Arrays

- HP StorageWorks XP48, XP512, XP128, XP1024
- HP StorageWorks EVA v2, EMA12000, MA8000
- HP StorageWorks MSA1000
- HP StorageWorks va7400, va7410, va7100
- EMC Symmetrix 4 and 5
- EMC CLARiiON 4700 and 5700
- Hitachi 9200 and 9900
- Dell Powervault 650F

Supported Host Operating Systems

- Windows 2000, requires AutoPath version 2.0 for failover
- Windows NT 4.0, requires AutoPath version 1.05 for failover
- Solaris 2.6, 2.7, 2.8, requires VERITAS DMP for failover
- HP-UX K, L, R, and V class servers running HP-UX 10.20, 11, 11i, requires PVlinks for failover
- IBM AIX 4.3.3, requires AutoPath version 2.0 for failover
- Red Hat 7.1/Linux Kernel 2.4, requires Native Red Hat failover
- Novell NetWare 5.1, requires Native NetWare failover

Configuration Rules

CASA supports the full range of HP StorageWorks Fibre Channel SAN configurations as documented in this Guide. The following additional rules apply to all HP StorageWorks SAN installations that include CASA appliances.

Ask your HP representative for additional guidance on configuration rules.

Note: It is required that all host HBA ports are individually zoned to CASA target ports and that all CASA initiator ports are individually zoned to storage target ports.

Number of SAN Fabrics

For the purpose of availability, CASA installations normally use four separate Fibre Channel fabrics. Two fabrics are used to provide redundancy for the connection between the application servers and the appliances. Two additional fabrics are used for the connections between the appliances and the storage arrays. For installations where all the storage capacity is to be managed by CASA, this is the preferred configuration because it maximizes the availability of the entire system.

CASA may be used in installations where some of the storage capacity is managed by the CASA and some is directly connected[1] to application servers. In this case two fabrics are required. The failover functionality in the application servers, CASAs, and storage arrays makes this a no-single-point-of-failure configuration, however, there may be additional failover delay associated with the failure of one of the fabrics.

Number of CASAs

CASA is deployed with pairs of nodes in order to provide failover capability. A minimum CASA deployment has two nodes and is described as “one CASA.”

Multiple CASAs may be included in a SAN. Storage capacity is not shared between CASAs, except in those cases where replication is used. There is no specified limit to the number of CASAs that may be deployed in a single SAN, but in practice the connectivity limits of the SAN will restrict the number of CASAs.

Recommended SAN Topology

The recommended SAN topology for CASA deployments is core-edge (or director-edge) interconnection. Other topologies may not provide adequate port-to-port bandwidth.

CASA is supported in all HP StorageWorks SAN topologies.

Connection Rules

CASA requires a high-performance connection to the SAN for all of its ports. For this reason, the CASA should be connected directly to the core.

Application servers may be connected directly to the core or to edge switches, depending on the application workload.

Storage arrays may be connected to edge switches or directly to the core, depending on the workload requirements. In many cases the storage array will see a heavy workload and will need to be connected to the core.

Failover Software Rules

If all of the storage capacity in the SAN is under the management of CASA, the application servers must have failover software appropriate for the CASA. The physical storage devices are consolidated by CASA, so the failover software depends only on the CASA.

The following failover software must be installed on the application servers. Note that this failover management software is used when connecting to the CASA regardless of the storage arrays that are present in the configuration.

- AutoPath VA for Microsoft Windows and IBM AIX
- Veritas DMP for Sun Solaris
- PVLinks for HP-UX
- Native Linux
- Secure Path for Microsoft Windows

In order to handle the event of a path failure between the CASA and a storage array, the following failover software is used in the CASA:

- Native Active-Active (XP, VA, EMC)
- Secure Path (HSG80, HSV110,and MSA)
- ATF (for Clariion)

---

1. The connection may be a direct physical connection between the application and the storage array, if this is supported for the required server/array combination, or may be through an intermediate SAN. In this discussion “direct connection” includes both possibilities.

If some of the storage capacity is managed by the CASA and some is directly connected to application servers, then the application servers must have the appropriate failover software for the storage arrays to which they are connected. In these configurations the following issues should be considered.

- May require multiple flavors of failover software on the host (one for CASA storage, one or more for physical storage).
- Requires LUN mapping/masking on storage to allocate CASA LUNs and host accessible LUNs. Ensure that CASA LUNs can only be accessed by CASA by using an appropriate combination of LUN mapping, LUN masking, and zoning.

Example Configurations

Three example configurations are shown below. They cover the following cases:

- A Single CASA Manages all the Storage Arrays
- A Single CASA Manages a Subset of the Available Storage Arrays
- Multiple CASAs Manage the Storage Arrays

Similar configurations may be suitable for customer installations, depending on the specific requirements at hand.

Single CASA Manages all the Storage Arrays

Figure 60 shows a simple CASA configuration with four single-switch SAN fabrics. CASA Node C and CASA Node D are the redundant pair of nodes that make up “the CASA” in this illustration.

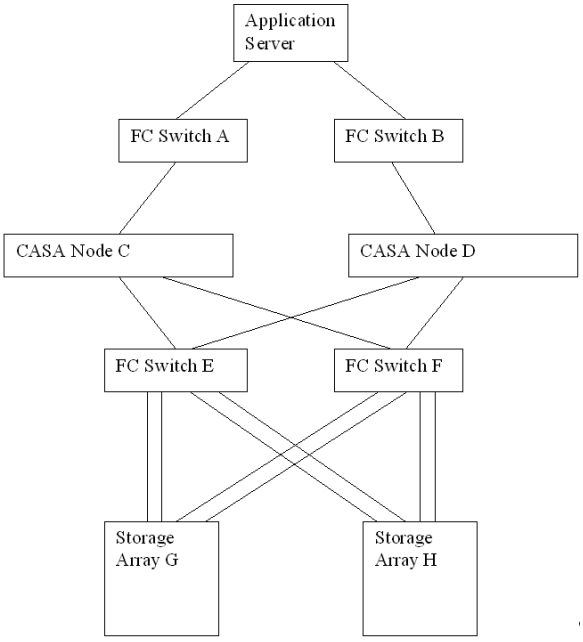


Figure 60: Single CASA Configuration

Single CASA Manages a Subset of the Available Storage Arrays

Figure 61 shows a more complex configuration where one CASA (pair of nodes) manages some of the storage capacity, while other storage capacity is connected directly to the application servers. Additionally, one of the storage devices, Storage Array H, is configured with LUN masking so that some of its capacity is connected to the servers and some to the CASA. Storage Array G is managed by the CASA while Storage Array I is connected directly to the application server.

In this case two fabrics are used because a connection between the application server and the storage arrays is needed. Each fabric has a core-edge topology, and the servers are connected to the edge switches as was discussed above. All of the CASA ports are connected directly to core switches.

Note that some of the connections to the storage arrays are not included on this drawing, for the purpose of simplification.

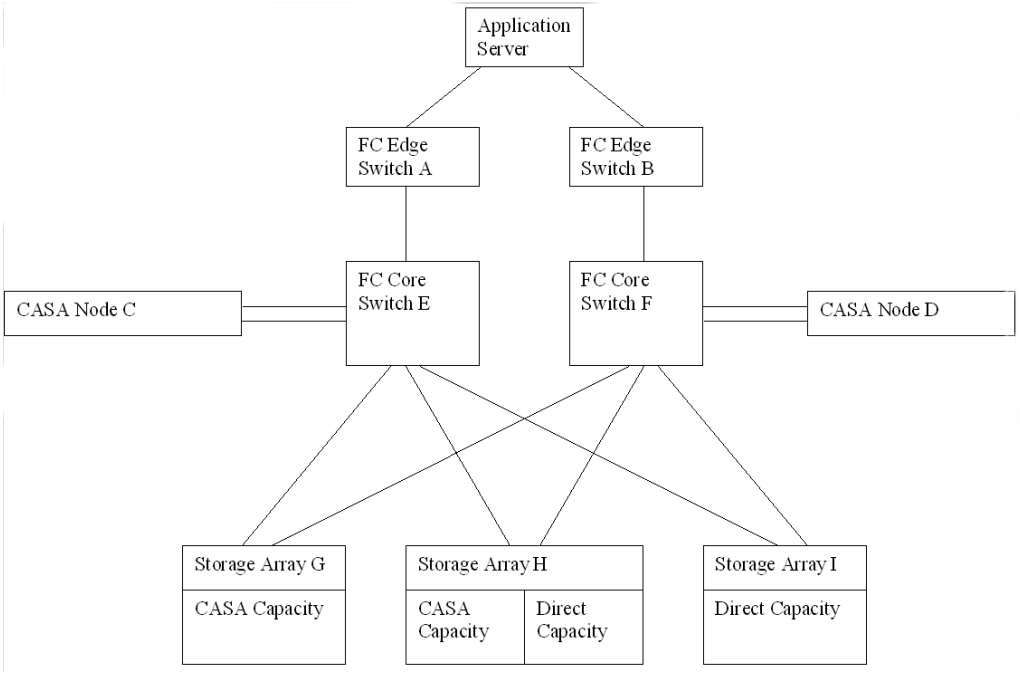


Figure 61: Single CASA Mixed with Non-CASA Storage

Multiple CASAs Manage the Storage Arrays

Figure 62 shows a larger configuration with multiple CASAs and multiple storage arrays.

