

**STORAGE AREA
NETWORK**

Native Fabric Connectivity for Today's SANs

Brocade offers a wide range of SAN fabric interconnect solutions to provide flexible deployment options that help maximize customer hardware investments.

BROCADE

Brocade® is committed to providing native fabric compatibility throughout its integrated family of Storage Area Network (SAN) platforms. This means that SAN users can expand their existing SANs and build new SANs in the most seamless, efficient, and supportable manner possible. Brocade native connectivity is a key component of the Brocade Data Center Fabric (DCF) architecture, a framework that helps organizations transform their data center infrastructures for maximum performance, flexibility, and investment protection.

This paper describes the various approaches Brocade is taking toward heterogeneous fabric connectivity, including:

- **Native Connectivity Challenges**
- **Heterogeneous Platform E_Port Mode Connectivity**
- **Brocade E_Port Native Connectivity**
- **Brocade Routing Native Connectivity**
- **Brocade Access Gateway Native Connectivity**

BROCADE IN 2007

Brocade's acquisition of McDATA in 2007 created a tremendous opportunity for users of SAN technology to leverage the fabric connectivity approaches available from the merged organization. Brocade views compatibility between Brocade Fabric OS® (FOS) and Brocade M-Enterprise OS (M-EOS) platforms as a top priority. Now that Brocade is leading the design and development processes on both sides of the inter-switch connection, connectivity issues between FOS and M-EOS fabrics are resolved very quickly. An example of this capability was the first switch released by Brocade since the completion of the acquisition: the Brocade 5000 Switch, which connects to any FOS or M-EOS platform in either McDATA Fabric or Open Fabric mode. Brocade has subsequently developed additional products that continue to expand options for SAN users, maximizing flexibility for fabric connectivity.

In the past, a major factor inhibiting fabric interoperability for all SAN switch vendors was the requirement to reverse-engineer the Inter-Switch Link (ISL) connection behavior. The process was limited by incomplete information about what the other vendor was doing and was always subject to last-minute changes in firmware updates. This lack of visibility into what the connecting switch is doing and sensitivity to change makes reverse-engineering an extremely difficult challenge. As a result, the process consumes both time and money and creates a greater potential for problems. Fortunately, for the majority of SAN customers, the integrated Brocade FOS and M-EOS design and development process has remedied this situation.

The ability of Brocade to reliably test and certify FOS and M-EOS product connectivity can:

- Enable basic connectivity and communications between FOS and M-EOS switches
- Support the full intelligent fabric services feature sets of both FOS and M-EOS platforms without causing fabric disruption or compromising functionality
- Enable non-disruptive upgrades and connectivity enhancements to both FOS and M-EOS for sustainable, ongoing interoperability
- Guarantee end-to-end support for comprehensive troubleshooting and firmware updates

Device interoperability within a SAN today is commonplace, since no single vendor provides switches, storage nodes, and host nodes (HBAs). In fact, virtually every SAN has more than one HBA vendor and multiple storage vendors (a disk vendor and a tape vendor, or two different disk vendors, for example). SAN device interoperability is well understood: SAN vendors provide comprehensive interoperability matrices and have extensive experience designing, implementing, managing, and troubleshooting heterogeneous SANs.

Much less common is native connectivity, in which host and storage nodes communicate using interconnected Fibre Channel switches based on different platforms and a single fabric mode. One or more switches providing connectivity for storage and hosts must have common services and settings to operate with stability and full performance. When switches based on different platforms are connected, they must each recognize the fabric mode of the other and exchange information. In this way, they can see if they are both configured in a compatible fabric mode. If so, they can form a fabric, and the fabric can function correctly over time.

Information shared by switches in a fabric includes:

- The nodes on the fabric (name server)
- Which nodes can communicate (Zoning database)
- How nodes on different switches reach each other (FSPF)
- Fabric-wide change announcements (RSCNs)
- Fabric-wide parameters, such as timeout values

These issues highlight the importance of robust native connectivity solutions based on intimate knowledge of the unique firmware code and behaviors of each platform. Also, thorough testing must be done and support facilities employed to ensure that fabric interoperability solutions will be stable in enterprise environments.

NATIVE CONNECTIVITY CHALLENGES

Even if vendors follow Fibre Channel standards, coordinating fabric information between heterogeneous platforms can still be an issue for fabric interoperability. Similar to other standards, Fibre Channel standards define a base level of functionality upon which every vendor then adds features and increased capabilities. Moreover, each vendor can interpret these standards differently. As a result, two vendors can follow the standards strictly, yet fabric connectivity still remains difficult or impossible without additional configuration and support efforts. Secondly, standards are constantly in a state of development and vendors usually implement standards that are in draft form, which can lead to other fabric connectivity issues.

