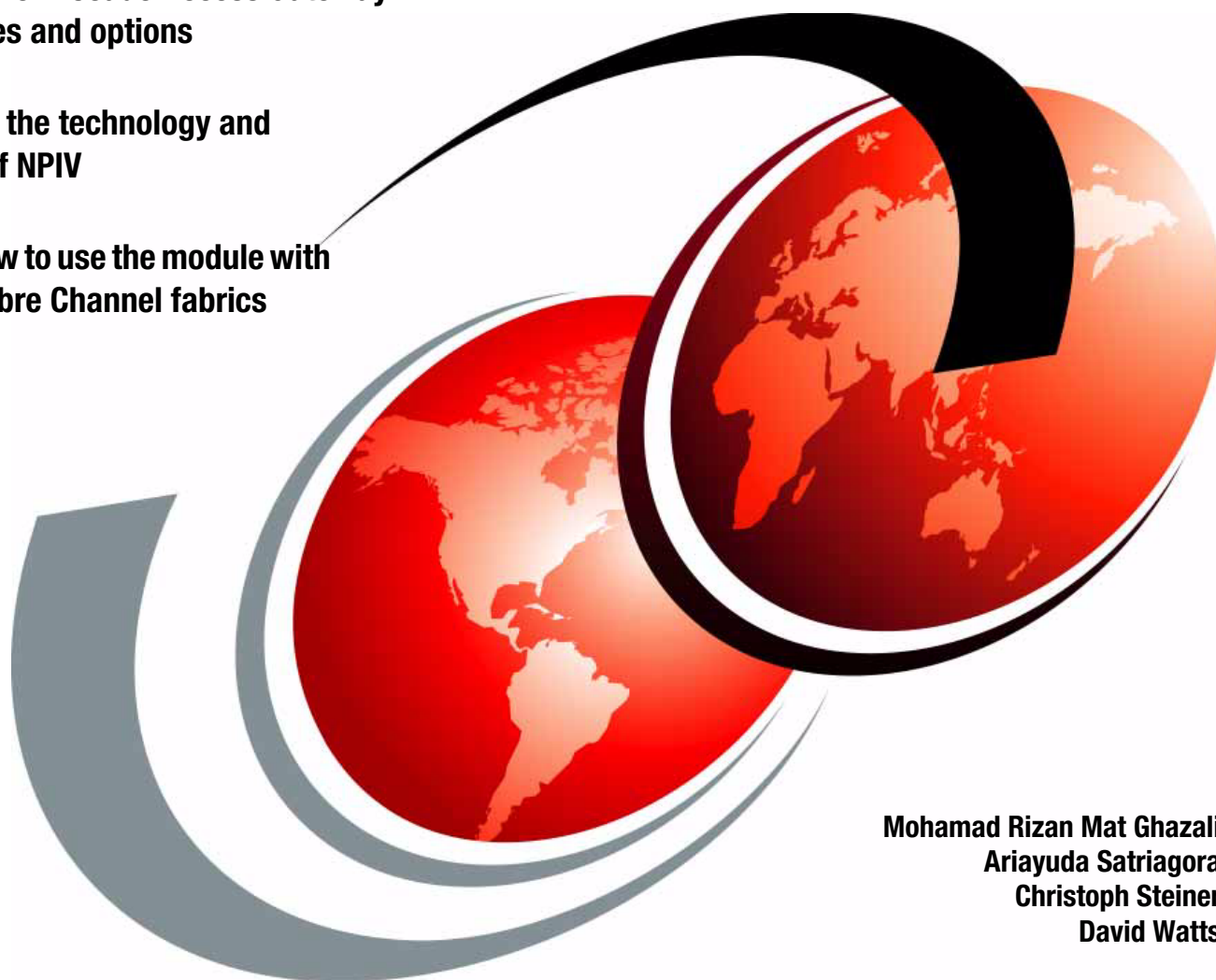


Implementing the Brocade Access Gateway for IBM BladeCenter

Explains the Brocade Access Gateway capabilities and options

Describes the technology and benefits of NPIV

Shows how to use the module with various Fibre Channel fabrics



Mohamad Rizan Mat Ghazali
Ariayuda Satriagora
Christoph Steiner
David Watts



International Technical Support Organization

**Implementing the Brocade Access Gateway for IBM
BladeCenter**

December 2007

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (December 2007)

This edition applies to the Brocade Access Gateway feature of Fabric OS v5.2.1b on the Brocade 4 Gb SAN Switch Module.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team that wrote this paper	vii
Become a published author	viii
Comments welcome	ix
Chapter 1. Introduction and Technology	1
1.1 Introducing the Brocade Access Gateway	2
1.1.1 Basic concept	2
1.1.2 Port mapping	4
1.1.3 About Dynamic Ports on Demand	6
1.2 N_Port ID Virtualization (NPIV)	6
1.3 Benefits of using the Brocade Access Gateway	7
1.3.1 Interoperability	7
1.3.2 Scalability	9
1.3.3 Administrative simplification	10
1.3.4 Cost reduction	10
1.4 Typical use cases of Brocade Access Gateway	11
1.4.1 Environment with many different fabric vendors	11
1.4.2 Environment where the fabric size is becoming a burden	11
1.4.3 Environment with compartmentalized administration	12
1.5 Limitations	12
Chapter 2. Planning	13
2.1 Compatibility	14
2.2 Prerequisites	16
2.3 Additional considerations and sample scenarios	18
2.3.1 Switch connection	18
2.3.2 Optical Pass-thru Module connection	19
2.3.3 Using an Access Gateway	20
2.4 Limitations	21
2.4.1 Failover and failback policies	22
2.5 Configuring additional F_Ports	24
Chapter 3. Implementation	29
3.1 NPIV support	30
3.1.1 Cisco MDS	30
3.1.2 Brocade B-Type	32
3.1.3 Brocade M-Type (formerly McDATA)	33
3.2 Enabling NPIV	35
3.2.1 Cisco MDS	35
3.2.2 Brocade	36
3.2.3 McDATA	38
3.3 Blade Server setup	40
3.3.1 Install the HBA	40
3.3.2 Manage the HBA	40

3.4 Setup of the Brocade Access Gateway in the AMM	41
3.4.1 Setting the switch module IP address and enabling external ports.	42
3.5 Firmware update to the latest version.	45
3.6 Converting to Access Gateway mode	48
3.6.1 Command line interface	49
3.6.2 Brocade Web Tools	50
3.7 Connecting to the fabric	54
3.7.1 Cisco MDS	55
3.7.2 Brocade.	56
3.7.3 McDATA	59
3.7.4 Storage attachment.	60
3.8 Command reference	66
3.8.1 Switch commands.	66
3.8.2 Access Gateway commands.	68
3.8.3 Commands on the external Switch	70
Abbreviations and acronyms	71
Related publications	73
IBM Redbooks	73
Online resources	73
Help from IBM	73

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.


This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®

BladeCenter®

Enterprise Storage Server®

FICON®

IBM®

Redbooks®

ServerProven®

System x™

System Storage™

TotalStorage®

The following terms are trademarks of other companies:

SANbox, QLogic, and the QLogic logo are registered trademarks of QLogic Corporation. SANblade is a registered trademark in the United States.

Fabric OS, Brocade, SilkWorm, and the Brocade logo are trademarks or registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries.

Microsoft, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Many SAN configurations continue to grow in size and complexity. As the number of switches in the fabrics increase, the fabric management complexity also increases. SAN usage continues to grow as companies continue to require more computing resources. One of the recent technologies which addresses this issue is N_Port ID Virtualization (NPIV) and the Access Gateway feature of the Brocade SAN Switch Module which implements this technology in IBM® BladeCenter®.

N_Port ID Virtualization (NPIV) is an extension to a standard already defined in Fibre Channel protocol that allows a host bus adapter on a server to use multiple Fibre Channel addresses. This enables zoning and LUN masking, giving each server and virtual machine unique access to required storage resources. In addition, exclusive assignment of storage and connectivity resources to priority virtual machines, through their virtual ports provides more granularity to fulfill service level agreements. Finally, the ability to tear down a virtual port and reinitialize it on different blade servers greatly enhances virtual machine portability for load balancing and incident recovery. In short, NPIV enhances SAN connectivity, flexibility in resource allocation, and recovery.

This paper introduces the Access Gateway feature of the Brocade SAN Switch Module and describes the technology and features of this module and the connectivity options. We go through use cases on each implementation, and identify and contrast the benefits of each implementation.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Mohamad Rizan Mat Ghazali is an Advisory IT Specialist for System x™ and BladeCenter within IBM Global Services in Malaysia. He has four years of IT service delivery experience in IBM System x, BladeCenter, SAN, and Storage environments. In his current role, he provides advice, direction, and resolution for customer problems.

Ariayuda Satriagora is a System Support Representative in Indonesia. He has three years of experience with IBM System x and BladeCenter servers. He holds a Bachelor of Engineering degree from Gadjah Mada University (Indonesia). His areas of expertise include IBM BladeCenter servers and the associated systems.

Christoph Steiner is a Support Specialist for System x and BladeCenter within IBM Global Services in Austria. He has nine years of IT service delivery experience in System x, BladeCenter, SAN, and Storage environments. In his current role, he provides direction and resolution to critical situations in customer environments.

David Watts is a Consulting IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces IBM Redbooks® publications on hardware and software topics related to IBM System x, BladeCenter servers, and associated client platforms. He has authored over 80 books, papers, and technotes. He holds a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM both in the US and Australia since 1989. He is an IBM Certified IT Specialist.



The team (l-r): Aria, David, Chris, and Mohamad

Thanks to the following people for their contributions to this project:

From the International Technical Support Organization:

- ▶ Carolyn Briscoe
- ▶ Linda Robinson
- ▶ Margaret Ticknor
- ▶ Erica Wazewski

From IBM Corporation

- ▶ Khalid Ansari
- ▶ Mary Beth Daughtry
- ▶ Robyn McGlotten
- ▶ Ishan Sehgal

From Brocade

- ▶ Dexter Monk
- ▶ Tim Werts
- ▶ Brian Steffler
- ▶ Matt Wineberg

From Cisco

- ▶ Matt Slavin

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You

will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400



Introduction and Technology

SAN solutions continue to grow in size and complexity. As the number of switches in the fabrics increase, the fabric management complexity increases correspondingly. SAN solution demand continues to grow as companies continue to demand more computing resources. One of the recent technologies applied in blade technology which address this issue is Brocade Access Gateway.

In this chapter, we discuss the following topics:

- ▶ 1.1, “Introducing the Brocade Access Gateway” on page 2
- ▶ 1.2, “N_Port ID Virtualization (NPIV)” on page 6
- ▶ 1.3, “Benefits of using the Brocade Access Gateway” on page 7
- ▶ 1.4, “Typical use cases of Brocade Access Gateway” on page 11
- ▶ 1.5, “Limitations” on page 12

1.1 Introducing the Brocade Access Gateway

This section discusses the basic concept of Brocade Access Gateway and the related technologies.

1.1.1 Basic concept

Brocade Access Gateway is a new feature of Fabric OS which enables a Brocade 4 Gb SAN Switch Module to be configured in Access Gateway mode. Once a Brocade SAN Switch Module has been configured in Access Gateway mode, it no longer participates in the SAN fabric as a Fibre Channel (FC) switch and is without FC services such as zoning, name server, and FC addressing.

Note: In this paper, we refer to the Brocade 4 Gb SAN Switch Module configured in Access Gateway mode simply as the Brocade Access Gateway.

The Brocade Access Gateway feature is a software-only extension of Fabric OS that addresses specific interoperability, scalability, and manageability concerns that might occur in certain Fibre Channel SAN fabrics. For most BladeCenter implementations, the Brocade SAN Switch Module should continue to be used in FC switch mode, providing the full suite of FC services available.

The primary benefits of the Access Gateway feature occur when connecting BladeCenter to heterogeneous SAN fabrics (e.g. Cisco and McDATA), providing separation between server and SAN administrative groups, and increasing scalability to ultra-large SAN fabrics.

Table 1-1 compares the Optical Pass-thru Module, the Brocade SAN Switch Module in Switch mode, and the SAN Switch Module in Access Gateway mode.

Table 1-1 Comparison between the OPM, the SAN Switch Module, and the Access Gateway

	IBM Optical Pass-thru Module	SAN Switch Module in switch mode	SAN Switch Module in Access Gateway mode
Interoperability	No issues	There might be E_Port interoperability issues	No Issues. Connects as NPIV-enabled HBA.
Domain proliferation	Domains increase as more external switches are added	Domains increase as BladeCenter chassis are added	No increase in domains
TCO (cables, edge switches, SFPs)	Relatively high	Relatively low	Relatively low
Connectivity flexibility	Connects to storage or switches	Connects to storage or switches	Connects to switches
Administrative effort	No setup. Zoning performed in SAN fabric.	Initial Setup. Port or WWN zoning performed on module or in SAN fabric.	No setup. Zoning performed in SAN fabric.

There are three Fibre Channel port terms used in this paper:

- ▶ **N_Port**, node port. A host, HBA, or storage device port connected to the F_Port of the switch.

- ▶ **F_Port**, fabric port. A switch port that connect a host, HBA, or storage device to the SAN.
- ▶ **E_Port**, known as Inter Switch Link (ISL). A switch port that connect the switch to another switch directly.

Figure 1-1 illustrates an example of the port types previously mentioned.

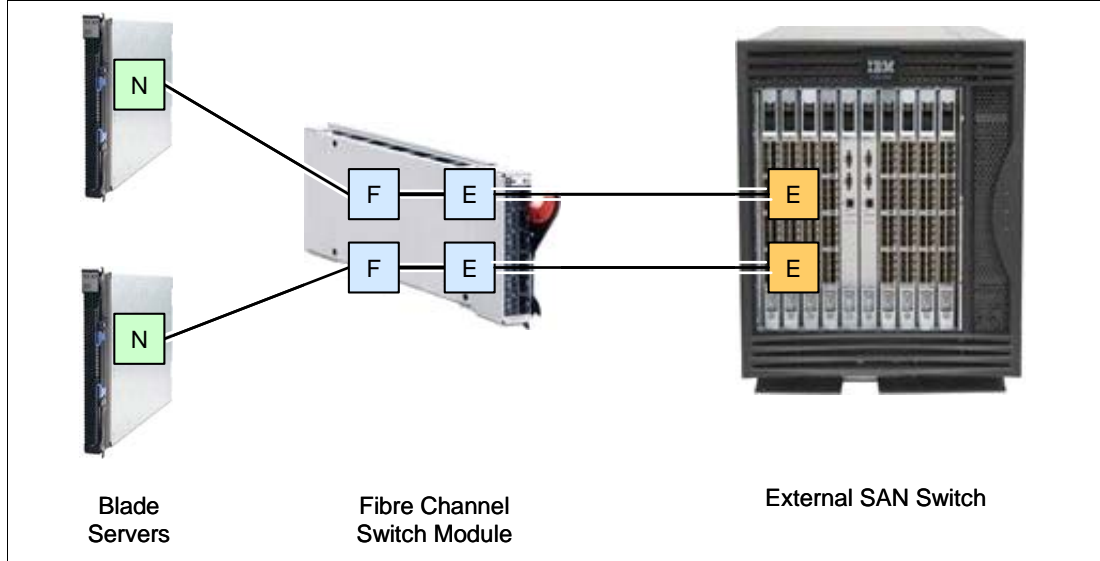


Figure 1-1 An example of three Fibre Channel port types in original switch mode

The Access Gateway multiplexes host connections to the fabrics. It presents an F_Port to the host and an N_Port to fabrics. Using N_Port ID Virtualization (NPIV) technology, the Access Gateway allows multiple FC initiators to access the same physical port. External ports on the Access Gateway appear to the fabrics as N_Port connections and no domain is added to the fabrics. More details about NPIV technology are discussed in 1.2, “N_Port ID Virtualization (NPIV)” on page 6.