Each CASA (node pair) controls a specific set of physical LUNs. The LUNs may be located on a single storage array, but in that case LUN masking (for example, Selective Storage Presentation on EVA arrays) must be used to isolate the LUNs.

CASA Nodes C and D are a pair, and have storage capacity assigned to them on storage arrays G and H. CASA Nodes J and K are a pair, and have storage capacity assigned to them on storage array G. Some of the capacity on storage array H, and all of the capacity on storage array I is assigned for direct access (through the SAN) by the application servers.

If one imagines an even larger configuration, and keeps in mind the requirement that all the CASA ports be connected directly to the fabric core, it is easy to see how the number of CASAs in a single installation is limited only by the number of ports on the fabric core.

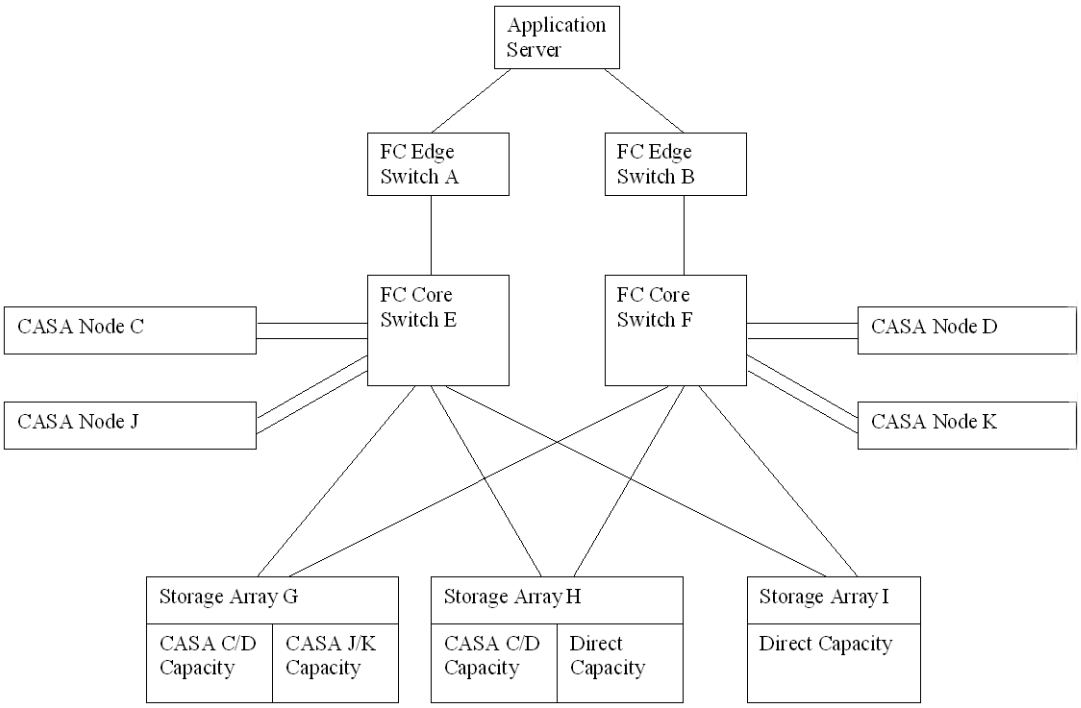


Figure 62: Multiples CASA Supporting Mix of Arrays

CASA Services

HP offers three levels of CASA Implementation Services. Simple (one operating system) and moderately complex (three operating systems, 12 hosts, and two Fibre Channel switches) installation services are available at fixed prices. Installation services for complex implementations are quoted after an assessment performed within the standard HP custom quoting process.

CASA Implementation Services include the following:

- Implementation planning and consulting for CASA.
- Hardware installation and configuration of CASA solution.
- Basic SANOS configuration including: password management, configuration of shared disk parameters, setting connections between nodes and shared disk, setting management and LAN network properties, and creating peer relationships between the nodes.
- Verify functionality of environment by performing: storage discovery, verification of host registration, creation of sample partitions and expansions, sample LUN mappings, and sample Fibre Channel Mirror and Fibre Channel Mirror configuration.
- Configure virtual LUNs and mappings per customer provided requirements and verify visibility of LUNs to the applicable nodes. The number of nodes verified is bounded by the complexity of the environment (simple, medium, or complex).
- Configuration of WAN IP addresses for each CASA and enablement of WAN interface.
- Configuration of IP Mirror relationship between source and target CASA units.
- Enablement of IP Mirror and creation of sample mirrored volume to verify functionality.
- Preparation of sample source and target LUN for Vsnap snapshot.
- Enablement of Vsnap snapshot, configuration of sample source and target LUNs to verify functionality.

The use of these services is highly recommended, particularly in complex environments.

Additional Information Sources

Refer to the CASA documentation at:

http://www.hp.com/products1/storage/products/virtualization_appliances/network/sv3000/index.html

for detailed information on supported RAID array storage devices.

Best Practices

11

This chapter describes “best practices” for implementing heterogeneous Storage Area Networks. The information contained in this chapter should be used as a guide for constructing your SAN. Although every attempt has been made to provide a best practice recommendation, some aspects of SAN implementation are a matter of preference. Also, the physical location of servers, storage, computer labs, or specific building layout and location may dictate particular aspects of your SAN implementation. In part, this is an expected reality and is often easily accommodated, given the inherent flexibility in implementing SANs and Fibre Channel technology.

Rather than just present a list of best practices, the information has been organized into these sections:

- Planning a SAN
- Configuring a SAN
- Upgrading a SAN
- Migrating SAN Topologies
- Merging SAN Fabrics
- Troubleshooting

Much of what is presented here is the result of the actual experiences of building large SANs within the internal HP engineering environment and at customer sites.

Although this chapter does describe portions of the design process in the planning phase below, it is not meant to convey the entire SAN design process. Contact an HP Enterprise Storage Consultant or the Professional Services organizations for assistance and consultation on designing SANs. HP Storage Services may be contacted through this link:

http://h18005.www1.hp.com/services/storage/index.html

Note: Much of the information in this chapter applies equally to SANs with the B-Series, M-Series, or C-Series Fabric product lines of switches. Any reference to specific switch features pertains only to the B-Series product line.

Planning a SAN

Proper planning considers both present and future requirements. This can be accomplished by over-planning your initial SAN capacity and connectivity requirements to accommodate expected future needs. Whether using an HP standard topology or designing your own topology, select a design that not only offers the best implementation for present usage, but also allows you to expand your SAN over time.

It is important that you allocate an adequate amount of time to plan your SAN. In general, the more detail you can define in the planning phase, the greater the benefit you will realize during the configuration phase.

Consider each of these items during the planning phase:

- Deployment Strategy: You can choose to deploy separate smaller SANs or SAN Islands with the idea of increasing capacity by growing the SANs independently or by interconnecting the independent SANs in the future. Smaller SANs are easier to construct, larger SANs offer economies of scale from an operational standpoint, but take longer and are more complex to build.
- Topology Design: Consider the topology design compared to the ease of migrating to another, higher capacity design. In most cases this can be accommodated; however, it is always preferable to choose an initial design that can grow, without the need to transition to a different topology.
- Experience Level: If you are just beginning deployment of SAN technology, consider starting with a smaller implementation. As you gain experience, deploy larger SANs.
- SAN Management Strategy: Refer to *Chapter 6, SAN Fabric Management Tools* and Chapter 6, SAN Storage Management Tools for information about SAN management tools. After reviewing this chapter, define the management strategy and the specific tools that you will utilize to manage your SAN.
- Technology Advances: The ideal design considers expected future technological advances, and can easily accommodate the resultant changes. Plan for flexibility in your initial design. Higher port count Fibre Channel switches and faster interconnect speeds are an inevitable evolution of Fibre Channel technology. Ensure that your initial plan addresses and can accommodate expected changes such as these.
- Document the Design: This is one of the most important aspects of the planning process. This allows you to fully review and evaluate the design beforehand, evaluate trade-offs, make changes, and effectively communicate specific plans to all groups affected. The other important benefit of documenting your design is that during the later phases of implementation, the documentation serves as the roadmap for the actual implementation.