Native connectivity introduces additional challenges to the SAN, including:

- Management interface inconsistencies in fabric topology, node port states, zoning, and performance measurement
- Slow fabric recovery when a switch, Inter-Switch Link (ISL), or node is added or removed from the fabric
- Fabric merges failing due to slight differences in how each platform interprets the relevant standards

Platforms and Native Connectivity

The term “platform” used throughout this paper means the operating system of a Fibre Channel (FC) switch or director, commonly called “firmware.” Platforms not only have different features and management interfaces but also have different fabric modes. Brocade FOS, Brocade M-EOS, and Cisco SAN-OS are all examples of platforms. The term “native connectivity” refers to the ability to connect products of one platform (for example, FOS) to products of another platform (for example, M-EOS) in a particular fabric mode (McDATA Fabric, Open Fabric) with each platform retaining the unique features of its firmware-based OS. Native connectivity between different platforms ensures stable operation of the storage network and provides customers with the flexibility to deploy fabric assets at will.

Brocade and Fibre Channel Standards

Brocade is well-positioned to implement native connectivity in the SAN, because it pioneered Fibre Channel switching, has written or co-written more than half of the Fibre Channel standards, and has a strong presence on the ANSI T11 committees that define Fibre Channel standards. Brocade is also a leader in the Storage Networking Industry Association (SNIA) standards initiatives for SAN management and security.

- Device discovery issues because of the name servers not synchronizing
- Potential discrepancies in the way different vendors implement security features and how they behave

In addition, switch vendors implement special features to differentiate their products. These features by definition are usually not interoperable because they are based on technology developed and owned by one vendor. In many cases these special features pre-date any relevant standards and tend to be common in operational SAN environments today.

Native connectivity is currently required in the following situations:

- Seamlessly migrating a fabric from platform X to platform Y
- Optimizing ports, when a fabric of platform X's switch is out of ports while a fabric of platform Y's switches has many ports available
- Temporarily merging platform X and platform Y fabrics for an array migration or other infrastructure change
- Merging two organizations that require a single SAN with switches based on heterogeneous platforms

Of these scenarios, the most common are the first two: fabric migration and port optimization. Even though migration is typically planned as a temporary measure, it can end up staying in place for the long term due to operational restrictions on application downtime.

Depending on the requirements for fabric connectivity, Brocade offers a wide range of interoperable solutions:

- Brocade and its partners provide an option for direct E_Port (switch-to-switch) interoperability between FOS and M-EOS switches and directors for a wide range of hardware and firmware combinations and for both McDATA Fabric and McDATA Open Fabric modes.
- Brocade Fibre Channel Routing (FCR) technology enables hosts and storage in different fabrics based on different platforms to communicate in a secure, controlled manner. Fibre Channel Routing support includes router connections to both McDATA Fabric and McDATA Open Fabric modes.
- Brocade Access Gateway, a feature of Fabric OS, is an approach to native connectivity supported on Brocade blade server SAN switches and on certain Brocade switches running Fabric OS 5.3.0 or later. This feature simplifies server and storage connectivity by enabling direct connection of servers to existing SAN fabrics, thereby eliminating traditional heterogeneous switch-to-switch connectivity challenges. Access Gateway connectivity is supported for M-EOS fabrics running in either McDATA Fabric or McDATA Open Fabric mode.

HETEROGENEOUS PLATFORM E_PORT MODE CONNECTIVITY

E_Port mode connectivity for heterogeneous environments involves directly connecting switches based on different platforms to form a fabric. E_Port connectivity in these situations is used most frequently when a SAN user already has switches based on different platforms and needs to form a single fabric without changing the fabric mode. The decision to interconnect either standalone switches or multi-switch fabrics might be driven by a lack of ports on one fabric or by an organizational change.

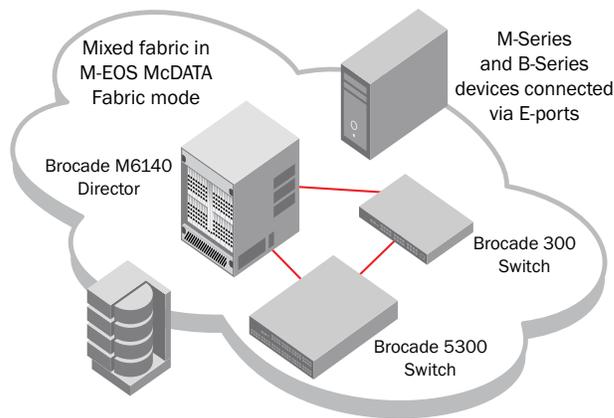


Figure 1.
Direct E_Port interoperability
for all Brocade platforms.