Host to fabric connection through the Access Gateway, port types used, and how it is compared to connection through SAN Switch Module in switch mode are illustrated in Figure 1-2 on page 4.

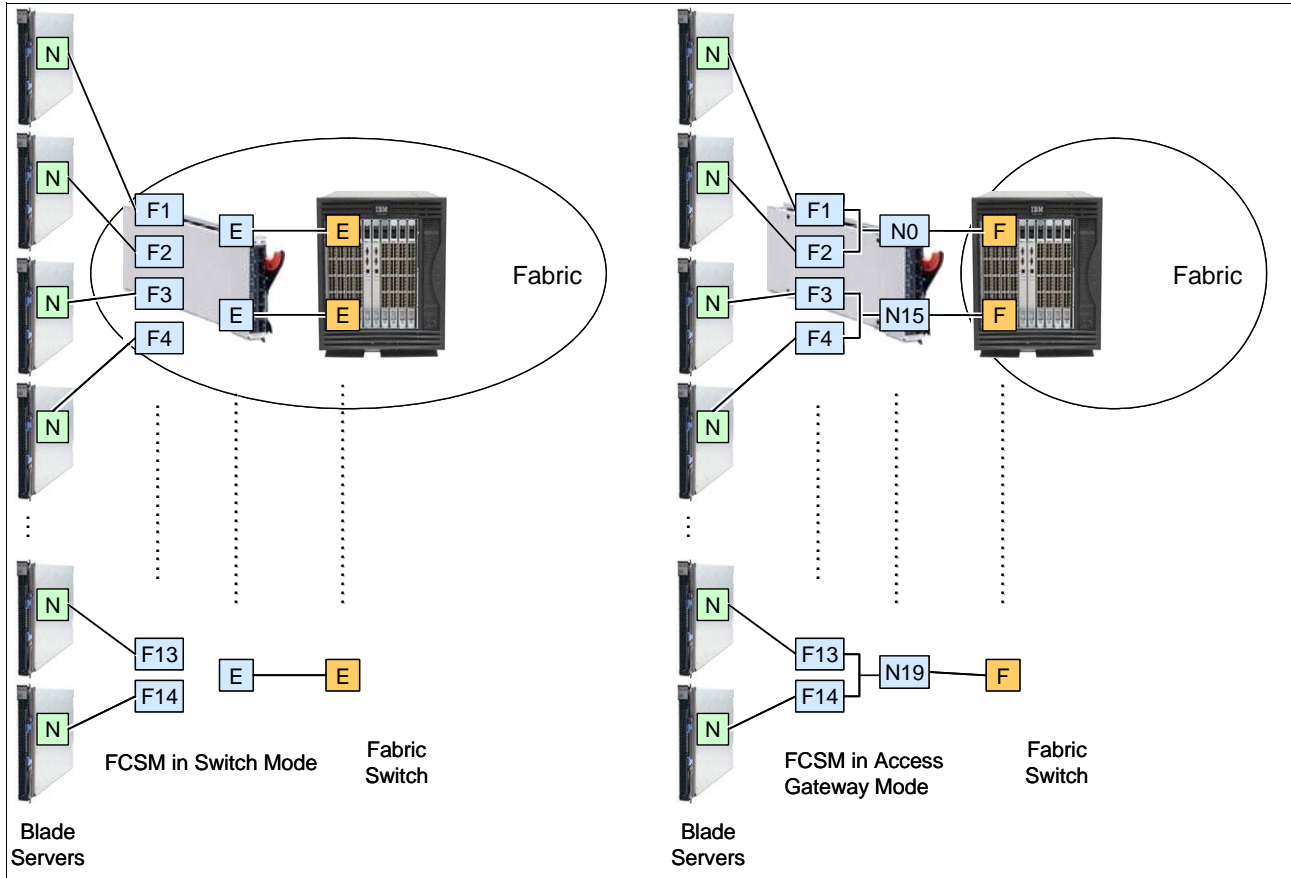


Figure 1-2 Comparison of the Access Gateway connection and switch connection

1.1.2 Port mapping

To manage traffic between hosts and the fabric, the Access Gateway uses mapping. This means that F_Ports must be mapped to N_Ports so that servers have a path to an external SAN fabric. This F_Port to N_Port mapping builds static routes between specific F_Ports and specific N_Ports.

There is a default port mapping that predefines the routes between the F_Ports and the N_Ports. By default, all external ports of the Access Gateway (Port 0, 15-19) are configured as N_Ports and all internal ports are configured as F_Ports and mapped to the N_Ports. The external port setting and default mapping can be changed if required.

Figure 1-3 on page 5 illustrates a port mapping example of an Access Gateway connecting blade servers to the external fabric.

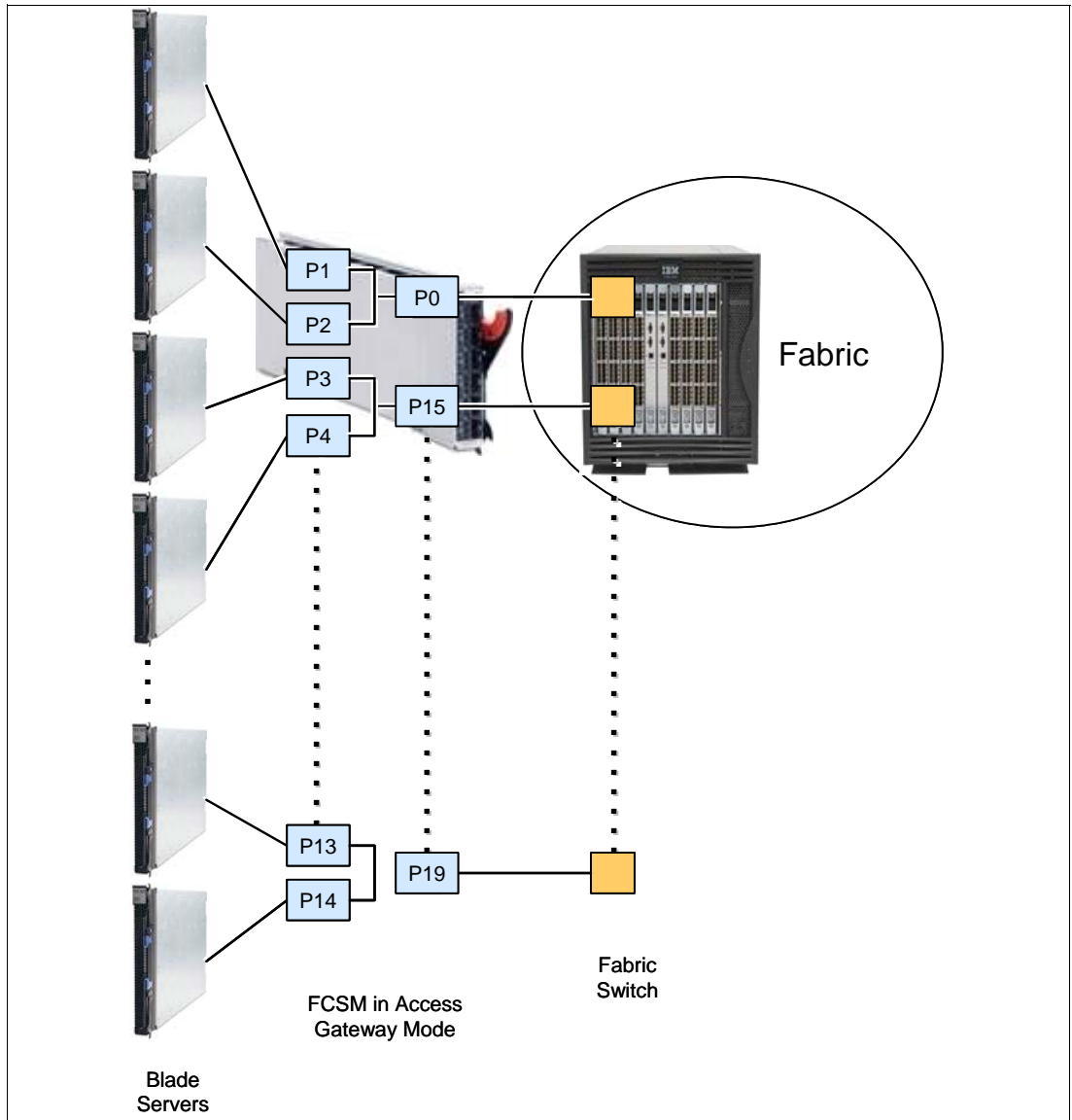


Figure 1-3 An example of port mapping

The mapping example shown in Figure 1-3 is summarized in Table 1-2.

Table 1-2 An example of port mapping

F_Ports	N_Ports
P1	P0
P2	P0
P3	P15
P4	P15
P13	P19
P14	P19

The complete port mapping table is in Table 2-8 on page 23.

An existing Brocade SAN Switch Module can be converted to Access Gateway mode through the Fabric OS command line interface (CLI) or Web Tools. SAN administrators can perform a firmware upgrade and run a simple CLI command or use the Brocade Web Tools to enable Access Gateway mode. If WWN zoning is applied, moving to Access Gateway mode requires no zoning changes in the existing fabrics. Rezoning is only necessary if port-level zoning is implemented.

Once operating as an Access Gateway device, a Brocade SAN Switch Module can easily be reverted to the original switch mode if required.

1.1.3 About Dynamic Ports on Demand

Dynamic Ports on Demand (DPOD) is a feature that is supported on all 10-port Brocade Fibre Channel switch modules for “pay-as-you-grow” scalability. DPOD automatically enables ports on the SAN Switch Module when the server is powered on and does not require a predefined assignment of ports. Available ports are determined by the total number of ports in use and the number of purchased dynamic ports. DPOD automatically detects HBA connected server ports or cabled ports, and assigns a POD license to each of these ports. In other words, when the DPOD mechanism detects a server blade in an online state, it automatically assigns a POD license to the blade.

Access Gateway functionality is compatible with DPOD. The ports that are licensed through DPOD will also participate in Access Gateway mode.

1.2 N_Port ID Virtualization (NPIV)

N_Port ID Virtualization (NPIV) is a Fibre Channel protocol that facilitates sharing a single physical N_Port among multiple N_Port IDs. Virtualization refers to the ability of a single physical N_Port allowing multiple distinguishable entities on the same physical ports. It makes a single FC port appear as multiple virtual ports, each having its own N-Port ID and virtual WWN. The NPIV protocol requires an N_Port (typically an HBA or any device that acts as an NPIV gateway) and a fabric (generally an FC switch) so that the N_Port can request and acquire multiple addresses from the fabric.

NPIV implementation requires two participating ports:

- ▶ An N_Port, which communicates with an FC fabric for requesting port addresses and subsequently registering with the fabric
- ▶ An F_Port, which assigns the addresses and provides fabric services

NPIV was developed initially to provide a more scalable access to Fibre Channel storage from Virtual Machine (VM) instances and to let administrators assign each Linux® OS partition on a Mainframe to its own virtual WWN. With NPIV, the WWNs can represent either hardware or VMs.

The combination of the ability of an N_Port device, such as an HBA, to have multiple N_Port IDs and the ability of fabric switches to accept NPIV capable devices is the basic concept of transparent switching.

Figure 1-4 on page 7 illustrates how a single HBA shares its single physical N_Port to a VM's virtual N_Ports.

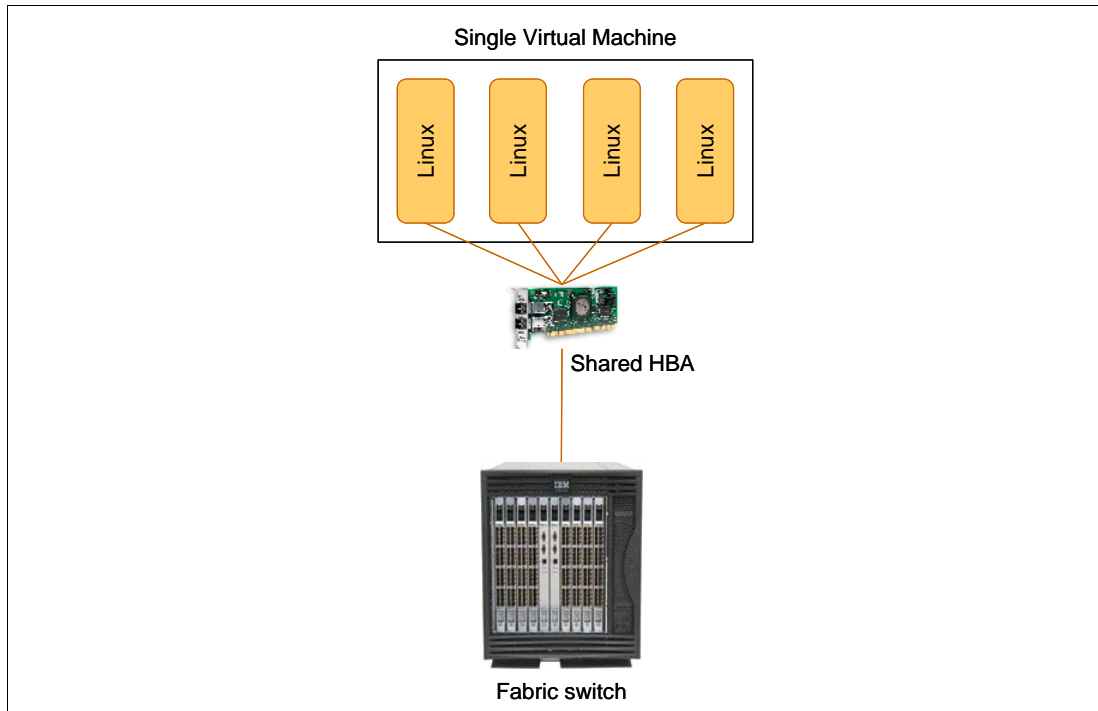


Figure 1-4 Illustration of NPIV

The benefits of NPIV and the Brocade Access Gateway module is that the NPIV prerequisites are handled by the module. This means:

- ▶ You do not need to change any settings on the HBA when switching to or from Access Gateway mode.
- ▶ An NPIV-capable HBA is not required in Access Gateway mode.
- ▶ The operating system on the blades is not required to recognize or take advantage of NPIV technology. The NPIV connection is fully handled by the Access Gateway.