HP recommends, at a minimum, that you document the following before beginning the actual implementation:

1. Topology Map–Shows the logical SAN topology and fabric interconnect scheme; conveys the overall design from a strategic standpoint, and can also serve to convey how future growth and technological advances will be accommodated.
2. Configuration Layout–Shows the physical layout of the entire implementation. More detailed then the topology map, the layout is used during implementation to verify the correct connectivity. This is also extremely helpful if troubleshooting is required in later phases.
3. Storage Map–Defines the storage system arrangement and configuration in the SAN, and storageset settings such as SSP and RAID levels. This map effectively defines how all of the storage is configured in the SAN.

4. Zoning Map–Defines the inter-node communication access within the SAN. This map defines which nodes or user ports are allowed to communicate with each other in the SAN.

General Planning Considerations

It is difficult to make general recommendations about the choice of a specific SAN topology. There are so many variables in large installations that each new configuration requires substantial customized design work. The following suggestions provide background information for designs that meet typical large SAN requirements and that are compatible with the future direction of StorageWorks SAN technology.

Advantages of Dual Fabric SANs

Most large SANs should have two independent fabrics. Each fabric operates independently, and the failure of one fabric does not cause a complete loss of SAN communication.

The reliability of modern electronic hardware is so high that it is difficult to make meaningful predictions of failure rates. Software is used in all components, but it is difficult to estimate the likelihood of software failures. Operator errors are the most likely cause of problems, and the frequency of operator errors depends strongly on operational discipline and employee morale, both of which are very difficult to quantify. All of these potential failure points are minimized by the use of multiple fabrics.

The advantage of dual fabric designs is that they support path failover technology. Path failover is available in most operating systems that are supported in HP SANs. Two host bus adapters are used in each server, and if the communication path from one HBA to the storage system fails, then the I/O traffic is re-routed through the other HBA.[1]

The two fabrics should be similar in size and topology. This minimizes the risk of asymmetrical performance under certain workloads, and minimizes the total cost of the SAN. Failover software does not support the concept of primary and secondary fabrics.

It should be noted that there is not an automatic increase in cost caused by the use of two separate fabrics. For example, two switches in a single fabric give about two dozen usable ports (depending on the topology). Two separate fabrics, each with a single switch, gives 32 ports at the same cost.

Many of the SAN illustrations in this document show only a single fabric. This is because most of the design and compatibility requirements apply to each fabric as a complete unit. However, practical SAN designs should have two or more fabrics, each satisfying the configuration rules described in this guide.

Data Access Patterns

There are several supported HP SAN topologies, suitable for a wide range of applications from small to very large systems. For small installations, the topology may be chosen to maximize connectivity or to minimize cost. SAN performance is not likely to be an issue for a small installation, because of the very high I/O throughput that is provided by basic Fibre Channel SAN components.

1. Failover can also be useful in SANs with only one fabric. This protects against HBA failures and certain extremely unlikely potential problems in array controllers. In general, failover technology should be used in SAN configurations that have two fabrics.

Large installations must be designed to maximize performance and minimize cost, to support current and future connectivity requirements, and to enable eventual migration to new technologies. Several factors must be taken into consideration to meet these requirements. The factors are categorized into three different data access patterns, one-to-one, many-to-one, and any-to-any.

- **One-to-one**

  The communication paths within the fabric are used in different ways, depending on the relationship between the servers and the storage systems. In some cases, each specific server stores data on only one or two storage systems. In this case, only a few specific storage systems service all I/O requests from a server, and there is little or no communication between the servers or between the storage systems. A given fabric port sends requests to one (or two) specific fabric ports. This is the traditional server-storage relationship. Many systems still operate this way today.

  From the viewpoint of the fabric, the I/O traffic has a "one-to-one" pattern, and the traffic pattern is stable. Each server sends I/Os to a small, specific set of storage systems, and each storage system is associated with only a handful of servers. Only significant changes to the configuration by the system manager will change the connection pattern.

- **Many-to-one**

  Multiple servers accessing data stored in a single centralized pool is another data access pattern. This is a common situation when high performance storage systems have enough capacity to handle a number of servers. In this environment, there is a "many-to-one" I/O traffic pattern on the SAN fabric, and the traffic pattern is stable. Each server sends I/O requests to a small set of storage systems, but each storage system may service a large number of servers. The connection pattern changes only when significant changes to the configuration are made by the system manager.

- **Any-to-any (or many-to-many)**

  In a third case, application servers access data that is distributed across many storage systems. This case may develop in several situations. The latest HP storage arrays may handle a large number of servers. (Refer to the configuration rules in this Guide for detailed information.) A system manager may decide to distribute information over a wide set of storage systems, thus requiring each application to access multiple storage systems. This situation can arise when host-based mirroring is used. Another possibility is that it may be easier to manage the data if it is partitioned and stored on multiple storage systems. For example, Accounting Department data might be stored on one storage system, and Personnel Records data on another. A server requiring access to both data types generates I/O requests to both storage systems.

  Another important situation where data is distributed across a range of storage systems is when the HP VersaStor virtualization technology is used. VersaStor distributes data over all the available storage systems in a SAN.[2] In this case, I/O requests from a given application server are handled by one or more storage systems, in a pattern that is controlled by the virtualization management appliance. In this environment, many servers access many storage systems, which is a "many-to-many" pattern. Management traffic may occur between servers, storage systems, and management appliances.

  From the viewpoint of the SAN fabric, any port may send traffic to any other port, which is an "any-to-any" pattern. Furthermore, since the virtualization manager performs dynamic reallocation of storage system capacity, the traffic patterns vary continuously without manual intervention.

2. The specific configuration details are controlled by management options.

The optimum SAN configuration depends on the I/O traffic, whether it be one-to-one, many-to-one, or any-to-any pattern.

Core and Edge Switch Concept

In the future, most large SANs will support any-to-any traffic patterns. The remainder of this chapter focuses on this problem.

The optimum fabric configuration uses a high performance “core” surrounded by a number of “edge switches.” The core provides roughly equal connection performance between any pair of ports. The edge switches provide port aggregation to match the performance requirements of the servers and storage systems to the performance of the core.

The figure below shows a large configuration that uses the core and edge switch approach. Using 16-port switches, the core is a 32 port fat tree. Four ISLs go between each switch pair in the fat tree. Two ISLs connect each edge switch to the core.

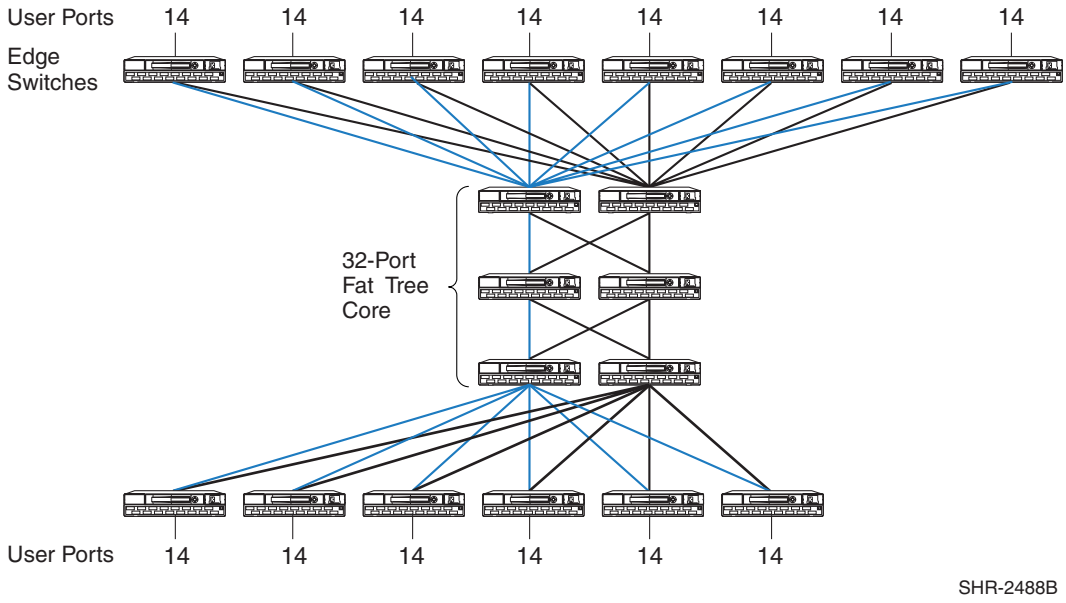


Figure 63: Example of Core Switch Plus Edge Switch Configuration

Fabric Core Options

The simplest fabric core is a single switch. Fibre Channel switches support simultaneous full bandwidth connections between any combination of port pairs. A single switch fabric core guarantees support for any-to-any traffic.