Brocade has supported classic E_Port interoperability with M-EOS switches and directors via the FC-MI Standard for several years. In addition, Brocade OEM Partners have tested and currently support many combinations of FOS and M-EOS hardware and firmware for direct E_Port connectivity. Both FOS and M-EOS have operational modes with different levels of direct E_Port compatibility and feature sets.

In conventional E_Port interoperability, both FOS and M-EOS fabrics must be set to “open” mode. While this enables fabric connectivity between different platforms, open mode also disables vendor value-added features in order to achieve basic connectivity. This has been problematic for customers who wish to integrate FOS and M-EOS fabrics but also want to retain vendor-specific functionality beyond open mode connectivity.

Brocade is now uniquely positioned to offer the most effective native connectivity solutions for platforms that have been historically difficult to make well work together.

BROCADE E_PORT NATIVE CONNECTIVITY

The Brocade 5000 was the first edge switch to support direct E_Port connectivity with a fabric in McDATA Fabric mode, which enables non-disruptive expansion of any fabric in this fabric mode. For SAN users familiar with M-EOS and EFCM management tools, the Brocade 5000 is a straightforward addition to an M-EOS, and it is backed by FOS and M-EOS engineering, test, and support expertise to help ensure reliable operation for SAN fabrics using any of the supported configurations.

Beginning with FOS 6.0.0, the Brocade 48000 Director and Brocade DCX Backbone offer core-level E_Port connectivity, which ensures native connectivity capability for maximum flexibility and optimal investment protection for users growing SAN fabrics. Customers now have the option of seamlessly expanding or integrating their existing M-EOS fabrics with FOS-based platforms using either core director E_Port connections directly from Brocade enterprise core platforms or any of Brocade’s latest edge switch products. In either case, the value-added functionality of M-EOS platforms is retained without having to disruptively convert M-EOS directors to conventional open mode operation.

See Appendix A for information about qualification and support matrices.

BROCADE FCR NATIVE INTEROPERABILITY

Brocade Fibre Channel Routing is a unique SAN technology that allows secure communication between hosts and storage in two or more separate, unmerged fabrics. Using FCR to communicate non-disruptively between two separate fabrics allows those fabrics to be managed independently. The Fibre Channel Routing management mechanism is the simple, well-understood, industry-standard fabric zoning. Using two or more FC routers provides redundancy and increases the total bandwidth between the routed fabrics.

Brocade Fibre Channel Routing is often employed as a means to divide very large fabrics into smaller, more manageable units called “edge fabrics.” Since connectivity between some devices in different fabrics may be required, routing enables customers to create this communication without building ever larger fabrics. The Brocade FCR solution allows devices to communicate when they are in independent edge fabrics, while preserving the platform-specific functionality of each edge fabric.

To implement Brocade FCR, two or more fabrics must be connected with a special router port, such as those available on the Brocade 7500 Extension Switch or FR4-18i Extension Blade or with Integrated Routing (IR) available on the Brocade DCX Backbone and Brocade 5300 and 5100 Switches. The router ports connecting to the edge fabrics are configured as special E_Ports called “EX_Ports.” These EX_Ports are lightweight versions of the full E_Port and have only the minimum functionality required to allow secure communication between fabrics.

Multiple EX_Ports appear to an edge fabric as a single FOS or M-EOS FC switch called a “front domain.” The domain ID for the front domain is automatically provided by the principal switch from the edge fabric and requires no user management. Another virtualized switch, called a “translate domain,” is automatically created by the router when nodes are imported into an edge fabric. Again, this is fully automated and requires no user intervention. Note that neither the front nor the translate domain can become the principal switch of an edge fabric, so they do not require any active management.

Brocade Fibre Channel Routing allows edge fabrics to remain independent and not merge into a single fabric with common FC services via these layers of switch virtualization. The more complex E_Port connectivity does not apply to routed fabrics, because an EX_Port appears to be a Brocade M-Series World Wide Name (WWN) identifier. Domain IDs can easily be duplicated in different edge fabrics, because the routers perform Fibre Channel Network Address Translation (FC-NAT) between edge fabrics to help make implementing FCR non-disruptive to the edge fabrics.