The only requirement is that the edge switches must support NPIV connections.

The benefit of having an NPIV-aware operating system such as VMware ESX Server is that it can set up separate virtual host partitions running independent guests (Windows® and Linux, for example), and that each could use a separate NPIV login to the fabric identified by a separate WWN even though they are carried over the same physical HBA port. Since zoning is based on WWN, the separate virtual hosts will have controlled access to the allocated storage.

1.3 Benefits of using the Brocade Access Gateway

Using the Brocade Access Gateway has benefits as described in the following sections.

1.3.1 Interoperability

Using the Access Gateway eliminates interoperability as one of the most challenging issues of blade server SAN deployment. This interoperability issue includes fabric management and reduced feature set in connection to third-party vendor fabric.

As previously mentioned, all Fibre Channel switches support login to F_Ports whether in the open or proprietary interconnect mode. Because the Access Gateway transparently presents the hosts as N_Port devices to the fabric, management of the fabric is unaffected.

The following figures show connections between blade servers and the fabric through an Access Gateway and show how they are represented in the fabric. Figure 1-5 shows the connection topology. Figure 1-6 shows the name server of the fabric switch.

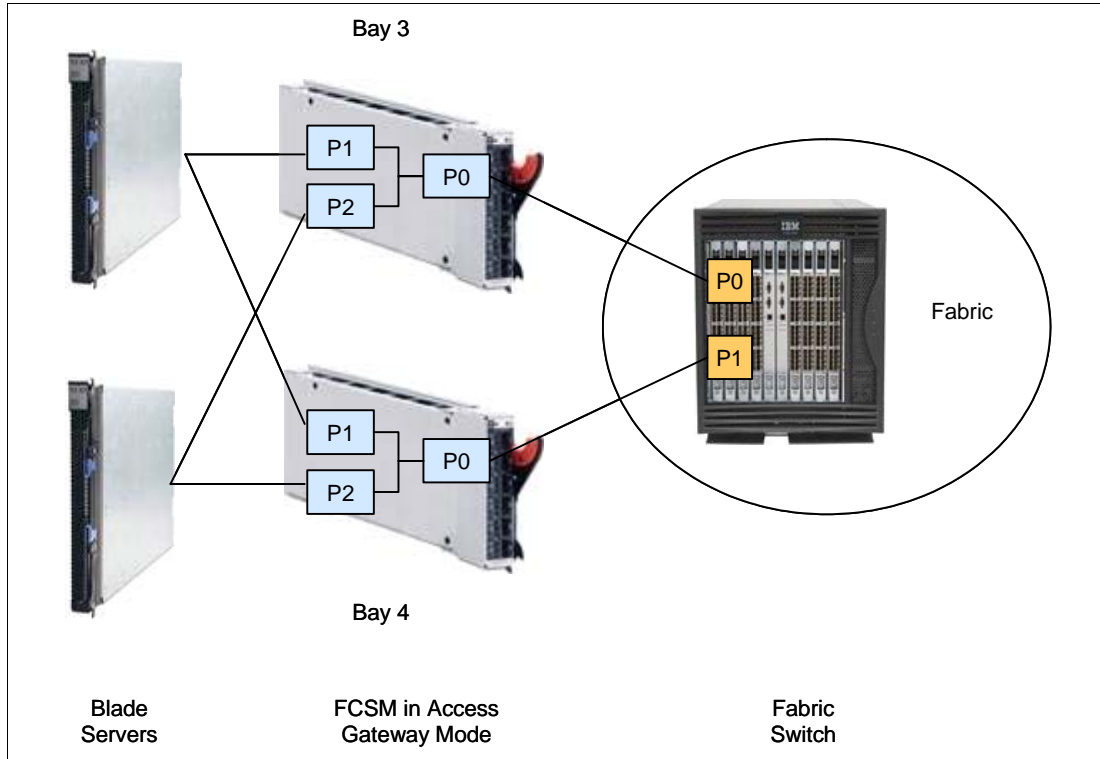


Figure 1-5 Blade server to fabric connection through the Brocade Access Gateway

The screenshot shows the Cisco MDS Name Server table for mds9216_BC3. The table has columns for VSAN Id, Type, PortName, NodeName, Fc..., and FabricPortName. There are 6 rows of data. The table is displayed in a window titled 'mds9216_BC3 - Name Server' with tabs for General, Advanced, Proxy, and Statistics. The 'General' tab is selected. The table shows the following data:

VSAN Id, ...	Type	PortName	NodeName	Fc...	FabricPortName
100, 0x610001	N	Brocade 20:00:00:05:1e:02:80:81	Brocade 10:00:00:05:1e:02:80:81		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610002	N	Brocade 20:00:00:05:1e:02:17:37	Brocade 10:00:00:05:1e:02:17:37		Cisco 20:01:00:0d:ec:01:ac:c0
100, 0x610500	N	IBM 21:00:00:11:25:93:af:4b	IBM 20:00:00:11:25:93:af:4b		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610600	N	Qlogic 21:01:00:e0:8b:bd:a8:d7	Qlogic 20:01:00:e0:8b:bd:a8:d7		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610700	N	IBM 21:00:00:11:25:93:af:4a	IBM 20:00:00:11:25:93:af:4a		Cisco 20:01:00:0d:ec:01:ac:c0
100, 0x610800	N	Qlogic 21:00:00:e0:8b:9d:a8:d7	Qlogic 20:00:00:e0:8b:9d:a8:d7		Cisco 20:01:00:0d:ec:01:ac:c0

6 row(s)

Figure 1-6 Cisco MDS Name Server table

In a multi-vendor (heterogeneous) SAN fabric using E_Ports between the switch module and the external fabric, vendor unique features are often disabled. This reduction of features does not occur when using Access Gateway mode because the connection is established as an N_Port and not an E_Port.

1.3.2 Scalability

By eliminating the switch domain, the Access Gateway directly addresses an important SAN scalability constraint: the number of domains in a fabric. Typically the SAN supplier will define the maximum SAN fabric size by using two parameters:

- ▶ The maximum number of domains supported
- ▶ The maximum number of devices connected

The limit occurs once either of these maximums is met. Check with your SAN fabric supplier to determine the SAN fabric tested and supported limits.

For customers with large existing SAN fabrics (for example, 30 domains) or those planning to add a large number of BladeCenter chassis to a small-to-medium SAN fabric, adding a Fibre Channel switch module with every BladeCenter chassis significantly increases the total number of domains and limits overall scalability of a SAN fabric. This becomes an undesirable situation, especially for enterprises with a large BladeCenter infrastructure.

Because the Access Gateway devices no longer participate as an FC switch in the fabric, they no longer require domains and have less of an impact on the overall SAN scalability. For example, consider an enterprise is connecting 32 BladeCenter chassis to 4 switches in the fabric. In switch mode, at least 36 domain IDs are needed in that fabric, but with Access Gateway mode, only four domain IDs are needed. Figure 1-7 illustrates this example.

Note: Adding NPIV based switch modules such as the Access Gateway might still impact SAN scalability since potentially more FC devices could be added to the fabric. Therefore, check with your SAN Supplier to determine the maximum number of Access Gateways and total number of devices supported in a SAN fabric.

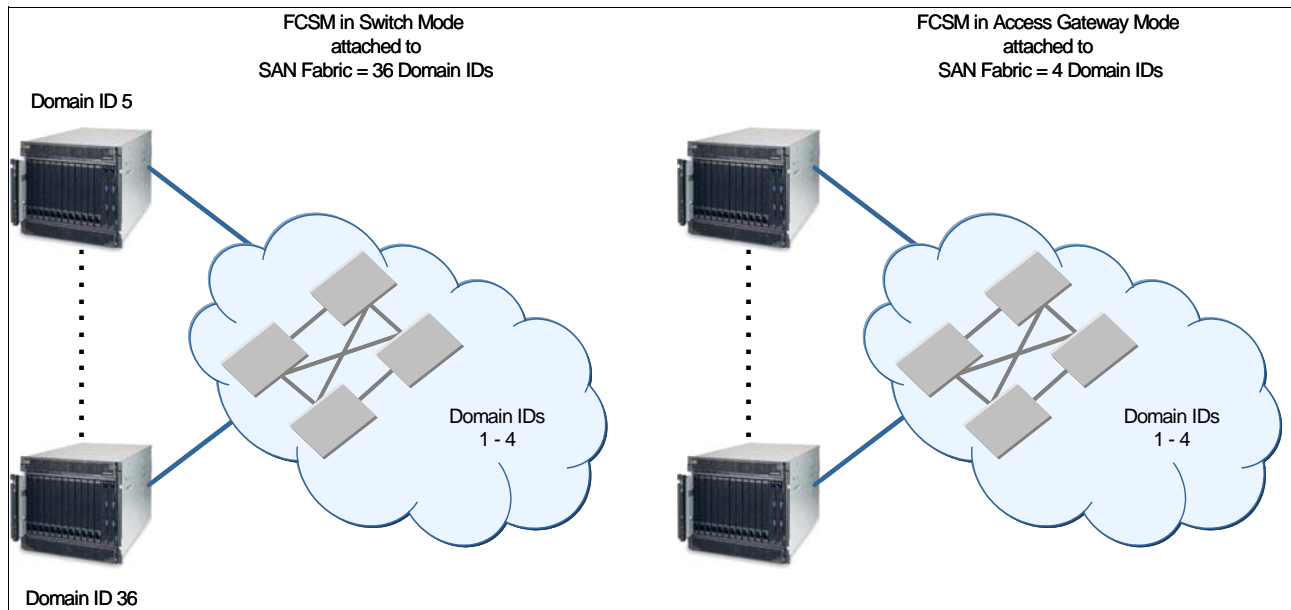


Figure 1-7 Brocade Access Gateway implementation reduces the number of domain IDs in a fabric

1.3.3 Administrative simplification

For customers with existing SAN fabrics and no BladeCenter chassis, adding a large number of BladeCenter chassis with FC switch modules greatly increases the complexity of the overall SAN fabric and might cause conflicts between the SAN administration group and the server administration group. On occasion, the SAN administration group might be reluctant to implement the blade server project for the following reasons:

- ▶ Increased SAN management effort: The SAN administration group must now manage a more complex fabric with all the additional SAN Switch Modules added.
- ▶ Increased SAN security concern: The SAN administration group may be concerned that the SAN Switch Module is embedded in a server product and therefore might be disabled or have configuration or zoning changed by the server administrators. These types of changes could affect the entire SAN.

By using Access Gateway mode both these concerns can be addressed:

- ▶ Simplified SAN fabric topology: Since the Access Gateway does not require a domain number, the SAN fabric is simplified.

However, NPIV-based switches such as the Access Gateway are intelligent FC devices and therefore some administration is required to monitor and manage the modules to ensure there are no errors and, when needed, to download firmware or change parameters. Typically this will be the SAN administration group.

- ▶ Improved Management Security: In Access Gateway mode, the module no longer has fabric-wide services that could affect the entire SAN, such as zoning. Therefore, there are fewer risks to the SAN. The worst case is that the Access Gateway is disabled which would prevent the server blades from accessing storage on the SAN. However, other devices in the SAN are not impacted.

Figure 1-8 illustrates the comparison of administration perspective in a typical blade environment.

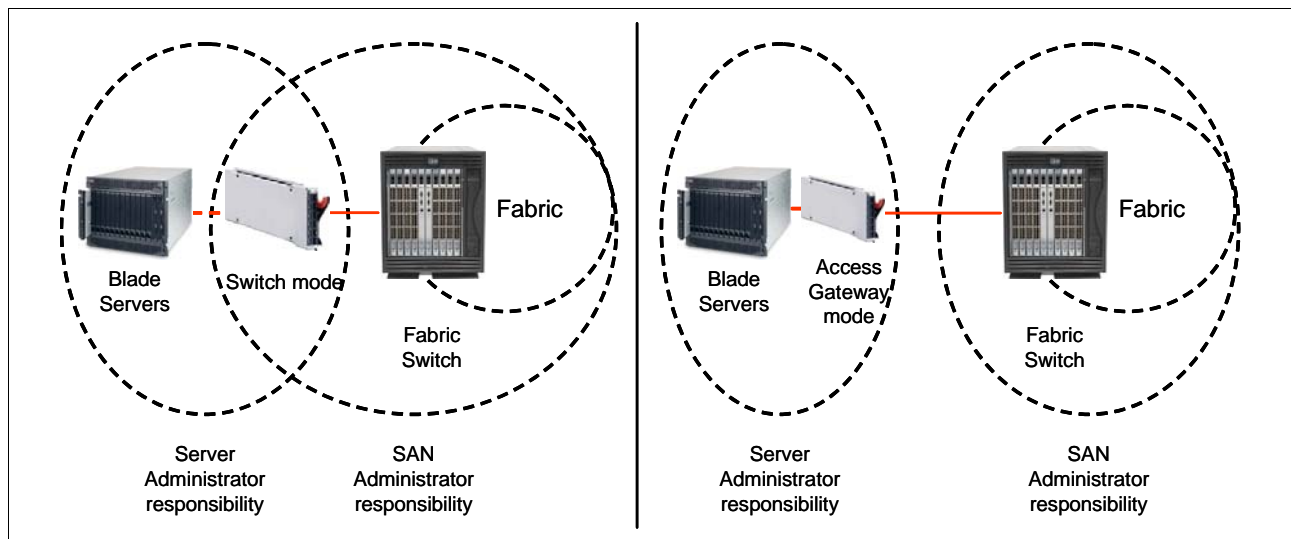


Figure 1-8 Comparison of administration perspective in a typical blade environment

1.3.4 Cost reduction

The existing pass-through solution, the Optical Pass Through Module (OPM), uses dedicated cabling to connect each blade server to a port on an external switch. It makes pass-through

solutions expensive to maintain. Each blade server requires dedicated connectivity hardware and dedicated ports on the external switch. Using an Access Gateway reduces the number of SAN ports required.

Converting an existing SAN Switch Module to Access Gateway mode is also financially acceptable since it requires no device change and no additional license.

1.4 Typical use cases of Brocade Access Gateway

Based on the benefits previously mentioned, there are some typical cases described in the following sections where Brocade Access Gateway can be recommended as a solution.

1.4.1 Environment with many different fabric vendors

This case happens typically in enterprises with large scale and a wide variety of SAN devices or in growing companies that implement devices provided by many different vendors to save costs.