Any combination of switches has less performance than a single switch, and the difference depends on the fabric topology. The best-performing topology is the “fat tree”, which has enough Inter-Switch Links (ISLs) to provide, on the average, full bandwidth connections between any combination of port pairs. While it is possible to construct workloads that force traffic contention on the ISLs of a fat tree, which reduces the throughput, fat tree fabric core topologies provide full-bandwidth any-to-any communication, on the average, for random traffic patterns.

A related topology is the “skinny tree”, which has fewer ISLs and fewer switches. This topology introduces an unavoidable performance limit to the fabric. In many cases this limit is beyond what is required by the application servers. The process to upgrade a skinny tree topology to a fat tree topology is fairly straightforward, involving the addition of switches and ISLs to the existing tree

Edge Switch Options

The simplest edge switch is a single switch with one ISL connecting it to the fabric core. Each edge switch provides “User Ports” for connecting servers and storage systems.

The single ISL is a potential bottleneck. All the I/O traffic from the servers or storage systems connected to the edge switch must pass through just one ISL. More ISLs can be provided. Several combinations of ISL and user ports may be used. For example, with sixteen port switches, the ISL to user port ratio could be 1:15, 2:14, 3:13, 4:12, etc. Each of these combinations represents a “port aggregation ratio.” The ratios are 1:15, 1:7, 3:13, 1:3, etc.

The workload of the servers and storage systems attached to an edge switch determines the required port aggregation ratio for the switch. For lightly loaded application servers, a 1:15 port aggregation ratio may be adequate. Heavily loaded servers may require a 1:7 or 1:3 ratio. Extremely high performance servers, such as high-end HP Alpha systems, may be able to completely “fill up” a Fibre Channel connection. In this case, there is no advantage to using an edge switch, and the server should be connected directly to the fabric core. Storage systems may also be able to support a full bandwidth Fibre Channel connection.

To select the appropriate port aggregation ratio, refer to the I/O requirements of your applications and servers. This information is available for many situations by using the Active Answers application sizing tools. In other cases, measurements of an existing system may be required to determine the workload.

Designing a Subsettable SAN

In many cases, the growth pattern for a storage installation is difficult or impossible to predict. Global economic growth, conditions in a given business market, the growth rate of your company, and internal reorganizations or reallocations of computing resources may all have a significant impact on the requirements that must be met by the SAN.

To accommodate this unpredictable variability, the SAN designer should plan for growth within a predefined design. The initial installation should be a subset of a larger pre-designed configuration.

The “core plus edge switch” approach supports this strategy for SAN design.

When the time comes to expand an existing installation, the system manager can make incremental changes to the configuration rather than a complete reconfiguration of the entire Fibre Channel fabric. Changes to the fabric core are isolated from the edge switches, which minimizes the impact of changes required to support core growth. Changes to a given server’s connection to an edge switch are isolated from the core, which minimizes the impact of server-related changes. Furthermore, since two or more fabrics are in use, server I/O traffic may be temporarily forced to a single fabric while the other fabric is undergoing modification.

Start with a single switch core for a moderate sized initial installation,. When needed, the core can be expanded by replacing the switch with one that has more ports, or by reconfiguring the core to a skinny tree or fat tree topology. An existing fat tree core may be expanded by replacing it with a fat tree made up of switches with more ports, or by reconfiguring it to a wider fat tree configuration.

Use a generous estimate of the required I/O performance when selecting edge switches. A port aggregation ratio of 1:7 or 1:3 is adequate for most applications. Increasing bandwidth is a simple, localized modification, if it turns out that more is required.

The initial design should include spare ports on the core to support the future addition of edge switches. For example, consider a configuration that uses sixteen port switches, a single switch core, and edge switches with a port aggregation ratio is 1:3. This design supports up to four edge switches and 48 user ports. This would be a suitable solution for a system where 36 ports are required now, requiring three edge switches. Future growth to 48 ports can be accommodated by adding another edge switch.

SAN Design Summary of Recommendations

Enterprise-level SANs should include the following features.

- Multiple independent fabrics.
- Core plus edge switch topology.
- Appropriate port aggregation ratio, depending on application server requirements.
- Appropriate core design, depending on number of ports required.
- Subsettable design, with initial installation suitable for current needs.

By following these guidelines for SAN planning, your design will be suitable for supporting future storage technology and future growth in your storage environment.

Configuring a SAN

Once you have completed the planning phase you can begin to configure your SAN. As described in the planning phase, it is important that you document the configuration. During the configuration phase, you should be recording the details of the actual physical configuration.

- Recording. As you construct the SAN, record the cable connections and mark this information on the configuration layout diagram. Record the WWN of all nodes and devices and identify where they physically reside. It is recommended that you place a label on each Fibre Channel HBA with the WWN clearly identified. HP storage systems are pre-labeled with this information; however, you may wish to place an additional label on the front of the unit in plain view.
- Cabling. Define a system for cable labeling. Even a small SAN can include a very high number of fiber optic interconnect cables. Label both ends of each cable with the same unique cable number or color code scheme. This will allow you to quickly identify each cable uniquely. Also consider placing a label at each end of the cables that identifies connection points at both ends, such as “TO” and “FROM”. Use label types that are easy to create and read, and ensure they are attached securely to the cable.
- Protect unused or open switch ports with port plugs. Never leave ports exposed.
- Cable Dressing. Use care when routing fiber optic cable and ensure that you do not exceed the recommended minimum bend radius. For single-mode and multi-mode fiber cable the minimum bend radius is 25 mm. Where cables are bundled or hanging unsupported, use velcro tie wraps to group and support the cables. Never use plastic tie wraps as they can damage the internal fiber core if over-tightened.
- Cable Symmetry. When connecting cables, consider slot/port-numbering symmetry. Be consistent across similar servers with cabling in terms of HBA slot placement and cabling to switches. If configuring with two SAN fabrics and multi-pathing, connect HBA 1 to SAN fabric 1, HBA 2 to SAN fabric 2, etc. Cable symmetry is not a requirement, but serves as an aid to troubleshooting if this is eventually required.
- Configure Fibre Channel Switches. Although all HP Fibre Channel switches are pre-configured, verify that all Fibre Channel switches in the fabric have the same parameter settings and that each has a unique domain ID.

  Label switches using a relevant naming scheme particular to the topology. For example, if implementing a ring topology, label each switch in the ring as Ring1, Ring2. Although not an absolute requirement in all configurations, it is highly recommended that all switches utilize the same switch firmware revision. Different switch code revisions running in the same fabric are supported during a rolling upgrade. This is considered a temporarily acceptable situation for the duration of the code update.
- Configure Servers. For each platform or operating system type, utilize the appropriate HP StorageWorks platform kit to ensure that the required server drivers and configuration settings are loaded. Ensure that servers are configured with the proper operating system versions and all required updates.

  Use a numbering type scheme for naming multiple servers of the same type, such as NT01 and NT02 for Windows NT servers.
- Configure Storage. Use the storage map created in the planning phase to configure each of the storage systems. Verify server-to-storage connectivity, and access one server at a time.

When initially defining storagesets, always disable all access first, and then enable the desired individual access. For Enterprise/Modular RAID Array storage systems, define connection names to be consistent with zoning alias names. Be consistent with connection names relative to storage port and controller connection. Choose a scheme that is easily understood and quickly conveys the physical connectivity.

- Define Zones. Use the zoning map to configure zones. Consider starting with small zones that allow a smaller logical subset of a larger physical SAN to be tested initially.

  Always save old zoning configurations before and after making any zoning change. If possible, it is recommended that no zoning changes be made when an individual switch normally configured in the fabric is temporarily not available.

  You can zone by operating system or by storage system. Zoning by operating systems is useful when the operating systems are accessing storagesets that are localized to specific raid arrays. For example, NT1, NT2 and NT3 have access to storage on ARRAY1, and VMS1, VMS2 and VMS3 have access to storage on ARRAY2.

ZONE NAME	**NT_ZONE**	**VMS_ZONE**
Members	NT1	VMS1
	NT2	VMS2
	NT3	VMS3
	ARRAY1	ARRAY2

  ARRAY1 will only have host connections for the NT1, NT2 and NT3 servers and ARRAY2 will only have host connections for the VMS1, VMS2 and VMS3 servers.