NOTE: Duplicate Domain IDs are not allowed in merged fabrics for the following reason. If there are two fabrics and each fabric has some Domain IDs in common, it is impossible to merge these fabrics without taking one or more switches offline. FCR resolves this situation with the use of FC-NAT, which allows nodes in the separate edge fabrics to communicate but does not actually join the fabrics.

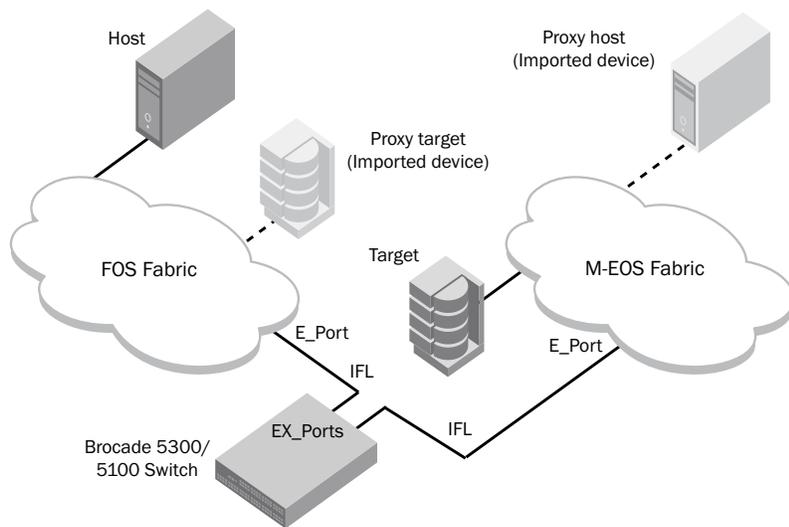


Figure 2.
Fibre Channel Routing interoperability
with FOS and M-EOS.

Enabling two nodes in different fabrics to communicate via a router is very simple:

- Create a zone with a name starting with “LSAN_” in each of the edge fabrics. Include the port WWNs for each of the two nodes as members of each zone and then enable the zone sets in each of the edge fabrics.
- The router sees these new LSAN_ zones, sets up the appropriate translations, and allows the communication between the selected devices.
- The fabrics remain separate so that no common problems (such as duplicate domain IDs or zone names) can spread between the routed edge fabrics.
- The router ignores all other zones in each edge fabric and does not allow communication between nodes in one edge fabric to the other edge fabric unless they are defined in LSAN_zones in each edge fabric.

Firmware levels, zoning, and some fabric parameters, such as E_D_TOV and R_A_TOV, can all be different in edge fabrics connected by Brocade FCR. In addition, edge fabrics can be in different fabric modes, including FOS native, McDATA Fabric, or McDATA Open Fabric modes. The Port ID (PID) addressing mode for FOS edge fabrics can be set to native PID (for much older switches), core PID (most common and currently shipping), and extended edge PID (much less common, for select UNIX hosts).

Most importantly, advanced features for each edge fabric based on different platforms continue to function. For example, a FOS edge fabric of two switches in native mode with the Brocade ISL Trunking feature could be connected via a router to an M-EOS edge fabric in native mode using port zoning (also known as “D,P zoning”) with no issues.

Fibre Channel Routing, using either Brocade’s new Integrated Routing or dedicated routing platforms, is an excellent solution for environments that need short- or long-term communications between fabrics based on different platforms. Currently, Brocade routers support simultaneous connections to FOS native, McDATA Fabric, and McDATA Open Fabric modes. With the addition of a Brocade router, any combination of fabrics with different fabric modes can operate with all features intact and have select devices (host and storage ports) communicate through the router. While this native connectivity solution requires the addition of a router, there is no disruption to the existing fabrics. Management of connectivity using a router relies on zoning, providing simple management of device connectivity.

Brocade routing technology is highly scalable, because only select devices communicate through the routing service and not all of the devices or any of the switches in the edge fabrics. See Appendix A for more information about Brocade Routing and support matrices.