For example, a small company was set up with a very limited SAN environment using low-budgeted and limited feature switches from a vendor. As it grew, its SAN environment added more advanced switches from many other vendors. Then they started experiencing interoperability problems.

By making the switches transparent to the fabric, the Access Gateway significantly reduced interoperability issues by maintaining a huge SAN environment with a multi-vendor fabric. It included a reduced feature set and more complex multi-vendor fabric administration.

1.4.2 Environment where the fabric size is becoming a burden

This situation happens typically in enterprises with large SAN fabrics. While the SAN specification allows for a maximum of 239 domains in a single fabric, realistically, the tested and supported domain count is much smaller, ranging from 20-60 domains and 1000-2500 devices. Today, many enterprises have SAN environments with more than 30 domains and therefore are consider *large*.

Adding numerous BladeCenter chassis to these environments can be a problem due to these domain and device limitations. Therefore, a solution for this issue is the Access Gateway feature that does not impact the domain count (but, as stated previously, does impact the device count) and will allow for greater scalability.

Always check with your SAN provider for their supported SAN fabric size before making any recommendations. The maximum size supported may be different between vendors and include many factors such as number of domains, number of devices, version of firmware, model, and speed of switches. Here are general guidelines for fabric size where the use of an Access Gateway may counter scalability concerns:

- ▶ Brocade-based SAN fabrics of 50 domains or more (Fabric OS v5.x or above)
- ▶ McDATA-based SAN fabrics of 30 domains or more (EOS v9.x or above)

1.4.3 Environment with compartmentalized administration

This case typically happens in enterprises with complex SAN topology that usually hire different administrators to manage the various jobs in their IT system.

For example, an enterprise hires people as server administrators, others as network administrators and the others as SAN administrators. In the case of servers in a BladeCenter chassis with an integrated SAN switch, there can be confusion or conflict regarding which administrative group will manage the SAN switch module.

As a result, the SAN switch is sometimes managed by both the SAN administrator and the server administrator (since it is considered a part of BladeCenter). Additionally, when the SAN administrator group does own management responsibility of the switch modules there can still be concerns since the server administrator group has some access to the module through the Management Module interface.

Often these concerns are alleviated by converting the switch modules to the transparent Access Gateway mode that does not allow any SAN fabric services and reduces the risk to the overall SAN fabric.

1.5 Limitations

There are some limitations of implementing Access Gateway devices:

- ▶ Direct connection to SAN targets

In Access Gateway mode, direct connection to SAN targets, such as tape or disk enclosure, is not supported.

- ▶ Number of devices in connection

Check the Release Notes for the specific Fabric OS version or the Support Matrix from your SAN vendor to determine the latest scalability numbers for using Access Gateway.

- ▶ Cascading devices

Cascading between Access Gateway devices is currently not supported.

- ▶ Switch features

When using a Brocade SAN Switch in Access Gateway mode, some switch features are no longer applicable. These features include Admin Domain, Advanced Performance Monitoring, FICON®, IP over FC, Extended Fabrics, Management Services, Name Services (SNS), port mirroring, and SMI-S. These features are available in the default switch mode operation.



Planning

This chapter provides information about the planning and installation of the Brocade Access Gateway. Although the hardware is equal to the existing Fibre Channel Switch, there are a few things to consider like prerequisites, compatibility matrixes, and failover matrixes before you start deploying.

This chapter has the following topics:

- ▶ 2.1, “Compatibility” on page 14
- ▶ 2.2, “Prerequisites” on page 16
- ▶ 2.3, “Additional considerations and sample scenarios” on page 18
- ▶ 2.4, “Limitations” on page 21
- ▶ 2.5, “Configuring additional F_Ports” on page 24

2.1 Compatibility

The implementation process of an Access Gateway is fast and simple, and when setting up new systems the necessary hardware is installed in a relatively short amount of time.

The Brocade SAN Switch Modules (in both switch mode and Access Gateway mode) is supported in the BladeCenter chassis as shown in Table 2-1.

Table 2-1 BladeCenter Chassis Support matrix

Part	I/O Module	BCS	BCE	BCT	BCH	BCHT
32R1812	Brocade 20 port 4 Gb SAN Switch Module	No	Yes	Yes	Yes	Yes
32R1813	Brocade 10 port 4 Gb SAN Switch Module	Yes	Yes	Yes	Yes	Yes

You must install SAN Switch Modules only in I/O-module bays 3 and 4 (see Figure 2-1) of the BladeCenter unit. An HBA is required on all blade servers that requires access. Installing a switch module in I/O-module bay 3 or bay 4 provides the first connection to any installed Fibre Channel expansion card in the BladeCenter unit. Installing a second switch module enables a second connection to a Fibre Channel expansion card in the BladeCenter unit. Adding a second switch module provides a redundant path and a separate Fibre Channel connection from the blade server to the external Fibre Channel network and SAN.

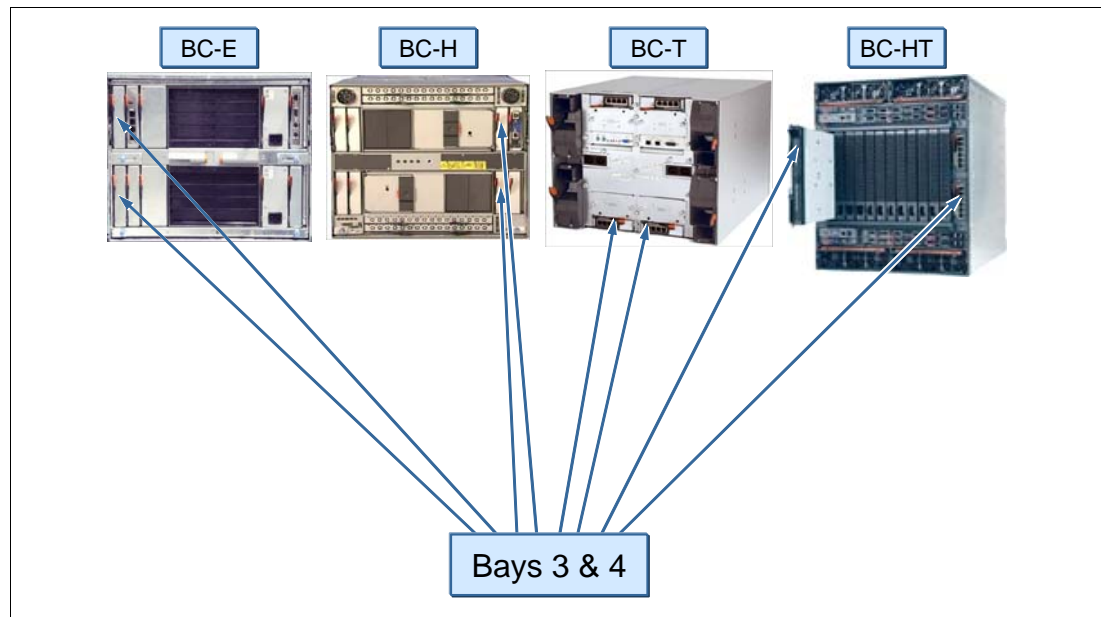


Figure 2-1 Ports 3 and 4 on the BladeCenter chassis

Use one of the expansion cards listed in Table 2-2 on page 15 and see in which specific server they are supported.

Table 2-2 on page 15 lists the available Fibre Channel expansion cards and which servers support them.

In all BladeCenter chassis, you use bays 3 and 4 to house the Access Gateway modules. You also install a matching Fibre Channel expansion card in each blade server. The compatible HBAs are shown in the top part of Table 2-2 on page 15.

Table 2-2 BC Server and Expansion Card Support matrix

Part number	Switch	HS20	HS21	HS21 XM	LS20	LS21	LS41	JS20	JS21
HBA expansion cards for use with switch modules in chassis bays 3 and 4									
26K4841	IBM SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
26R0884	QLogic® 4 Gb Standard FC Expansion Card	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
26R0890	QLogic 4 Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
39Y9186	Emulex 4 Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
41Y8527	QLogic 4 Gb Fibre Channel Expansion Card (CFFv)	No	Yes	Yes	No	Yes	Yes	No	Yes
43W6859	Emulex 4 Gb CFFv FC Expansion Card	No	Yes	Yes	No	Yes	Yes	No	Yes
HBA expansion cards for use with an MSIM in BladeCenter H and HT chassis									
39Y9306	QLogic Ethernet and 4 Gb FC Expansion Card (CFFh)	No	Yes	Yes	No	Yes	Yes	No	Yes

The BladeCenter H and HT chassis also support Access Gateway modules in a Multi-switch Interconnect Module (MSIM), see Figure 2-2, provided you install a suitable CFFh type expansion card, such as the QLogic Ethernet and 4 Gb Fibre Channel CFFh expansion card (part number 39Y9306), as listed in bottom part of Table 2-2.



Figure 2-2 Multi-switch Interconnect Module

The ports on the CFFh expansion cards in each server are hard wired to specific bays in the switch modules in each MSIM. Refer to Table 2-3 on page 16 for mappings of expansion card ports to the I/O bays of MSIMs.

Note: All supported SAN Switch Devices must be installed in the right hand I/O slot, while the supported Ethernet Switch Devices operate only in the left hand I/O slot of the MSIM. The OPM works in both of the MSIM slots.

Table 2-3 Mapping of expansion card ports to the I/O bays of MSIMs

Port number of the CFFh expansion card	Corresponding switch module bay in the MSIM
1	7 (Upper left interconnect module bay)
2	8 (Upper right interconnect module bay)
3	9 (Lower left interconnect module bay)
4	10 (Lower right interconnect module bay)

The compatibility between HBAs with the respective blade chassis is shown in Table 2-4.

Table 2-4 Compatibility between expansion cards and chassis

P/N	Expansion Card	BC-E	BC-T	BC-H	BC-HT
HBA expansion cards for use with switch modules in chassis bays 3 and 4					
26K4841	IBM SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
26R0884	QLogic 4 Gb Standard FC Expansion Card	Yes	Yes	Yes	Yes
26R0890	QLogic 4 Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
39Y9186	Emulex 4 Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
41Y8527	QLogic 4 Gb Fibre Channel Expansion Card (CFFv)	Yes	Yes	Yes	Yes
43W6859	Emulex 4 Gb CFFv Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
HBA expansion cards for use with an MSIM in BladeCenter H and HT chassis					
39Y9306	QLogic Ethernet and 4 Gb FC Expansion Card (CFFh)	No	No	Yes ^a	Yes ^a

a. Requires the use of a Multi-switch Interconnect Module (MSIM)

For the latest support information, see one of the following resources:

- ▶ ServerProven®:
 - <http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html>
- ▶ Configuration and Option Guide:
 - <http://www.ibm.com/support/docview.wss?rs=1201&uid=psg1SCOD-3ZVQ5W>

2.2 Prerequisites

Apart from the Hardware Prerequisites which are covered in the Compatibility section above, there is only the NPIV functionality on the edge switches that you have to consider.

Firmware of the Fabric (edge) Switches

An *edge switch* is a switch that provides the entry point into the Fabric. As described in Chapter 1, "Introduction and Technology" on page 1, the use of an Access Gateway requires

NPIV functionality to be enabled on the edge switch. An Access Gateway can connect to the edge switches listed in Table 2-5 with its dedicated firmware only:

Table 2-5 Prerequisites for the edge switches

Manufacturer	Models	Firmware	Notes
Brocade	SilkWorm 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4100, 4900, 7500, 24000, 48000	v5.1.0 or later	Notes ^a
Cisco	MDS9120, MDS9140, MDS9216, MDS9506, MDS9509	SAN-OS 2.1(2b) or later	Notes ^b
QLogic	SANbox® 5200, 5202, 5600, 5602, SANbox 9000	v6.0 or later	Notes ^c
McDATA	Sphereon 3016, 3032, 3216, 3232, 4300, 4500, Intrepid 6064, 6140, 10000	E/OS 8.0 or later	Notes ^d

- a. Brocade models 3014, 3250, 3850, 3900, and 24000 have NPIV support defaulted OFF and must be activated on a port by port basis. All other models support NPIV by default.
- b. Cisco switches have NPIV support defaulted OFF. It is activated on a switch wide basis.
- c. QLogic switches have NPIV support defaulted ON.
- d. McDATA switches require an optional license to activate NPIV capabilities on the listed switches. McDATA switches will not require an additional NPIV license after E/OS 9.6.x because the license is included.

Note: The optional licenses for the McDATA Switches for enabling NPIV can be ordered from Brocade with no additional cost. With EOS 9.6 and later no NPIV license is necessary. However, NPIV needs to be enabled on each port.

Zoning

Use zoning to create an isolation of the fabric and the different environments so that only members in the same zone can communicate.

Because all zoning features are removed on the Access Gateway, you have to set up the zoning configuration on the fabric switch outside of the BladeCenter.

There are two zoning methods:

- ▶ Port-based zoning:

It is based on the physical fabric port number. The members of a zone are physical ports on the fabric switch. One of the disadvantages of hardware zoning is that devices have to be connected to a specific port, and the whole zoning configuration could become unusable when the device is connected to a different port. In cases where the device connections are not permanent, the use of hardware zoning is not recommended.

- ▶ WWN zoning:

It is implemented by the fabric operating systems within the fabric switches. When using software zoning the members of the zone can be defined using their World Wide Names. With software zoning there is no need to worry about the physical connections to the switch. If you use WWNs for the zone members, even when a device is connected to another physical port, it will still remain in the same zoning definition, because the device's WWN remains the same. The zone follows the WWN.

If you have a zoning configured in your existing fabric, moving from pass-through mode to Access Gateway mode requires no changes to the zoning configuration.

If you change from the full switch mode to the Access Gateway and you use WWN zoning, there are also no changes required to the existing configuration.

Dynamic Ports on Demand

If you use a 10-Port SAN Switch Module with Dynamic Ports on Demand (DPOD) enabled, you can choose which of the ports you want to use so the ten ports are not fixed to the slots in the chassis.

There are no limitations when using DPOD associated with Access Gateway mode.

Licensing

The Access Gateway can be mode enabled on a 10-port 4 Gb SAN Switch Module as well as in the 20-port 4 Gb SAN Switch Module that has FOS v5.2.1b or later.

The 10-port switch module with DPOD allows connection for any combination of internal blade servers and external ports up to a total of 10 ports. The 20-port switch module allows connection to all 14 internal ports and six external ports. The 10-port switch module is upgradeable to the 20-port version with a simple pay-as-you-grow scalability through a license key.

Table 2-6 lists the product and order information for these modules and the upgrade license.

Table 2-6 Product and order information

Description	Order number
Brocade 10-Port 4 Gb SAN Switch Module	32R1813
Brocade 20-Port 4 Gb SAN Switch Module	32R1812
Brocade 10-Port Upgrade to a 20-Port Module	32R1822

Note: If you need to attach a storage or tape device to the module, you will need to run the switch module in Full Fabric Switch Mode instead of Access Gateway mode. You can switch between Brocade Access Gateway Mode and the standard switch mode operation using the CLI or Web Tools. For details, refer to 3.6, “Converting to Access Gateway mode” on page 48.