  Zoning by storage system will limit the connections to the G80 to those systems actually having storagesets on them. This is useful when the storagesets for a specific system are on multiple storage systems.

  In the above example, we add 3 more NT servers and another storage system to the NT zone:

ZONE NAME	**NT_ZONE**	**VMS_ZONE**
Members	NT1	VMS1
	NT2	VMS2
	NT3	VMS3
	ARRAY1	ARRAY2
	NT4	
	NT5	
	NT6	
	ARRAY3	

  Both Array1 and Array2 will have host connections from all 6 NT systems. This may not be a problem in a small SAN, but as the SAN grows the connections will increase. Also, we do not know which of the NT servers are accessing storage on ARRAY1, and which ones are accessing storage on ARRAY2.

  If we zone by storage system we get:

ZONE NAME	**ARRAY1_ZONE**	**ARRAY3_ZONE**	**ARRAY2_ZONE**
Members	NT1	NT4	VMS1
	NT2	NT5	VMS2
	NT3	NT6	VMS3
	ARRAY1	ARRAY3	ARRAY2

  Zoning this way also makes it much easier to troubleshoot, especially if servers access storage on multiple arrays. We could have a zone that looks like this:

ARRAY1_ZONE	ARRAY3_ZONE	ARRAY2_ZONE
ARRAY1	ARRAY3	ARRAY2
NT1	NT1	NT4
NT2	VMS2	NT5
VMS2	VMS3	VMS1
VMS3	NT5	NT2
NT6	NT6	NT6

This way it is more apparent that NT1 is only accessing storage on ARRAY1 and ARRAY3. If part of storage can not be seen then it is easy to locate the source of the problem.

Due to some zoning restrictions, you may need more than one zone for a particular ARRAY. If ARRAY1 also has IBM AIX servers, we must zone that separately.

ARRAY1_ZONE1

ARRAY1

AIX_1

AIX_2

Zone and Zone Alias Names

When setting up zoning, use meaningful names for zones and zone aliases and be consistent with the naming convention throughout the fabric.

Servers are identified by the WWN of the host bus adapter. Name these by using the system name and the host bus adapter number. For example, server NT1 with one Fibre Channel HBA would have an alias of NT1_HBA1. Server NT1 with a second HBA would have an alias of NT1_HBA2

RA8000 storage systems in a transparent failover configuration will have two WWN's on the fabric, one for port 1 and one for port 2. Give each RA8000 a unique number. RA8000 number 1 could have aliases of R1_P1 (port 1) and R1_P2 (port 2)

For a multiple-bus failover configuration the RA8000 will present 4 WWNS to the fabric. If you have a multi-path NSPOF configuration, two of the WWN's will be in one fabric, the other two will be in the second fabric. Name the ports using an alias such as R2_A1 (Controller A Port 1), R2_A2 (Controller A Port 2), R2_B1 (Controller B Port1), and R2_B2 (Controller B Port 2).

Ports A1 and B2 will be cabled to the first fabric. Ports A2 and B1 will be cabled to the second fabric. The aliases in fabric 1 will be R1_A1 and R1_B2, the aliases in the second fabric will be R1_A2 and R1_B1. Keep the ports and HBAs the same throughout the setup. For example, always have HBA 1, R1_A1 and R1_B2 in fabric1 and HBA 2, R1_A2 and R1_B1 in the second fabric.

Using this convention conveys the failover mode that the RA8000 is configured for. Any alias with a P1 or P2 is in transparent mode, any alias with A1, A2, B1, or B2 is in multiple-bus mode.

Define RA8000 host connection names for the adapter WWN's in the same manner as you defined the alias name in the fabric. For example, the fabric alias name for NT1, HBA1 will be NT1_HBA1. The host connections on the RA8000 controller should match this as closely as possible.

Example:

Alias NT1_HBA1 in the fabric would have host connection names on the RA8000 of:

```
NT1-P1  WINNT   THIS   1      081200 OL this  30
HOST_ID=2000-0000-C922-8ADC     ADAPTER_ID=1000-0000-C922-8ADC

NT1-P2  WINNT   OTHER  2      081200 OL other 130
HOST_ID=2000-0000-C922-8ADC    ADAPTER_ID=1000-0000-C922-8ADC
```

Note: While storage system connection names are not case sensitive, switch alias names are. That means that the switch might have a alias name of TRU64_1 and another alias name of Tru64_1 that refer to two different sets of things.

Upgrading a SAN

Upgrading a Fibre Channel Switch

See the Installation and Hardware Guide for your switch.

Scaling a SAN

The information in this section applies to all SAN topologies, whether a custom design or HP defined.

- Replace 8-port switches with 16-port switches.
- Add additional switches, up to the limits specified for a single fabric in Chapter 3, "SAN Fabric Design Rules".
- Add a second fabric as a high availability no single point of failure solution.
- Deploy multiple independent SANs.
- Migrate to a different topology (see below).

Scaling Specific SAN Topologies

The information in this section is specific to the HP-defined topologies. Refer to the Fibre Channel switch replacement procedure elsewhere in this chapter for information about preventing fabric segmentation when adding new switches to an existing fabric.

Whenever you are expanding a topology, ensure that the new switch and device connectivity is consistent with the original SAN topology design requirements and goals. Avoid making changes to the topology that may serve to disrupt the original topology design goals. If you need to make topology changes based on a change in data access requirements, consider migrating to a different topology that is better suited to meet these needs. It is important in any expansion that the original data access needs be maintained.

If you have implemented a high availability fabric design (refer to Chapter 2, "SAN Topologies"), it may be possible to expand your SAN in a non-disruptive manner. It is highly recommended, however, as a precaution, that all data be backed up and that I/O activity quiesed when adding new switches to the fabric.

Cascaded Fabric

Expand an existing cascaded fabric by connecting a new switch to an available port on an existing switch. If there are no available ports, remove a device or set of devices from an existing switch, connect the new switch to those ports, and connect the device or devices to the new switch.

Meshed Fabric

Expand an existing meshed fabric by connecting a new switch to available ports on an existing switch. If there are no available ports, remove a device or set of devices from an existing switch, connect the new switch to those ports, and connect the device or devices to the new switch. To maintain the meshed topology, you must ensure that there are multiple paths (ISLs) connecting the new switch to the existing meshed fabric.

Ring Fabric

Expand an existing ring fabric by breaking the ring and inserting another switch into the ring.

Add new switches cascaded off of the ring, up to the maximum number of switches supported in a single fabric. When expanding outside of the ring, ensure that no two devices that need to communicate are more then seven hops apart.

Tree Backbone Fabric

Add edge switches. Expand an existing Tree Backbone SAN fabric by adding additional edge switches. Connect these edge switches to available ports on the one or two backbone switches.

Add a second backbone switch (if your current design only contains one). Connect all of the edge switches to the new backbone switch.

Migrating SAN Topologies

This section describes how you can convert from one topology type to another if required. HP highly recommends that you thoroughly review your initial design to ensure that it meets your present and future requirements in order to avoid having to modify your initial topology design. There may be situations, however, based on changes in business requirements, that require you to consider converting to another topology type. For those circumstances, information is provided below that can help you gain an understanding of how the different topologies can be converted.

As described in the planning phase, it is important that the SAN fabric topology be well documented. If you are required to change from one topology type to another, use the existing topology diagrams to determine the most efficient manner in which to modify the topology. Create a new diagram that details the desired final connectivity scheme and use this as a map for the topology migration or conversion.

If you have implemented a high availability fabric design, depending on the specific cabling changes required, it may be possible to migrate your SAN in a non-disruptive manner. It is highly recommended, however, as a precaution, that all data be backed up and that I/O activity be quiesced when migrating or reconfiguring any portions of the fabric.

If you have implemented a two-fabric, no single point of failure (NSPOF) SAN, you have the ability to failover over all operations to one fabric while you reconfigure the other fabric. This makes it possible to perform a totally non-disruptive topology migration.