N_Port ID Virtualization

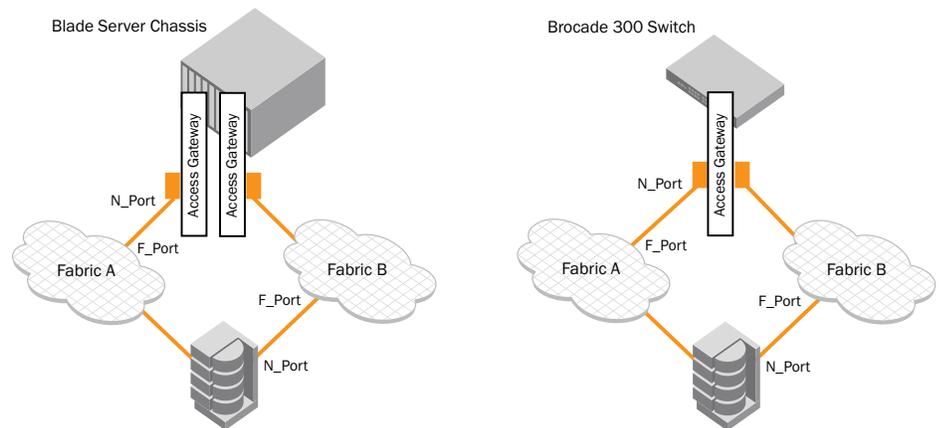
N_Port ID Virtualization (NPIV) is a Fibre Channel port virtualization technology that was first used to allow mainframe computers with multiple Linux OS instances to share a single physical port but still retain individual WWNs. NPIV allows the mapping of multiple virtual nodes to a single physical node/port. Without NPIV, zoning between a mainframe port with 10 Linux partitions and a storage port, for example, would allow all 10 Linux partitions access to the storage port. With NPIV, each Linux partition has its own WWN, which can be zoned to storage ports for granular zoning control.

BROCADE ACCESS GATEWAY FABRIC INTEROPERABILITY

Brocade Access Gateway leverages N_Port ID Virtualization (NPIV) technology to present servers as Fibre Channel Host Bus Adapter (HBA) connections directly into the fabric, thus mitigating switch-to-switch connectivity challenges that arise when mixing fabrics from different vendors. This approach significantly increases flexibility for connecting Brocade Fibre Channel SAN platforms to any SAN fabric. Access Gateway is a standard feature available to all 4 Gbit/sec Brocade blade server switches with Fabric OS 5.2.1 or later, the Brocade 200E Switch with Fabric OS 5.3.0 or later, and the 8 Gbit/sec Brocade 300 Switch with FOS 6.1.0 or later.

Blade server switches connect to a fabric switch. By applying NPIV to an embedded blade server switch, its external ports appear to the fabric switch that supports NPIV as N_Ports with server HBAs. These external ports and the internal ports that connect to the blade servers are still switched in the same way as a traditional Fibre Channel switch. But an embedded switch configured for Access Gateway mode does not appear as a Fibre Channel switch and does not use E_Ports to connect to the fabric—instead a switch in Access Gateway mode uses N_Ports for fabric connections.

Figure 3.
Brocade Access Gateway examples.



In non-bladed server environments, the Brocade 300 Switch can be used, as shown on the right in Figure 3. With Fabric OS 6.1.0 or later, the Brocade 300 can be configured to Access Gateway mode and operated in the same way as discussed for blade server switches in Access Gateway mode.

Because it connects to any NPIV-enabled edge device or director, Access Gateway removes the dependency on vendor-specific SAN fabrics, increasing deployment flexibility and simplifying the integration of heterogeneous storage networks. Access Gateway can provide a good solution if a SAN user is standardized on a vendor for directors and the vendor does not offer embedded blade switches or Fibre Channel SAN switches. In another situation, one vendor might be the standard for directors but another vendor is chosen for embedded blade switches or Fibre Channel SAN switches. A split decision is likely to happen more frequently with blade servers, because storage and server groups in an IT organization could be making independent purchases. Users needing to add a small switch and new servers to an existing fabric can use the Brocade 300 in Access Gateway mode and connect it to any fabric that supports the NPIV standard.

Because Access Gateway presents external N_Ports and not E_Ports to the fabric, the fabric switch simply sees a device node participating in the SAN instead of another switch in the fabric (a configuration that is more complicated). Using the Access Gateway mode instead of the traditional switch mode also moves the administrative boundary between the servers and fabric to outside the server rack. That is because to the SAN, rebooting a switch in Access Gateway mode is the same as rebooting a server HBA. Adding Access Gateways to a fabric adds more ports to the fabric but not additional switch domain IDs, which allows for much greater fabric scalability. Therefore, SAN users who have fabrics constrained by domain ID count can now add more switched ports to a fabric using Access Gateway.