Tip: If you are converting an existing switch to a Brocade Access Gateway, save the switch configuration before enabling Access Gateway mode.

2.3 Additional considerations and sample scenarios

Previously, we had two options for connecting BladeCenter to a SAN: using a Fibre Channel switch or using an Optical Pass-thru Module.

2.3.1 Switch connection

Connectivity to the SAN over a switch with all features and administration gives you:

- ▶ 14 internal ports (ports 1 to 14) connect to IBM BladeCenter server blades
 - Auto-sensing at 2 Gbps or 4 Gbps and server blades log into the switch as F-ports (requires optional Fibre Channel Expansion Card installed on server blade)

- ▶ Six external ports (ports 0, 15, 16, 17, 18, and 19)
 - Connect to existing Fibre Channel SAN switches, other Brocade FC Switch modules, or directly to Fibre Channel Storage devices
 - Auto-negotiate link speed (1 Gbps, 2 Gbps, or 4 Gbps)
 - U-port initialization (E-port, F-port, or FL-port)
 - Can form up to two 12 Gbps ISL Trunks (requires ISL Trunking license)
 - Dynamic Path Selection (DPS) for improved load balancing the 24 Gbps of available external bandwidth between the two ISL Trunk groups
- ▶ Two internal full-duplex 100Mbps Ethernet interfaces, terminated at a single MAC
- ▶ Hot code activation
- ▶ Frame-filtering technology that enables Advanced Zoning and Advanced Performance Monitoring capabilities
- ▶ Integrated security features, including SSH (secure shell), SSL/HTTPS, Radius Support, SNMPV3, Audit Logging, and Role Based Access Control (RBAC)
- ▶ Redundant power and cooling provided by IBM BladeCenter chassis

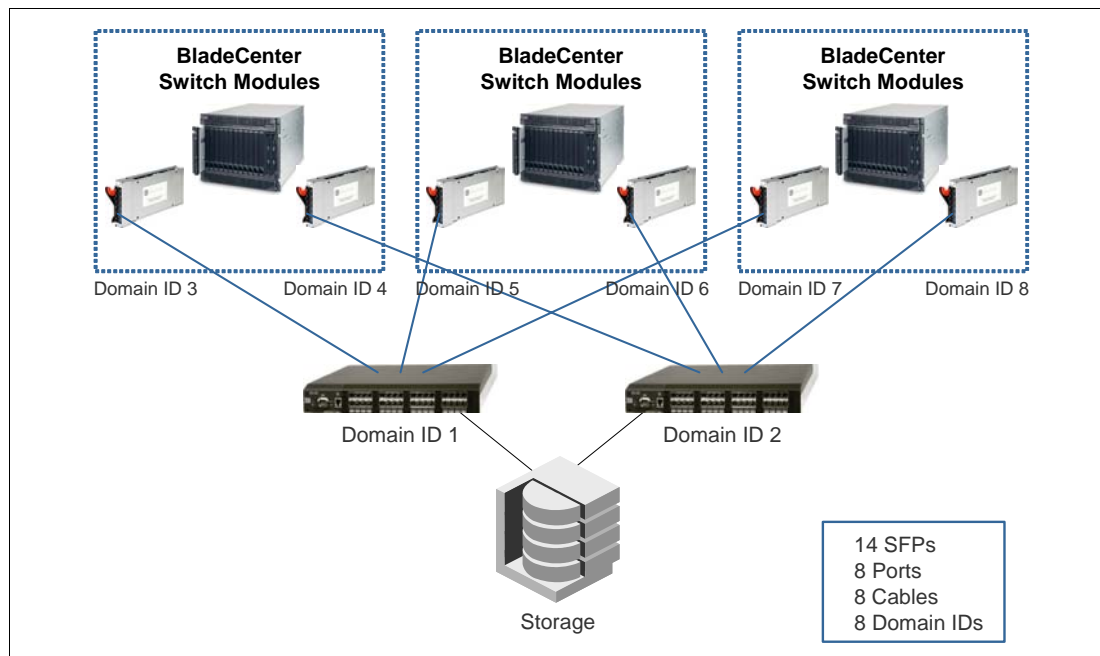


Figure 2-3 Switch Connection

2.3.2 Optical Pass-thru Module connection

The Optical Pass-thru Module (OPM) is an unswitched/unblocked optical connection to each blade server and delivers additional flexibility in data center network architectures. The OPM provides seamless integration into existing infrastructures that have already standardized on a specific SAN fabric. The OPM delivers compatibility with TotalStorage® family, Enterprise Storage Server®, and IBM SAN switches.

The OPM has these features:

- ▶ Conforms to mechanical and electrical requirements for BladeCenter

- ▶ Transmits and receives network data between blades and the following network environments:
 - Gigabit Ethernet
 - Fibre Channel
 - Myrinet
- ▶ Auto-sense capability to allow single design to work in network
- ▶ Self test and diagnostics capability

A configuration using OPMs is shown in Figure 2-4.

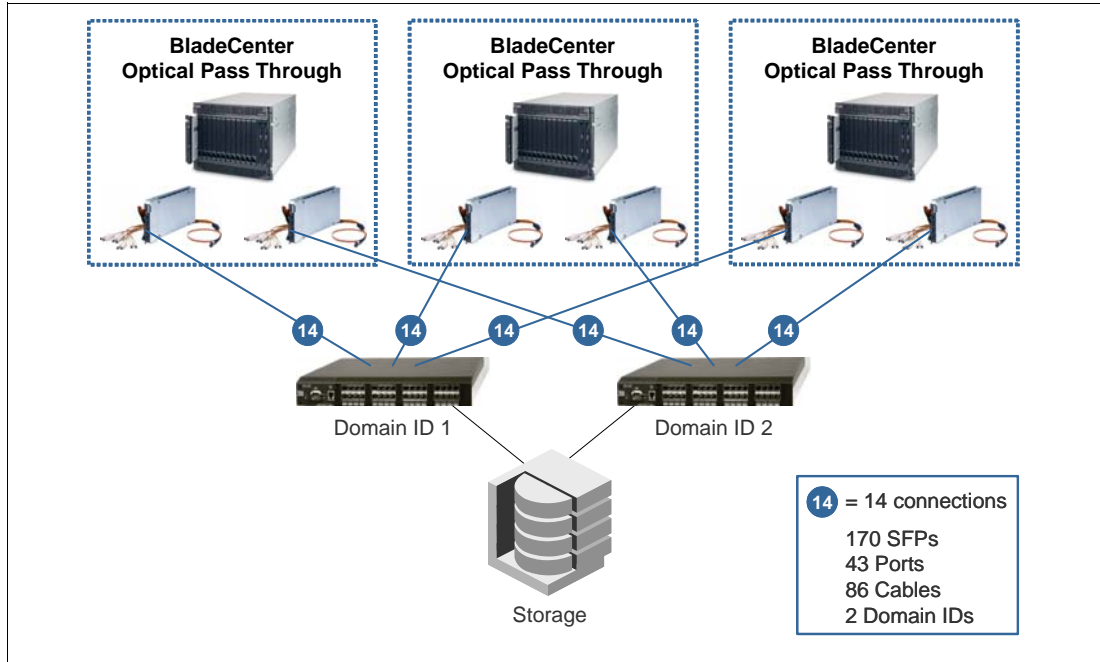


Figure 2-4 OPM Connection

Note that the OPM configuration shown here requires two external switches with at least 43 ports (3x14+1), whereas with the Access Gateway you only need an 8-port external switch. This represents a significant cost savings for the switches, cables, and SFP media.

2.3.3 Using an Access Gateway

If you have large Fibre Channel fabrics that exceed 30 switches, then choosing either of the above configurations can result in:

- ▶ Potentially excessive domains since each switch gets its own domain ID (McDATA fabrics cannot exceed 31 domains) or
- ▶ A lot of cables, SFPs, and physical ports (28 for each BladeCenter chassis) if you use OPMs

The Access Gateway offers a new way to connect to a SAN without these drawbacks:

- ▶ The Access Gateway uses NPIV technology, which means that the internal server ports (up to 14) are mapped to the six external ports. Extensive cabling, large number of SFPs, and port licenses are no longer required.
- ▶ With the Access Gateway, no domains are added to the SAN fabric, allowing greater scalability for environments that are nearing the maximum domain limits.

Figure 2-5 shows a sample Fibre Channel fabric with the minimum HW requirements.

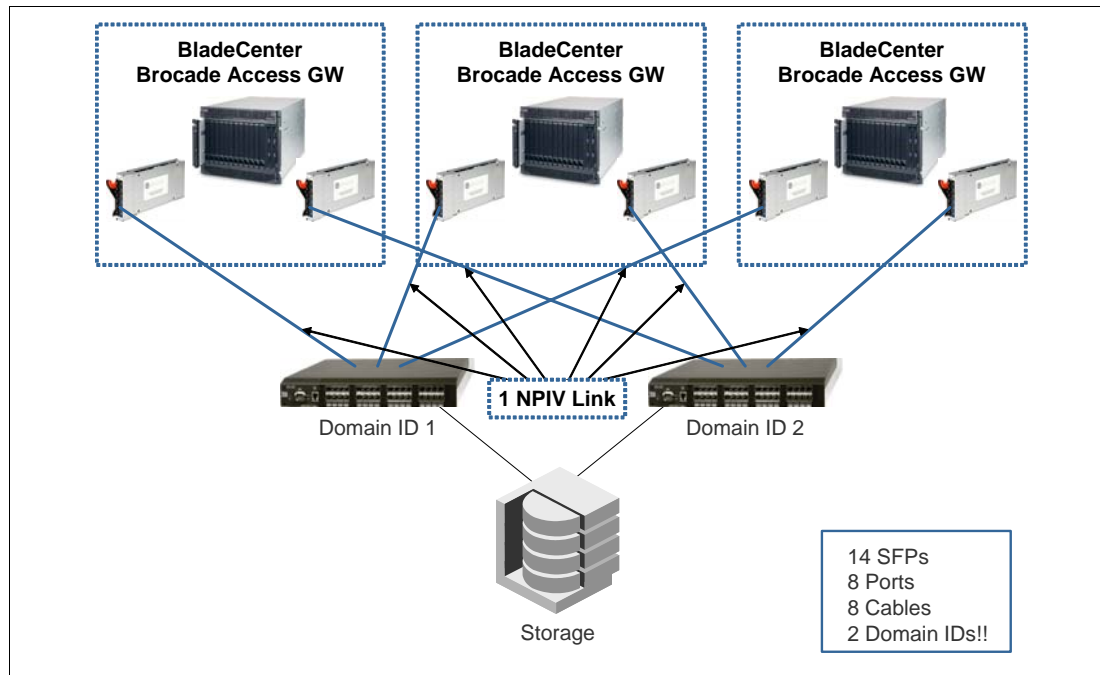


Figure 2-5 Brocade Access Gateway Connection

2.4 Limitations

If you plan to implement an Access Gateway, pay attention to the following limitations:

- There is no physical-port or virtual-port limitation on the Brocade Access Gateway Module; that means all of the 14 internal ports can be mapped to one physical external port.

The only limits which have to be considered is on the edge switches, which depend on the port limit of the NPIV technology shown in Table 2-7.

Table 2-7 PID Limit

	Default	Maximum
Per port	126	255
Per switch	15 x switch ports	126 x switch ports

Theoretically, there can be a maximum of 255 virtual PIDs per port. However, every port in the switch might not have 255 virtual PIDs because of the limit on the maximum number of virtual PIDs a switch can have.

- Only hosts/initiators can be connected to the Access Gateway, so no target devices (storage or tape) are initially supported.

Note: By default all external ports present N_Ports to the edge fabric switch. If you want to use an external port for connecting a host, you have to configure this port as an F_Port which is described in 2.5, “Configuring additional F_Ports” on page 24.

- ▶ The Access Gateway does not support loop devices:
 - FL_Port is the fabric connection in a public loop for an arbitrated loop topology
 - NL_Port is the node connection in a public loop for an arbitrated loop topology
- ▶ Cascading between Access Gateway devices is currently not supported.
- ▶ An Access Gateway cannot connect to multiple fabrics although this support is planned for FOS Version 6.0.
- ▶ Up to 30 Access Gateway devices can be connected to a director and 10 to an edge switch (this is a tested support statement, not a hardware or software limitation). This number will increase with future releases.

2.4.1 Failover and failback policies

By default, both policies, failover and failback, are enabled on all external ports. So if an N_Port fails, all F_Ports that are mapped to this will be distributed among all the online N_Ports in a sequence which is described in the following example:

Figure 2-6 displays a simple configuration with two hosts (blades) for explaining the failover and failback policies. The green line shows the default mapping according to Table 2-8 on page 23.

To demonstrate the failover we disconnected the active FC Connection from N_Port 0 to the Fabric (marked with the red X). After that, the second connection becomes active and the mapping changes to the N_Port 15 which is highlighted by the red line.

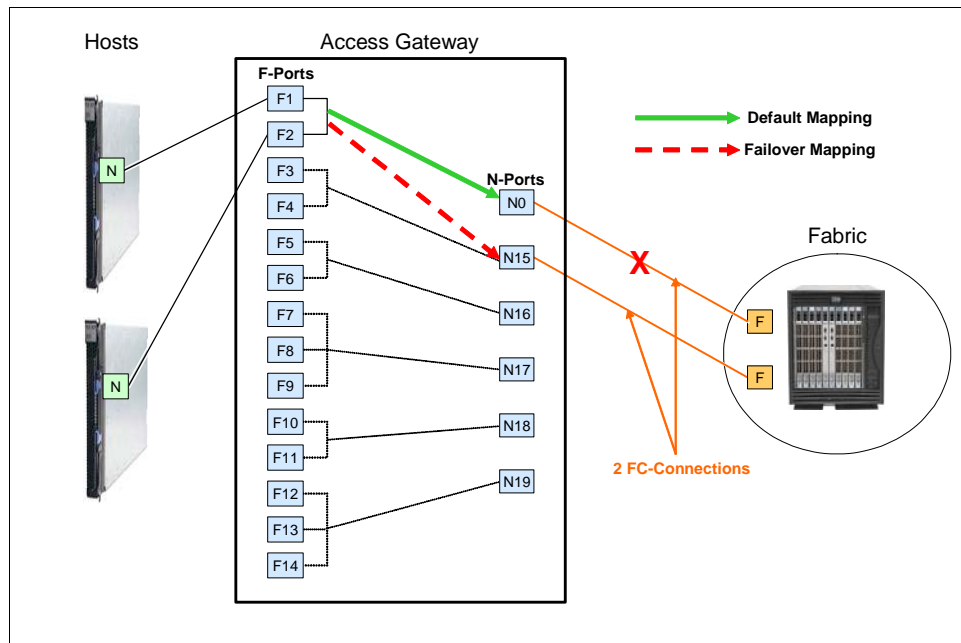


Figure 2-6 Failover scenario

Table 2-8 Default port mapping

		External Ports					
		0	15	16	17	18	19
Internal Ports	1	Yes	No	No	No	No	No
	2	Yes	No	No	No	No	No
	3	No	Yes	No	No	No	No
	4	No	Yes	No	No	No	No
	5	No	No	Yes	No	No	No
	6	No	No	Yes	No	No	No
	7	No	No	Yes	No	No	No
	8	No	No	No	Yes	No	No
	9	No	No	No	Yes	No	No
	10	No	No	No	No	Yes	No
	11	No	No	No	No	Yes	No
	12	No	No	No	No	No	Yes
	13	No	No	No	No	No	Yes
	14	No	No	No	No	No	Yes

The following sequence describes the behavior of the module in case of an offline N_Port caused by a failed connection.