- As a general rule, migrations that only require the addition or re-cabling of ISLs are less disruptive then migrations that require devices be moved from one switch to another. When planning a migration, try to avoid or minimize scenarios that require moving devices from one switch to another.
- Cascaded to a Meshed Fabric. Whether you have implemented a linear cascade or branched cascade of switches from one top switch, additional ISLs are required to connect all switches together as required in a mesh fabric design. Proper planning requires that you carefully calculate the number of additional ports that are needed for the additional ISLs. This may require that devices be moved from one switch to another.
- Cascaded to Ring Fabric. If you have implemented a linear cascade, connect the last switch in the cascade to the first switch to create a ring fabric. For a branched cascade, extensive ISL re-cabling may be required.
- Cascade to Tree Backbone Fabric. Whether you have implemented a linear cascade or branched cascade, determine which switch or switches will be utilized as the backbone (typically no devices) and which switches will be edge switches. Connect all edge switches to the backbone switch or switches; connect all devices to the edge switches. This conversion is less disruptive if you add new switches to the fabric for the backbone and use all of the existing switches as edge switches. In this case, you can simply connect one end of the existing ISLs to the new backbone switches.
- Meshed to Ring Fabric. A meshed fabric can be converted to a ring fabric by simply removing the cross-connected ISLs, leaving the outer connected ISLs connected as a ring. The available ports can be utilized as additional redundant ring ISLs or for additional devices.
- Meshed to Tree Backbone Fabric. Determine which switch or switches will be utilized as the backbone (typically no devices) and which switches will be edge switches. Connect all edge switches to the backbone switch or switches; connect all devices to the edge switches. This conversion is less disruptive if you add new switches to the fabric for the backbone and use all of the existing switches as edge switches. In this case, you can simply connect one end of the existing ISLs to the new backbone switches.

- Ring to Meshed Fabric. If you have implemented two ISLs between all switches in the ring, move one end from an ISL between any two switches to the appropriate switch based on the final mesh design. Repeat this for all of the second ISLs between any two switches. There may be an optimal place to "break" the ring relative to re-cabling. Evaluate different scenarios prior to performing the actual conversion.
- Ring to Tree Backbone Fabric. Determine which switch or switches will be utilized as the backbone (typically no devices) and which switches will be edge switches. Connect all edge switches to the backbone switch or switches; connect all devices to the edge switches. This conversion is less disruptive if you add new switches to the fabric for the backbone and use all of the existing switches as edge switches. In this case, you can simply connect one end of the existing ISLs to the new backbone switches. It is also less disruptive if you have implemented 2 ISLs between all switches in the ring in your original design.

Zoning Rules and Guidelines

Configure the zones based on the 'zoning map' prepared during the SAN planning stage. There are several possible supported ways to configure zones and let us examine briefly these before looking at suggested guidelines for each of the product series.

First of all, one need to understand the distinction between configuring the zones and zoning enforcement within the switches and any correlation between the two. This may vary from product to product and hence the following paragraphs describe some general description about each of them, followed by specific details on all HP supported switches.

Note: When enabling a new configuration, it is strongly recommended that the fabric be quiesced. Zone membership should not be changed for devices that are actively performing I/O in a fabric. Once the new zoning is enabled, a state change notification is sent to all the nodes that have registered to receive the state change.

Zoning enforcement

Generally there are three types of zoning enforcement/authorization techniques in use in FC switches today.

Access Authorization

Access authorization provides frame level access control in hardware and verifies SID-DID combination of each frame and allows the frame to be delivered to the destination if that is a valid combination per the zone definition. This is definitely more secure and generally referred to as "hard zoning", and requires hardware resources at the ASIC level to implement this.

Discovery authentication

Zoning enforcement or protection of unauthorized access is only provided during access to the Name Service directory where the switch or fabric presents only a partial list of devices from the NS directory corresponding to the partition in which the requesting device is part of. This type of zoning enforcement is generally referred to as "soft zoning". While this is secure enough in most of the cases, it is prone to security threats if malicious hosts attempt to access unauthorized devices violating FC-Protocols.

Login Authentication

Some switches enforce authentication during fc protocol login frame level like PLOGI/ACC/ADISC/PDISC etc, in addition to providing discovery authentication. For example, if a host sends a PLOGI to a device that is not part of its zone, this frame gets dropped before reaching the destination. This type of enforcement has some additional protection compared to discovery authentication, but still not the same as access authorization at every frame level.

Zoning Configuration

Domain/port numbers

Zones can be defined using switch domain ID and port number combination to uniquely identify zone members. Advantage of this type is primarily ease of configuration and zoning definition remains intact even when an HBA or target controller is replaced with another having a different "world wide name". Disadvantage is that there is no flexibility to move around devices in the fabric and as soon as any device is moved to a different port in the switch/fabric it will not be part of the zone any more.

WWN

Zones can be defined using device WWN to uniquely identify zone members. Advantage of this type of definition is zoning definition remains intact even when the device is moved to a different port/switch in the fabric. Disadvantage is that whenever an HBA is replaced with another, having a different WWN, zoning definition has to be changed accordingly.

Mixture of both

Zones can be defined using combination of switch domain ID /port number as well as WWNs to uniquely identify zone members. Advantages and disadvantages as described in the above two methods are applicable to individual zone elements based on their definition.

Note: Movement of devices within the fabric, as described above depending on zoning definition, is only applicable from a zoning perspective. However, there can be other restrictions that will not let movement of devices within the fabric, irrespective of zoning type in effect. For example, some OSs like HP-UX which create device filenames based on 24-bit fabric address will not allow moving the device to a different port since it will change the 24-bit port address and hence will be treated as a different device.

There should not be any dependency between the way zones are configured and the way zones are enforced -meaning it should be possible to have any combination of zoning configuration/zoning enforcement from the above definitions. Due to implementation limits certain switch products impose restrictions the way zones are defined and the way zones are enforced.

The following tables and paragraphs detail how zoning is implemented followed by suggested guidelines for HP supported switches.

B-Series Product Line Switches

Table 55: Zone Types on HP B-Series Product Line Switches

Switch Models	Configuration	Enforcement	Comments
Compaq StorageWorks SAN Switch-8, SAN Switch 8-EL; SAN Switch-16 SAN Switch 16-EL; SAN Switch Integrated/32, SAN Switch Integrated/64 (FC-6164) (All 1Gb switches)	Define zones using all domain#,port# Define zones using only WWNs Define zones using combination of domain/port numbers and WWNs	Access authorization at frame level in hardware Discovery authentication Name Servers (NS) directory based Discovery based authentication	HARD zoning SOFT zoning SOFT zoning
Compaq StorageWorks SAN switch 2/8-EL, SAN switch 2/16-EL, **HP reseller** FC-8B, FC-16B(SAN switch 2/16); **HP StorageWorks** Core switch 2/64; SAN switch 2/32 (All 2Gb switches)	Define zones using all domain#,port# Define zones using only WWNs Define zones using combination of domain/port numbers and WWNs	Access authorization at frame level in hardware Access authorization at frame level in hardware Name service plus login authentication	HARD zoning HARD zoning SOFT+ (NS authentication plus login protection)
QuickLoop Zoning (all QL supported switch models)	Define zones using ALPAs, Domain/port numbers or combination of the above	Implemented in hardware tables, access prevented by hardware between unauthorized devices	HARD zoning

Maximum Zone Size

Generally the supportable 'maximum number of zones' and 'maximum members in a zone' are very large and are usually constrained by memory usage. These numbers are far larger than the maximum devices that could be connected in fabric configurations currently supported and hence usually there are no limitations on zone sizes.

However, there is an exception in pure hardware enforced zoning environment on all the above 2Gb switch models where it's likely that we exceed some preset architectural limits in which case those ports transition from HARD enforcement to SOFT type.

The current B-Series switches have a limitation of 64 unique SID entries per quad (pre-defined groups of 4 ports) and whenever this limit is exceeded the affected port/ports will transition from hard to soft enforcement.

This transition is completely transparent to fabric operations, though switch administrator may see warning messages displayed in switch logs. However, data integrity is completely preserved during this transition and HP validated this in large SAN configurations.

The following CLI output indicates a port transitioning to soft zoning:

```
WARNING ZONE-ZONEGROUPADDFAIL, 3, WARNING - port 7 Out of CAM
entries

WARNING ZONE-SOFTZONING, 3, WARNING - port 7: zoning enforcement
changed to SOFT
```

These two messages are related and indicate that the zoning configuration has outgrown internally preset architectural limits, thereby forcing the mentioned port be switched from hardware-enforced zoning to software-enforced zoning. It is important to note that only this specific port has turned "soft" and all other members that were zoned with the relevant port still remain hardware-enforced.These warning messages could be seen either statically at zoning configuration/setup time (in case if port-level zoning) or dynamically at run time (in case of WWN zoning).

The command "portzoneshow" will display the status of all ports as follows:

Hard - hardware enforcement

Soft - Name Server plus ASIC assisted authentication

All - no zoning enforcement

Zoning Guidelines (B-Series switches)

The following are suggested best practices only. However, other zoning configuration methods and zone types as appropriate for each switch are also supported.