In addition to these benefits, using a blade server platform or a switch in Access Gateway mode allows excellent overall fabric compatibility, because the switch now appears to the fabric as a server HBA, thus avoiding fabric connectivity problems. Making E_Ports based on different platforms interoperate directly is more challenging and requires more changes than just making a node port (host or storage) operate with a switch. In this situation, the Fibre Channel protocols (name server, zoning, RSCN, and so on) do not have to match, since an N_Port (host, server, or Access Gateway uplink port) does not use these fabric parameters.

Attaching storage and host nodes to a fabric is a very well-understood process and is much simpler than directly attaching switches. The fabric connectivity capabilities of Access Gateway are the same as the SAN device compatibility capabilities achieved by connecting HBAs to a switch. This means that a switch in Access Gateway mode should fully interoperate with any Fibre Channel switch that supports NPIV, and qualification testing has to focus only on SAN device compatibility issues, not the more challenging fabric connectivity issues. There are no fabric mode behaviors to configure and no routing to perform— Access Gateway simply connects to the external switch in the same way a host attaches to a switch.

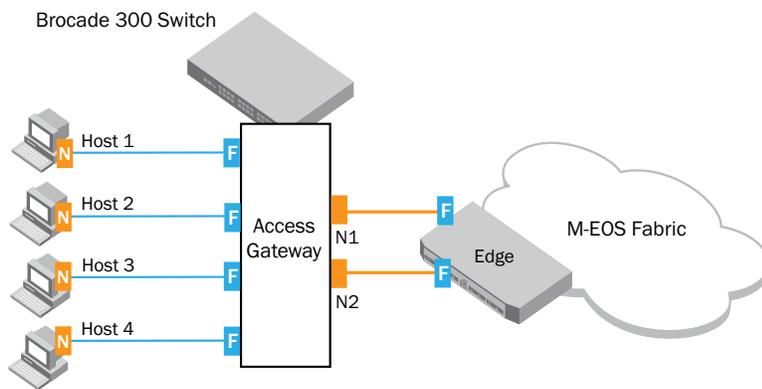


Figure 4. Access Gateway interoperability with M-EOS fabric.

Access Gateway mode is perfectly suited for any blade server with embedded Fibre Channel switches or servers connecting to a fabric through a small switch that needs to attach to fabric, whether the fabric comprises switches from the Access Gateway switch vendor or another vendor. A Brocade 300 in Access Gateway mode works with multi-vendor fabrics in heterogeneous data centers, enabling SAN administrators to connect heterogeneous fabric deployments for consolidation or easier management. Brocade plans to continue adding new features to Access Gateway to improve performance and resiliency with upcoming Fabric OS releases and new hardware platforms.

NOTE: Direct connectivity to SAN target devices is not applicable in Access Gateway mode.

SUMMARY

Brocade currently has three types of solutions to enable native connectivity: direct E_Port connect for both core and edge solutions, Fibre Channel Routing connectivity, and Access Gateway connectivity. Each of these solutions has a number of use cases and each has its own unique strengths. Brocade is further developing these native connectivity techniques and anticipates broadening its support for a wide range of configurations. Brocade also plans to offer additional connectivity options via new software and hardware releases over time.

For more information, visit www.brocade.com.

APPENDIX A. REFERENCES

These following resources are available from Brocade and other SAN vendor Web sites:

- [Brocade.com > Products > Technology & Architecture > Interoperability](#)
- [EMC.com > Products > EMC Interoperability Support Matrices > EMC Support Matrix](#)
- [Powerlink.emc.com > Support > Documentation > Topology Guides](#)
EMC Networked Storage Topology Guide
- [HP.com > Support&Troubleshooting > Storage > Storage Networking > HP StorageWorks SAN Solutions > Manuals](#)
Merging Fabrics Based on M-Series and B-Series Fibre Channel Switches
Merging Fabrics Based on C-Series and B-Series Fibre Channel Switches
- [Cisco.com > Support > Documentation > Storage Networking > Cisco MDS 9000 SAN-OS Software > Compatibility Information](#)
Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide

Corporate Headquarters

San Jose, CA USA
T: (408) 333-8000
info@brocade.com

European Headquarters

Geneva, Switzerland
T: +41 22 799 56 40
emea-info@brocade.com

Asia Pacific Headquarters

Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2008 Brocade Communications Systems, Inc. All Rights Reserved. 06/08 GA-WP-883-04

Brocade, Fabric OS, File Lifecycle Manager, MyView, and StorageX are registered trademarks and the Brocade B-wing symbol, DCX, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.



BROCADE