1. According to the default mapping the two online F-Ports 1 and 2 are mapped to the external Port 0 (N-Port).

The `ag --mapshow` command displays the current mapping as shown in Figure 2-7. The columns **Failover** and **Failback** indicate whether or not the FO or FB policies are enabled or disabled.

```

brocade4Gb:USERID> ag --mapshow
N_Port  Configured_F_Ports    Current_F_Ports    Failover  Failback
-----
  0      1;2;                  1;2;               1         1
 15      3;4;                  None                1         1
 16      5;6;7;                None                1         1
 17      8;9;                  None                1         1
 18      10;11;                None                1         1
 19      12;13;14;             None                1         1
-----

```

Failover and Failback is enabled

Figure 2-7 ag --mapshow

To enable or disable those two settings, use the commands shown in Table 2-9 on page 24:

Table 2-9 Commands to enable and disable policies

	Enable	Disable
Failover	<code>ag --failoverenable <portnr></code>	<code>ag --failoverdisable <portnr></code>
Failback	<code>ag --failbackenable <portnr></code>	<code>ag --failbackdisable <portnr></code>

2. We disconnect the cable from the fabric to Port 0 and the N_Port goes offline.
3. All F_Ports mapped to that N_Port are disabled.
4. The F_Ports failover to the other online N_Port 15.

If there is more than one online N_Port, the F_Ports would be distributed among the remaining online N_Ports.

The `mapshow` command in Figure 2-8 shows the mapping after the failover.

```

brocade4Gb:USERID> ag --mapshow
N_Port  Configured_F_Ports      Current_F_Ports      Failover Failback
-----
  0      1;2;                      None                  1         1
 15      3;4;                      1;2;                 1         1
 16      5;6;7;                    None                  1         1
 17      8;9;                      None                  1         1
 18      10;11;                   None                  1         1
 19      12;13;14;                None                  1         1
-----
brocade4Gb:USERID> timed out waiting for input: auto-logout

```

Figure 2-8 `ag --mapshow`

5. The F_Port is re-enabled on the new N_Port.
6. The host establishes a new connection with the fabric.
7. After reconnecting the cable to external port 0, the N_Port becomes active again and the enabled failback policy reroutes the F_Ports 1 and 2 back to the originally mapped N_Port 0.

Note: The failover and failback processes have the potential of being disruptive. After the N_Port goes offline all mapped F_Ports are disabled and are re-enabled on the new N_Port. That means that the host has to establish a new connection to the fabric.

This process is similar to a cable pull on a fixed switch. The host will re-establish its fabric connection automatically. In many instances, this would be transparent to the OS and user level applications.

2.5 Configuring additional F_Ports

By default all internal blade ports are defined as F_Ports and only external ports are configured as N_Ports. The Access Gateway lets you configure the external ports as F_Ports so that you can connect additional FC_Initiators (no target devices) to the external ports.

The Access Gateway must have at least one configured N_Port. All remaining ports can be mapped to an N_Port.

- Map the newly converted F_Port 19 to the N_Port 0 using the `ag --mapadd` command as shown in Figure 2-11.

```

brocade4Gb:USERID> ag --mapadd 0 19
F-Port to N-Port mapping has been updated successfully

```

N_Port
F_Port

Figure 2-11 `ag --mapadd`

- Finally, you can verify the new mapping with the `ag --mapshow` and `ag --mapshow 0` commands.

```

brocade4Gb:USERID> ag --mapshow
N_Port  Configured_F_Ports  Current_F_Ports  Failover  Failback
-----
  0      1;2;19;              1;2;            1         1
 15      3;4;                None            1         1
 16      5;6;7;              None            1         1
 17      8;9;                None            1         1
 18     10;11;              None            1         1
-----

brocade4Gb:USERID> ag --mapshow 0

N_Port                : 0
Failover(1=enabled/0=disabled) : 1
Failback(1=enabled/0=disabled) : 1
Current F_Ports       : 1;2;
Configured F_Ports    : 1;2;19;

```

new mapped F_Port 19

Figure 2-12 `ag --mapshow`

- Lock the port again using the `portcfgnport` command again as shown in Figure 2-10 on page 25.

To delete the new mapping use the following command as shown in Figure 2-13:

`ag --mapdel <N_Port> <F_Port>`

```

brocade4Gb:USERID> ag --mapdel 0 19
F-Port to N-Port mapping has been updated successfully

```

N_Port
F_Port

```

brocade4Gb:USERID> ag --mapshow 0

N_Port                : 0
Failover(1=enabled/0=disabled) : 1
Failback(1=enabled/0=disabled) : 1
Current F_Ports       : 1;2;
Configured F_Ports    : 1;2;

```

Figure 2-13 `ag --mapdel`

The `ag --mapshow` command also in Figure 2-13 on page 26 displays that the mapping has been deleted successfully.



Implementation

This chapter describes the simple implementation of the Brocade Access Gateway. It starts with the basic setup of the fabric switches and ends with the WWN availability in the name Server of the Fabric switches.

The topics we cover in this chapter are:

- ▶ 3.1, “NPIV support” on page 30
- ▶ 3.2, “Enabling NPIV” on page 35
- ▶ 3.3, “Blade Server setup” on page 40
- ▶ 3.4, “Setup of the Brocade Access Gateway in the AMM” on page 41
- ▶ 3.5, “Firmware update to the latest version” on page 45
- ▶ 3.6, “Converting to Access Gateway mode” on page 48
- ▶ 3.7, “Connecting to the fabric” on page 54
- ▶ 3.8, “Command reference” on page 66

Our sample configuration consists of three different Fabric switches from these vendors:

- ▶ Cisco MDS
- ▶ Brocade B-Series
- ▶ Brocade M-Series (formerly McDATA)

Note that the use of the Access Gateway is not limited to just the switches used in our testing. Check the Brocade Connect Web site and check for the Tech Notes for the latest technical notes available regarding connecting Access Gateway to external SAN fabrics. Go to the following URL and select **Documentation Library** then **Technical Notes**:

<http://www.brocadeconnect.com>

In this chapter, we show how to configure each of these switches using both command-line (CLI) tools and browser-based (GUI) tools.

Figure 3-1 on page 30 shows the configuration used including the World Wide Names and IP addresses of the devices.

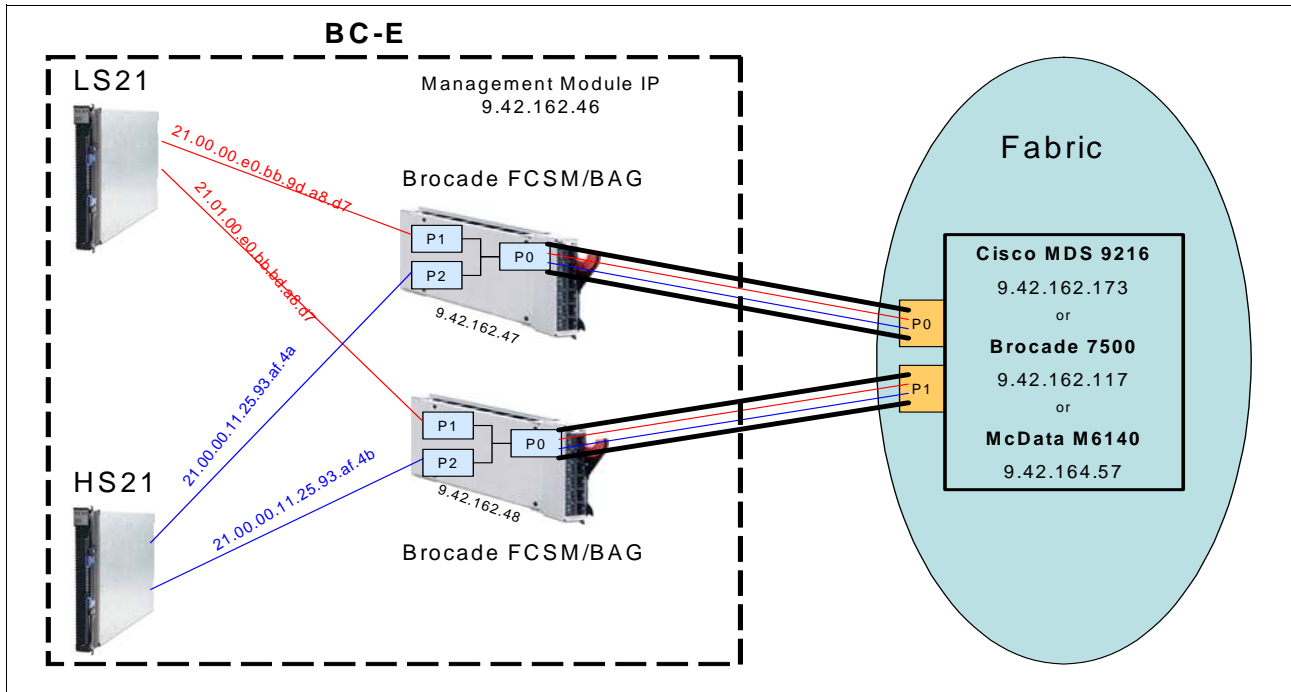


Figure 3-1 Lab configuration

3.1 NPIV support

Brocade Access Gateway must connect to a fabric that supports NPIV. Check the firmware of the edge switches to confirm if NPIV is supported:

- ▶ Brocade: Version 5.1.0 or later
- ▶ Cisco: Version 3.0 or later
- ▶ McDATA: Version 9.0 or later
- ▶ QLogic: Version 6.0 or later

Note: Before executing a firmware update, visit the support site of your switch vendor for the prerequisites and the installation instructions.

3.1.1 Cisco MDS

The IOS version, uptime, and hardware information are displayed using the following CLI command:

show version

Figure 3-2 on page 31 shows the output on our Cisco MDS 9216 switch.

```

mds9216_BC3# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

Software
  BIOS:      version 1.1.0
  loader:    version 1.2(2)
  kickstart: version 3.1(3a)
  system:    version 3.1(3a)

  BIOS compile time:      10/24/03
  kickstart image file is: bootflash:///m9200-ek9-kickstart-mz.3.1.3a.bin
  kickstart compile time: 5/22/2007 17:00:00 [06/16/2007 14:00:22]
  system image file is:   bootflash:/m9200-ek9-mz.3.1.3a.bin
  system compile time:    5/22/2007 17:00:00 [06/16/2007 14:16:29]

Hardware
  cisco MDS 9216 ("1/2 Gbps FC/Supervisor")
  Intel(R) Pentium(R) III CPU with 963828 kB of memory.
  Processor Board ID JAB074907UK

  bootflash: 250368 kB
  slot0:      0 kB

mds9216_BC3  kernel uptime is 4 days 20 hours 46 minute(s) 1 second(s)

  Last reset at 968127 usecs after Thu Aug 16 15:27:29 2007
    Reason: Reset by installer
    System version: 2.0(3)
    Service:

```

Figure 3-2 show version

Ensure that the highlighted entries show Version 3.0 or later.

If the Cisco Device Manager is used, you can also determine the installed version of the firmware by clicking **Physical** → **System** and viewing the description field, as shown in Figure 3-3 on page 32.

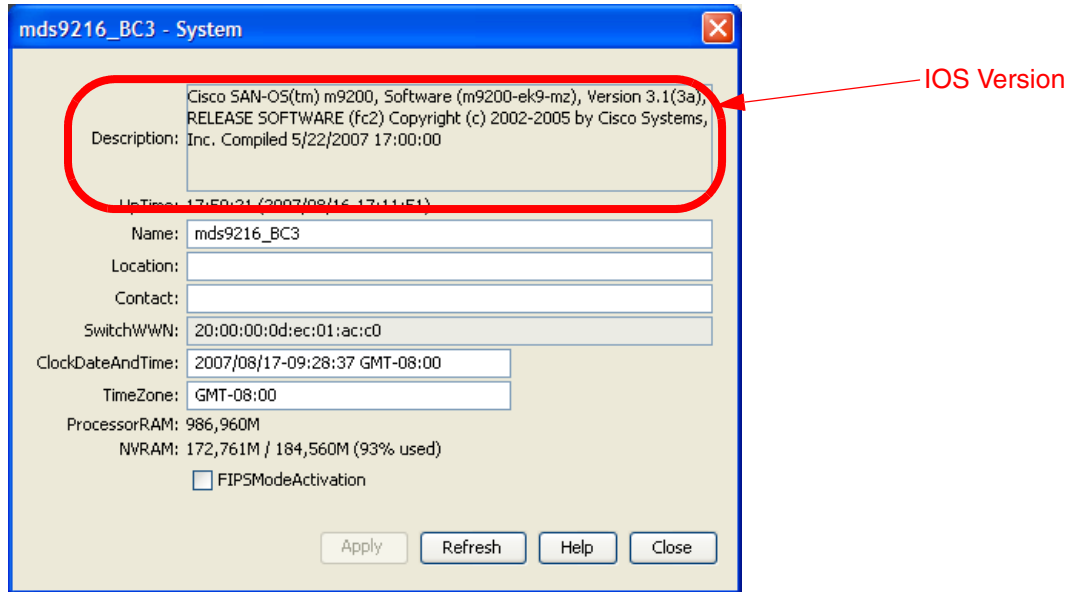


Figure 3-3 Cisco Device Manager

3.1.2 Brocade B-Type

You can determine the firmware level of the Brocade using either a command or through a browser-based UI.

The **version** command displays the Fabric OS release as you can see in Figure 3-4.

```
swd77:admin> version
Kernel:      2.4.19
Fabric OS:   v5.2.0a
Made on:    Thu Oct 5 21:23:41 2006
Flash:      Tue Feb 20 15:53:36 2007
BootProm:   4.5.3
```

Figure 3-4 Firmware version using the CLI

The Web Tools management software can be launched from the Advanced Management Module or directly using a browser and the switch's IP address. The main window, shown in Figure 3-5 on page 33, displays the Fabric OS version.