- Define zones using WWNs always. All switch models support this type of definition, irrespective of zoning enforcement technique they use, whether it is hardware enforced or name server based or combination of both. Use port WWNs and not node WWNs.
- Exception: For all 1Gb fabric switches, define zones using domain/port numbers for selecting hardware enforced zoning
- Define zones for all devices in a fabric whenever any zone is defined. In other words do not define zoning partially for few devices in the fabric and leave others un-zoned.
- Overlapped zones can be defined and there is no upper limit on the number of zones and number of members in a zone
- Configure zones based on operating environment, on a “per OS” basis,
  See the SAN/Platform zoning requirements for individual storage arrays for exact details, as defined in Chapter 4.
- Switch zoning provides security at the port level only and for maximum security in a SAN environment, it's required to use array based LUN security- Secure Manager for XP/VA arrays and SSP (Selective Storage Presentation) for HSG/HSV array controllers.
- To minimize/avoid "soft" port transition/s in pure hardware enforced zoning environment(2Gb SAN fabric switches)
- Maintain locality as defined in your SAN design but avoid hosts/targets on the same quad. Quad is a group of pre-defined consecutive 4 ports (0-3,4-7,8-11,12-15 etc).
- Maintain a connectivity model that populates each quad with the members of the same zone or in other words avoid members of different zones on the same quad particularly when each of them are part of bigger zones. For example, if we have an UNIX zone and an WINDOWS zone, populate all UNIX zone members on one quad and WINDOWS members on a different quad.
- Minimize zone entries by including hosts and targets that practically need to talk to each other. For example, instead of combining all hosts of the same OS type into one zone, consider making smaller zones with only hosts and targets that need to talk to each other.

- Switch CLI command "portzoneshow" can be used to display and verify the individual status of each port whether it's "hard" or "soft" at any given time.

C-Series Product Line Switches

Table 56: Zone Types on HP fabric switches

Switch Models	Configuration	Enforcement	Comments
Cisco MDS 9506 Cisco MDS 9509 Cisco MDS 9216 Cisco MDS 9120 Cisco MDS 9140	Define zones using all domain#/port# Define zones using all WWNs Define zones using a combination of domain#/port# and WWNs	Access authorization at frame level in hardware	HARD zoning

M-Series Product Line Switches

Table 57: Zone Types on M-Series Product Line Switches

Switch Models	Configuration	Enforcement	Comments
HP Surestore FC-64 Compaq StorageWorks SAN Director 64 1Gb director class switches	Define zones using all domain#,port#	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)
	Define zones using only WWNs	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)
	Define zones using combination of domain/port numbers and WWNs	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)
HP StorageWorks Edge Switch 2/16 Edge Switch 2/24 Edge Switch 2/32 Director 2/64 Director 2/140 (All 2Gb switches)	Define zones using all domain#,port#	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)
	Define zones using only WWNs	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)
	Define zones using combination of domain/port numbers and WWNs	Discovery authentication Name Servers (NS) directory based Access authorization at frame level in hardware	SOFT zoning Hard Zoning (5.01.00-24 and above)

Note: In Open Fabric mode (which is the default mode), director/edge switches allow only WWN based zoning configuration.

Maximum Zone Size

The supportable 'maximum number of zones' and 'maximum members in a zone' are very large and are usually constrained by memory usage. These numbers are far larger than the maximum devices that could be connected in fabric configurations currently supported and hence there are no limitations on zone sizes.

Zoning Guidelines (M-Series switches)

The following are suggested best practices only. However, other zoning configuration methods and zone types as appropriate for each switch are also supported.

- Define zones using WWNs always. All switch models support this type of definition. Use port WWNs and not node WWNs.
- Define zones for all devices in a fabric whenever any zone is defined. In other words do not define zoning partially for few devices in the fabric and leave others un-zoned.
- Overlapped zones can be defined and there is no upper limit on the number of zones and number of members in a zone
- Configure zones based on operating environment, on a “per OS” basis.
  See the SAN/Platform zoning requirements for individual storage arrays for exact details, as defined in Chapter 4.
- Switch zoning provides security at the port level only and for maximum security in a SAN environment, it's required to use array based LUN security- Secure Manager for XP/VA arrays and SSP (Selective Storage Presentation) for HSG/HSV array controllers.

Special considerations in zoning (for all switch models)

- In high availability environments like HP-UX service guard, it is required to have homogeneous OS environments on a storage array port and this can be achieved by securing LUNs using array secure manager software and also by properly configuring zones.
- Software environments like OVSAM and CommandView for XP/VA do not impose any restrictions on switch zoning. The same supportability exists in these environments as well.
- SANs with Data Protection (tape back up) may require separate rules. Contact your HP representative for more information.

Merging SAN Fabrics

This section describes the process for merging two (or more) independent fabrics into a single, larger fabric. This is typically done when you:

- have grown independent SAN islands to the point where more resources are needed
- wish to share the resources in two or more fabrics
- wish to make information in one SAN available to servers in another SAN

With support for longer distances you may also desire to connect geographically separated SAN islands together into a single SAN, spanning across very long distances.

Although StorageWorks SAN designs and components allow versatile configurations, HP highly recommends that you thoroughly review all SANs to ensure they will meet existing SAN rules after they are merged into a single fabric. The newly created fabric should not exceed any existing SAN rules.

Merging fabrics can be a complicated process, especially if the fabrics are large. The procedures in the document require a complete understanding of fabrics, zoning commands, and rules. They also require that the user understand how to use the telnet commands as well as the web-based GUI.

It is important to consider not only current SAN configurations but any future SAN needs that may be required. Most difficulties related to merging SANs are due to the fact that not enough planning was put into future SAN considerations at the time the initial SAN was designed and built. Another problem is that the SANs being merged may be implemented differently.

When fabrics discover each other they must go through basic login procedures, or sanity checks, to determine if they are compatible to work as one fabric. If the discovery process determines they are not compatible then the fabric will segment. This means that although they are physically connected, they will still run as separate fabrics.

When zoned fabrics merge they append their zone configuration database to include each fabric's zone configurations. If a non-zoned fabric merges with a zoned fabric, all zoning information is proliferated to the non-zoned fabric switches. If there was a zone configuration enabled at the time of the merge, then that zone configuration will be enabled on the non-zoned fabric switches as well. This means that any devices that were in the non-zoned fabric will be not accessible until they are added into the current enabled configuration.

Please review these causes of SAN segmenting prior to physically connecting multiple fabrics together.

- *The name of a zone object in one fabric should not be used for a different type of zone object in the other fabric (Zone type mismatch).* In other words, if you create a zone name on Fabric A, that same name should not be an alias or configuration name in Fabric B; otherwise the fabrics will not merge.
- *The definition of a zone object in one fabric is different from its definition in the other fabric (Zone content mismatch).* If an alias, zone or configuration name is the same on both Fabric A and B but the content or definition of that object is different between the fabrics the fabrics will not merge.
- *Zoning is enabled in both fabrics and the zone configurations that are enabled are different (Zone configuration mismatch).* Because of this mismatch the switches within each fabric are not going to assume one fabric has the correct zone configuration enabled. The fabrics will not merge until one of the merging fabrics has its zone configuration disabled.

- *Not only must each switch within a fabric have a unique domain ID but each switch within the multiple fabrics of the enterprise should have a unique id as well.* For example, If Fabric A has five switches with domain IDs 1 through 5 and Fabric B has five switches with the same domain IDs these two fabrics will not merge until all switches within both fabrics have a unique domain ID.

Note: If you use port level zoning, changing the domain ID's may affect access to devices. Port level zones are based on the domain ID and the port number.

Note: When enabling a new configuration, it is strongly recommended that the fabric be quiesced. Zone membership should not be changed for devices that are actively performing I/O in a fabric. Once the new zoning is enabled, a state change notification is sent to all the nodes that have registered to receive the state change.

Merging fabric together can be accomplished by simply disabling the effective configuration on one fabric, then plugging both fabrics together. The problem with this method is that once you disable the effective configuration, you open up that fabric so all servers will see all storage. Also once you plug the fabrics together, devices from the second fabric will not be accessible until you add them into the effective configuration.

To merge these two fabrics without having to disable the effective configuration for the entire fabric, it is necessary to disable at least one switch in each fabric or have a spare switch available. This will be the switch used for merging the zones and creating the new configuration. Keep in mind that there can be multiple defined configurations, but only one can be the effective or enabled configuration.

Troubleshooting

The following section describes troubleshooting steps for isolating problems related to storage access. When initially building a SAN, lack of access either to individual storagesets or entire storage systems is not uncommon. This can usually be traced to an incorrect device setting or an inadvertent cabling or configuration setup error in the initial hardware configuration. The steps listed will assist you in isolating access problems.

1. On the server:
   a. From the server, determine if lack of access is to all of the storage (the entire storage system) or only to a portion of the storage (specific storagesets). If there is no access to only a portion of the storage system, refer to step 3.
   b. If access is not available to the entire storage system, verify from the server that the correct driver versions are loaded and that all parameters for the driver are correct. For multi-path applications, verify that the multi-path software is set up correctly.
   c. Verify that all Fibre Channel cables are plugged in and that all green indicator LEDs are on.
   d. Examine the event or error logs on the system.
2. On the Fibre Channel switch to which the server is connected:
   a. Verify the appropriate cable connection and that the port Link LED is on.
   b. Execute commands on the switch and verify that the server HBA is logged into the fabric correctly. Verify the correct port connection: F-Port, L-Port public, or L-Port private (refer to the specific HBA for more information on the correct login port types).

      F-Port: Tru64 UNIX, HP OpenVMS, HP-UX Fabric, Linux, Microsoft Windows NT, Windows 2000, SGI IRIX, and Sun Solaris.

      L-Port, 1 public: Novell NetWare.

      L-Port, x private, x phantom: HP-UX FC-AL.
   c. Verify all switch configuration and parameter settings.
   d. Verify that the switch is in the fabric and not segmented.
   e. Verify that all E-Ports are online.
3. On the Fibre Channel switch to which the storage is connected:
   a. Verify the appropriate cable connection and that the port green indicator LED is on.
   b. Execute commands on the switch and verify that the server HBA is logged into the fabric correctly. Verify the correct port connection: F-Port or L-Port private.

      F-Port: MA6000, MA/RA8000, EMA/ESA12000, EMA16000 set to FABRIC Topology.

      L-Port, x private, x phantom: MA6000, MA/RA8000, EMA/ESA12000, EMA16000 set to LOOP_HARD Topology.
   c. For MA6000, MA/RA8000, EMA/ESA12000, EMA16000:

      Verify the connections to the storage system. Execute a “show connections” command at the CLI and verify that the server connection is “online.” Verify the connections are named correctly.

4. On the storage system:
   a. Verify correct controller settings and configuration, “show this” and “show other.”
   b. Verify that the controller ports are online and configured for the correct topology setting.
   c. Verify that the storagesets are online to the appropriate controller without errors.
   d. Verify that the storagesets are correctly configured and enabled for access, “show unit dn.”
   e. Verify that unit offset parameters are correct. Also verify that the appropriate storage controller port is indicated in the connection name that will be accessed by the unit you have enabled.
   f. Verify that the connection OS parameter type is set correctly for the operating system that is using the connection.
5. General Fibre Channel switch verification:
   a. If zoning is in effect, verify that the effective zone matches the enabled zone.
   b. Verify that all zone definitions are correct.
   c. Verify that zoning alias/nick names are assigned to the correct WWNs.
   d. Verify that the servers and storage being accessed are in the same zone. If zoning is in effect, the WWN must be in a zone that is in the enabled configuration or it will not have access to the fabric.
   e. From the switch GUI, examine the name server table. Verify that the appropriate WWNs are listed and what zones they are in. Verify that the zones required are in the enabled configuration.
   f. Fabric segmentation occurs when you connect together two switches or two fabrics and one of the following mismatch conditions exists between them:
      — Zoning configuration mismatch
      — Zoning type mismatch
      — Zoning content mismatch
      — Switch configuration parameter mismatches

Note: All switches in a fabric must have the same switch parameter settings with the exception of the following parameters:
switch name
IP address
domain ID

If you are experiencing fabric segmentation, carefully review and compare these settings in each of the two switches or fabrics.

6. QuickLoop verification:

Note: QuickLoop is only required for HP-UX private loop attachment.

   a. Verify that the QuickLoop license is installed.
   b. Verify that the switch ports are set to QuickLoop mode.
   c. If using QuickLoop with two Fibre Channel switches, verify that the switches are in a QuickLoop partnership.

glossary

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

Access Authorization
Also know as hard zoning or port zoning.

ACS
Array Controller Software. The firmware that runs HSG80-based storage systems.

arbitrated loop
See FC-AL

Asynchronous Transfer Mode (ATM)
Communications networking technology for LANs and WANs that carries information in fixed-size cells of 53 bytes (5 protocol and 48 data)

B-Series Product Line
Fibre Channel switches typically manufactured by Brocade.

C-Series Product Line
Fibre Channel switches typically manufactured by Cisco Systems.

Continuous Access EVA
This storage-based HP StorageWorks product consists of two or more EVA storage systems performing disk to disk replication, along with the Continuous Access management user interface that facilitates configuring, monitoring and maintaining the replicating capabilities of the storage systems.

Continuous Access Storage Appliance
This is a storage appliance based HP StorageWorks product consisting of two or more storage appliances with some number of attached storage systems performing disk to disk replication, along with the management interface that facilitates configuring, monitoring and maintaining the replicating capabilities of the storage appliances.

Continuous Access XP
This a XP storage-based HP StorageWorks product consisting of two or more XP storage systems performing disk to disk replication, along with the management user interface that facilitates configuring, monitoring and maintaining the replicating capabilities of the storage systems.

controller pair
Two interconnected controller modules which together control a disk array

Corporate Fabric
A SAN fabric using HP StorageWorks SAN Switch 8, 16, 8EL, and 16EL model switches. A Corporate Fabric can also include the SAN Switch Integrated 32/64 model switch.

Director Fabric
A SAN fabric using HP StorageWorks Director 64 or 2/64 model switches

Discovery Authentication
Also known as soft zoning or WWN zoning.

DRM
DRM is a storage-based HP StorageWorks product consisting of two or more storage systems performing disk to disk replication, along with the management user interface (DRM-UI) (only available from services) that facilitates configuring, monitoring and maintaining the replicating capabilities of the storage systems.

Enterprise Virtual Array
The StorageWorks Enterprise Virtual Array is a high performance, high capacity, and high availability storage solution for the high-end enterprise class marketplace. Each Enterprise Virtual Array storage system consists of a pair of HSV virtualizing storage controllers and the disk drives they manage.

Enterprise/Modular RAID Array
Storage system based on an HSG60 or HSG80 controller. These systems include MA6000, MA8000, RA8000, EMA12000, EMA16000, and ESA12000 storage systems

Entry-Level Fabric
A SAN fabric using HP-Compaq C8 model switches

fabric
A network of at least one Fibre Channel switch and attached devices.

failover
This term is context-specific.

- Fabric or path failover - the act of transferring I/O operations from one fabric or path to another.
- Controller failover - when a controller assumes the workload of its partner.

Fibre Channel Arbitrated Loop (FC-AL)
A Fibre Channel topology that links multiple ports (up to 126) together on a single shared simplex media

gigabit interface converter (GBIC)
The hardware devices inserted into the ports of the Fibre Channel switch that hold the Fibre Channel cables. GBIC devices are available for short-range applications (0.5 to 500 meters), long-range applications (up to 10 km), and very long distances (up to 100 km)

gigabit link module (GLM)
A 1 Gbps fibre optic transceiver

Heterogeneous SAN:
A SAN is defined as heterogeneous if it contains one or more of the following items:

- Different operating system types
- Servers, storage systems, or Fibre Channel switches from different vendors
- Storage systems from the same vendor that are implemented with different architectural designs requiring different SAN interoperability rules

hop
One or more interswitch links between a pair of Fibre Channel switches

Host Bus Adapter (HBA)
An adapter used to connect the host server to the fabric

in-band communication
Communications that uses the same communications pipe as the operational data. See also out-of-band communication.

inter-switch link (ISL)
A fibre cable connecting a port on one switch to a port on another switch

M-series Fabric Product Line
Fibre Channel switches typically manufactured by McDATA.

out-of-band communication
Communication that uses a different communications pipe than that used by operational data. See also in-band communication.

Selective Storage Presentation (SSP)
This feature provides the ability to restrict access to a given Fibre Channel LUN.

SFP (small form factor pluggable GBIC)
A 2-Gbps GBIC.

Storage Area Network (SAN)
A high-speed network that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users, typically using Fibre Channel technology

VCS
Virtual Controller Software. The firmware that runs the Enterprise Virtual Array storage systems.

Wavelength Division Multiplexing (WDM)
The technique of placing multiple optical signals on a single optical cable simultaneously. Dense wavelength division multiplexing (DWDM) places many signals on a cable. Coarse wavelength division multiplexing (CWDM) places only a few signals on a cable.

Zone
A collection of device or user ports that are permitted to communicate with each other through the fabric. Any two device or user ports that are not members of at least one common zone are not permitted to communicate through the fabric.

index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z