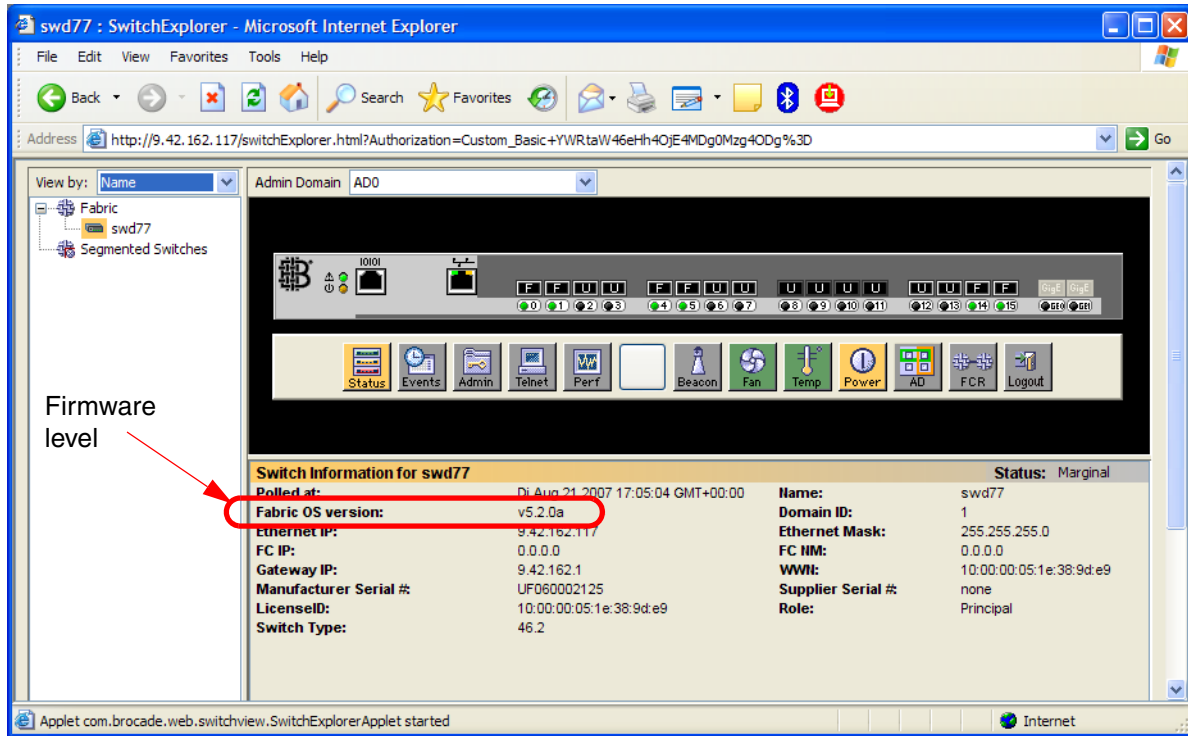


Figure 3-5 System properties

3.1.3 Brocade M-Type (formerly McDATA)

You can determine the firmware level of the McDATA switch using either a command or through a browser-based Enterprise Fabric Connectivity Manager (EFCM) UI.

If you connect to the switch using the browser-based EFCM, you will see the firmware level on the main window as shown in Figure 3-6 on page 34.

EFCM™ Basic Edition

Model Name: Intrepid 6140
 Switch Name: McData Core_ID5 (.57)
 IP Address: 9.42.164.57
 Domain ID: 1

Login: Administrator Logout
 Status: ⚠ Minor Failure
 State: Online

Fabric Product Configure Security Logs Maintenance Upgrade Help Last Updated 8/23/07 [14:08:53] Refresh

Product > Hardware

Front View **Rear View**

Name	McData Core_ID5 (.57)
Description	McData 6164
Location	SAN Central Lab
Contact	Parker Grannis
World Wide Name	1000080088A06E68
Type Number	006140
Model Number	001
Manufacturer	MCD
Serial Number	1312AD6
EC Level	1030716
Firmware Level	09.03.01 3

Firmware Level

Figure 3-6 Firmware level as seen in the Enterprise Fabric Connectivity Manager

The CLI command `show system` displays the system information including the firmware level as shown in Figure 3-7 on page 35.

```

Root> show system
Name:          McData Core_ID5 (.57)
Description:   McData 6164
Contact:       Parker Grannis
Location:      SAN Central Lab
Date/Time:    08/27/2007 15:44:00
Serial Number: 1312AD6
Type Number:  006140
Model Name:    Intrepid 6140
Model Number:  001
EC Level:     1030716
Firmware Version: 09.03.01 3
Beaconing:    Disabled

```

Figure 3-7 *show system*

3.2 Enabling NPIV

The next step is to verify that the NPIV function is enabled. We describe how to do that with all three switches, using both the GUI and the CLI as appropriate.

3.2.1 Cisco MDS

You must globally enable NPIV for all VSANs on the MDS switch to use multiple N_Port identifiers. Activation of NPIV on individual ports is not possible.

Figure 3-8 shows the sequence and the commands to enable NPIV.

```

mds9216_BC3 login: admin
Password:
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html
mds9216_BC3#
mds9216_BC3# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
mds9216_BC3(config)# npiv enable
mds9216_BC3(config)#

```

Figure 3-8 *Enabling NPIV on the Cisco switch*

To disable the NPIV function on the switch use the following command:

```
no npiv enable
```

Additionally, as a best practice, you should ensure that Open Systems Management Server (OpenSysMS) is enabled and that the PID allocation method is set to “Flat” as shown in Figure 3-9 on page 36.

```

conf t
no fcdomain fcid persistent vsan x
fcinterop fcid-allocation flat
end

```

← Optional

Figure 3-9 Setting PID allocation method to flat

Tip: For this setting to take place, you might need to disable and enable the VSAN or restart the switch.

3.2.2 Brocade

On the Brocade switches, you have to enable NPIV for each port that you want to use the NPIV functionality. This can be done through the GUI or from the command line.

On the main window, click the port that you want to change the settings of, and then click **Enable NPIV** in the General tab, as shown in Figure 3-10.

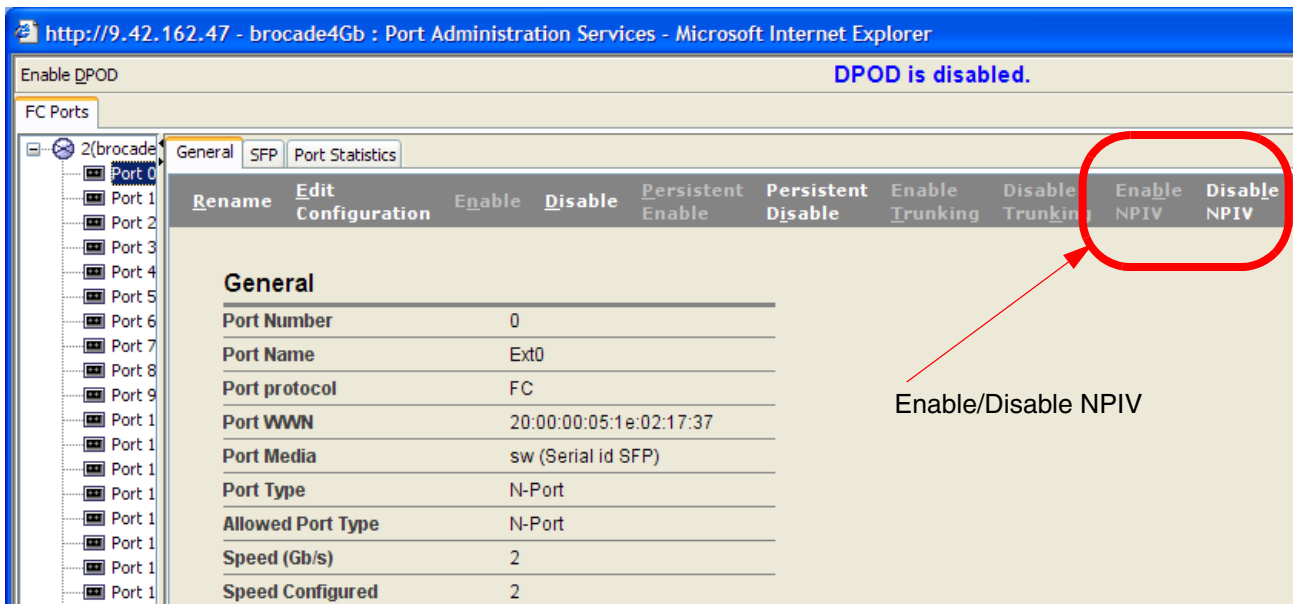


Figure 3-10 Port config

Using the CLI, the **portcfgnpiport** command enables or disables the NPIV capability on the dedicated port. The syntax of the command is:

portcfgnpiport Slot/PortNumber,Mode

where:

- ▶ Mode = 0 means disable NPIV on the port
- ▶ Mode = 1 means enable NPIV on the port

Figure 3-11 on page 37 shows the status of the ports before enabling NPIV.


```

swd77:admin> portcfgshow
Ports of Slot 0  0  1  2  3  4  5  6  7  8  9 10 11  12 13 14 15
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Speed           AN AN AN AN  2G 2G AN AN  AN AN AN AN  AN AN AN AN
Trunk Port      ON ON ON ON  ON ON ON ON  ON ON ON ON  ON ON ON ON
Long Distance   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
VC Link Init    .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Locked L_Port   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Locked G_Port   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Disabled E_Port .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
ISL R_RDY Mode .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
RSCN Suppressed .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Persistent Disable.. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
NPIV capability ON ON ON .  ON ON ON ON  ON ON ON ON  ON ON ON ON
EX Port        .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Mirror Port     .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..

                                where AN:AutoNegotiate, ..:OFF, ?:INVALID,
                                SN:Software controlled AutoNegotiation.
                                LM:L0.5
                                NPIV is disabled on Port 3

```

Figure 3-11 The portcfgshow command shows NPIV is not currently enabled on port 3

In Figure 3-12 we enabled the NPIV capability on port 3. The portcfgshow command confirms that NPIV is enabled.

```

swd77:admin> portcfgnpiport 0/3,1
swd77:admin> portcfgshow
Ports of Slot 0  0  1  2  3  4  5  6  7  8  9 10 11  12 13 14 15
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Speed           AN AN AN AN  2G 2G AN AN  AN AN AN AN  AN AN AN AN
Trunk Port      ON ON ON ON  ON ON ON ON  ON ON ON ON  ON ON ON ON
Long Distance   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
VC Link Init    .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Locked L_Port   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Locked G_Port   .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Disabled E_Port .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
ISL R_RDY Mode .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
RSCN Suppressed .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Persistent Disable.. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
NPIV capability ON ON ON ON  ON ON ON ON  ON ON ON ON  ON ON ON ON
EX Port        .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..
Mirror Port     .. .. .. ..  .. .. .. ..  .. .. .. ..  .. .. .. ..

                                where AN:AutoNegotiate, ..:OFF, ?:INVALID,
                                SN:Software controlled AutoNegotiation.
                                LM:L0.5
                                NPIV now enabled
swd77:admin>

```

Figure 3-12 Enabling NPIV on port 3

3.2.3 McDATA

McDATA switches require the installation of a feature key. This key is free of charge and can be requested from Brocade. To check if the feature is installed, you can use the EFCM as shown in Figure 3-13.

Note: With EOS 9.6 or later, no key is required.



Figure 3-13 EFCM

To check if the feature is installed using the command line, use the **config features show** command as shown in Figure 3-14 on page 39.

```

Root> config features show
Installed Feature Set      Feature              State  Exp
-----
NPIV                      NPIV                Enabled
Element Manager License   Element Manager License
SANtegrity Binding*      Binding Trial*       Disabled
SANtegrity Authentication*
SANtegrity Auth Trial*    SANtegrity Auth Trial*
Open Trunking*           Open Trunking Trial*
                          Disabled
* - Trial license is available for this feature
NPIV feature active

```

Figure 3-14 config features show

The next step is to activate NPIV on the ports and configure the number of virtual connections. In our scenario, we configured 10 virtual connections on port 0 and port 1 using the EFCM as shown in Figure 3-15. We recommend a setting of 15 because the maximum is 14 NPIV connections on a single lane.

The screenshot shows the EFCM Basic Edition interface for a switch named 'McData Core_ID5 (.57)'. The 'Configure > Ports > NPIV' page is active, displaying a message: '*Your changes have been successfully activated.' Below this, the 'NPIV State' is 'Enabled', with 'Enable' and 'Disable' buttons. A table lists ports 0 through 11. Ports 0 and 1 have a 'Login Limit' of 10, while ports 2 through 11 have a 'Login Limit' of 1. Red boxes and arrows highlight the 'NPIV State' and the 'Login Limit' values for ports 0 and 1.

Port	Name	Attached WWN	Port Type	Login Limit
0		None	G Port	10
1		None	G Port	10
2		None	G Port	1
3		None	G Port	1
4		None	G Port	1
5		None	G Port	1
6		None	G Port	1
7		None	G Port	1
8		None	G Port	1
9		None	G Port	1
10		None	G Port	1
11		None	G Port	1

Figure 3-15 Enable NPIV

This can also be achieved from the command line. Use the commands in Figure 3-16 for enabling NPIV, configuring virtual connections, and checking if NPIV is active as requested.

```
Root> config features NPIV 1 ← enables NPIV feature
Root>

Root> config NPIV maxPortIDs 0 10 ← enables 10 virtual connections on port 0
Root>

Root> show NPIV config ← shows NPIV configuration
NPIV State: Enabled
Port Max Allowed NPIV Logins
-----
0 10
1 10
2 1
3 1
4 1
5 1
```

Figure 3-16 NPIV configuration

3.3 Blade Server setup

This section discusses the steps required to set up blade servers regarding the Access Gateway implementation.

3.3.1 Install the HBA

To implement this solution we need to install a supported HBA in each blade server. Refer to Table 2-2 on page 15 for the list of all supported HBAs.

3.3.2 Manage the HBA

Go to the HBA BIOS configuration menu to manage the card. There are some different configuration menus depending on the card type. QLogic Fast!UTIL is one of the most commonly used in blade system.

There are two basic steps required to manage the HBA card.

1. Record the World Wide Port Name (WWPN) of the HBA.
It will be needed to define the storage group, host, and host port in the storage sub-system. It will also be needed to configure the zone in the external switches as shown in Figure 3-17 on page 41.

```

Press <Ctrl-Q> for Fast!UTIL

<CTRL-Q> Detected, Initialization in progress, Please wait...

ISP23xx Firmware Version 3.03.08

BIOS for Adapter 1 is disabled
QLogic adapter using IRQ number 7

```

Figure 3-17 HBA BIOS

2. Configure the Host Adapter BIOS.

The default value is Disabled. If we need to configure a Boot from SAN, we have to change the value to Enabled as shown in Figure 3-18.

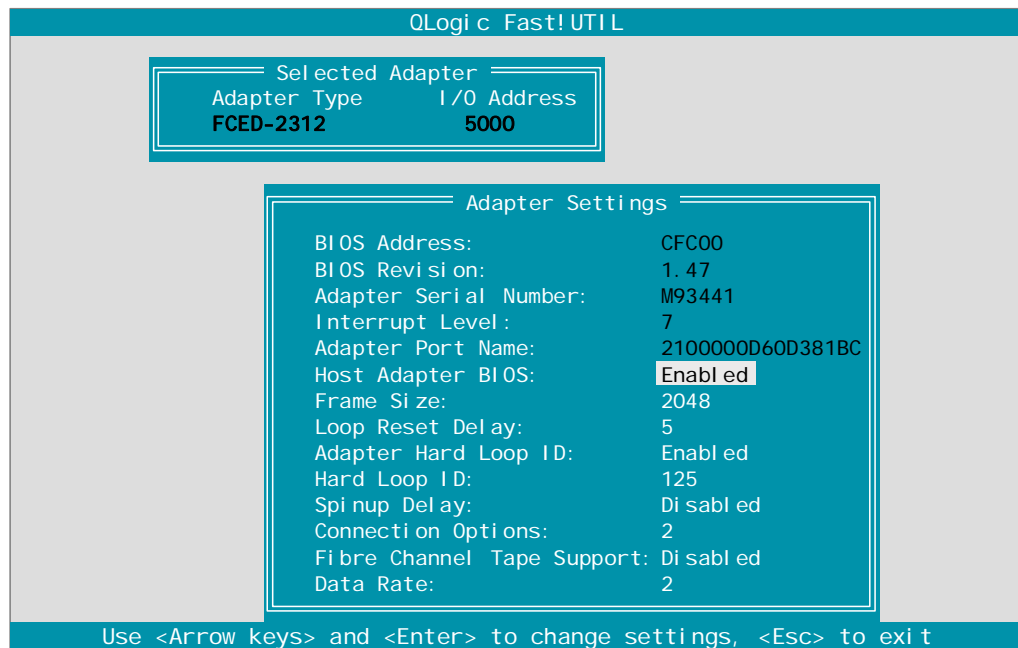


Figure 3-18 Manage the Host Bus Adapter BIOS

Note: Basic SAN connectivity requires no changes in Host Adapter BIOS settings.

3.4 Setup of the Brocade Access Gateway in the AMM

Note: Ensure that the appropriate and latest firmware for the Management Module or Advanced Management Module is installed.

The firmware is available on the IBM BladeCenter Web site:

<http://www.ibm.com/systems/bladecenter/support>

To connect to the switch module using the BladeCenter Management Module:

1. On your workstation, open a supported browser window.
2. In the address field, type the IP address of the Management Module.
3. When prompted, enter the user name and password. By default, the IBM BladeCenter Management Module user name is USERID and the password is PASSWORD (where 0 is a zero). User names and passwords are case sensitive.

Figure 3-19 shows the initial AMM view.

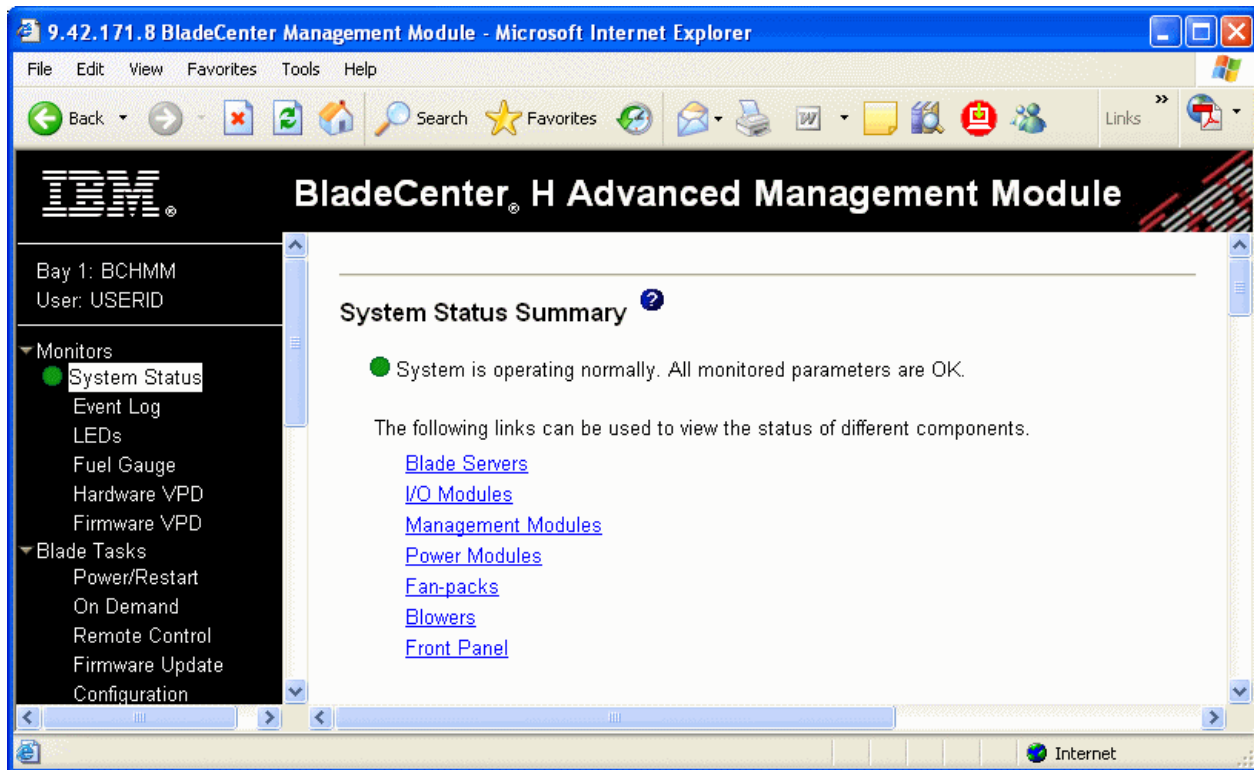


Figure 3-19 Initial BladeCenter H Advanced Management Module view

3.4.1 Setting the switch module IP address and enabling external ports

The default IP address for the switch module is 192.168.70.129 (for Bay 3) or 192.168.70.130 (for Bay 4) of the BladeCenter chassis. To change the IP address, perform the following:

1. In the I/O Module Tasks tab, click **Configuration**. Select Bay 3 or 4.
2. Change the IP address and click **Save** (see Figure 3-20 on page 43).

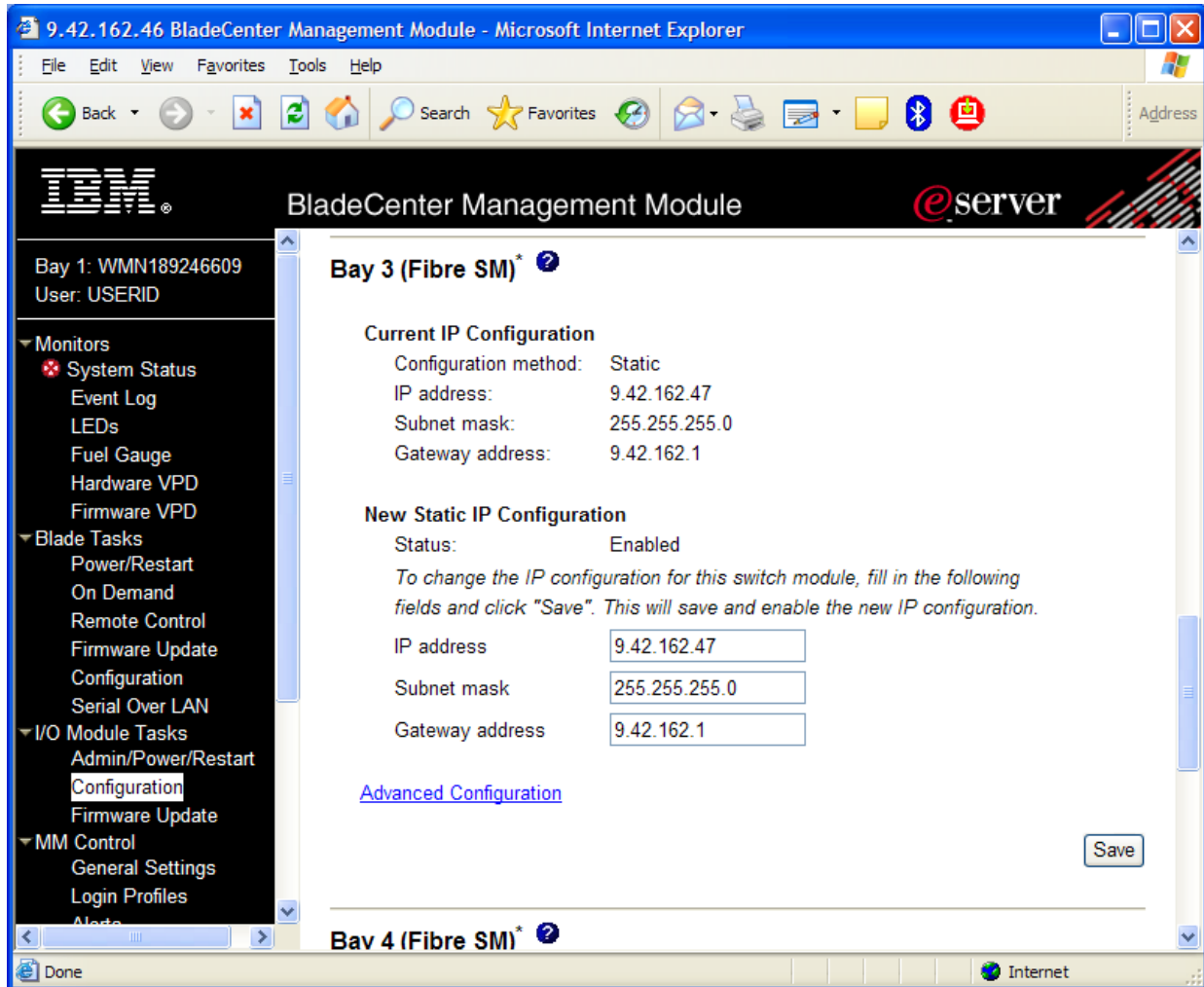


Figure 3-20 Setting the switch module IP address

Note: Use only the BladeCenter Management Module to set the switch module IP address. Do not use the switch module's CLI or Web Tools. Doing so can cause a loss of connectivity between the Management Module and the switch module. The switch module's IP address must be on the same IP subnet to communicate.

- While in the window shown in Figure 3-20 on page 43, click **Advanced Configuration** for the switch module. You will see a window similar to Figure 3-21. Ensure that the external ports are enabled. Click **Save**.

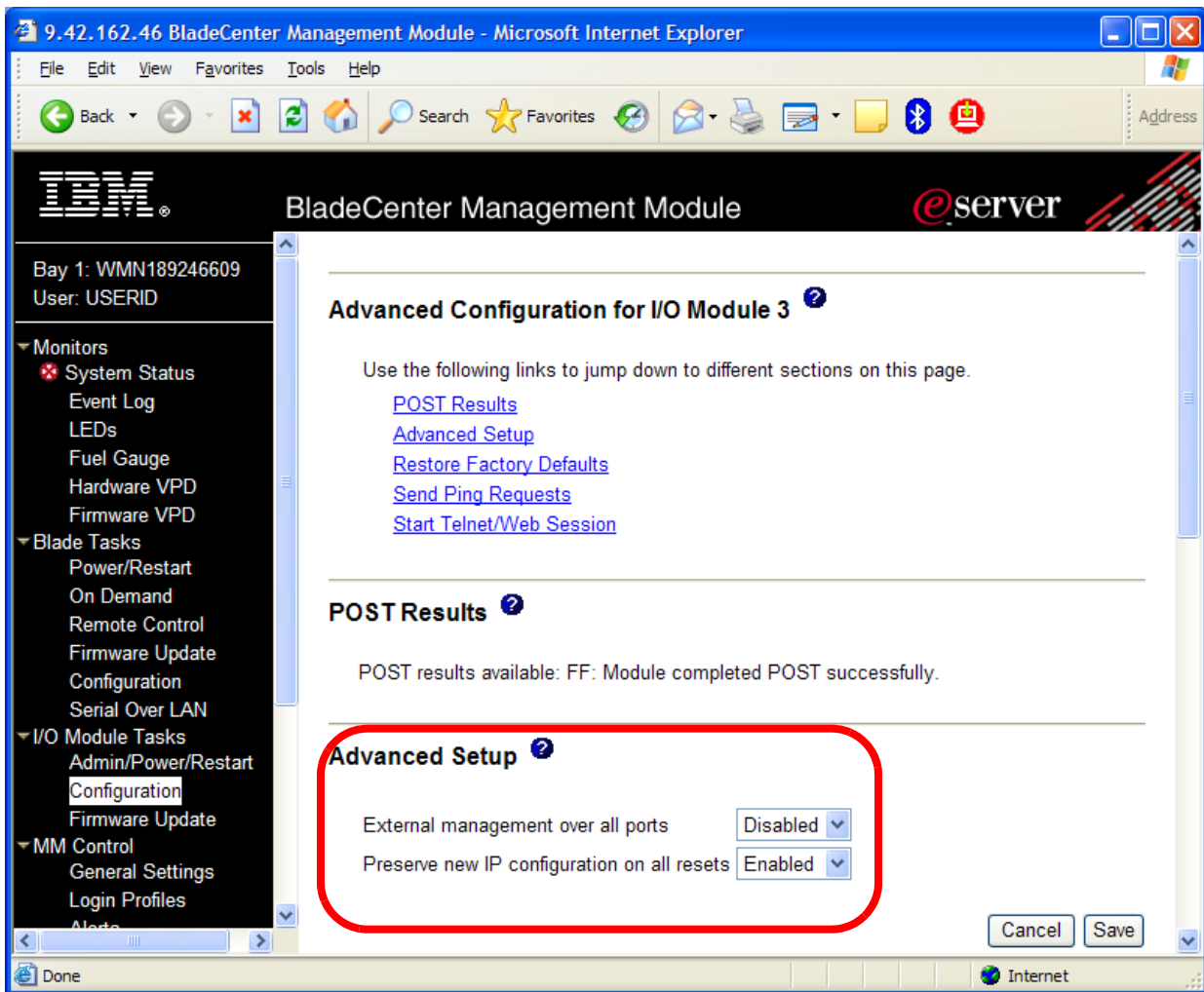


Figure 3-21 Enabling External Ports on switch module

- The remaining steps for configuring the switch module are performed either from the command line interface (CLI), through Telnet, or with Web Tools (through a browser). The Telnet/Web session is accessible from the Management Module window (see Figure 3-22) or you can access it outside the Management Module by using the switch module's IP address.

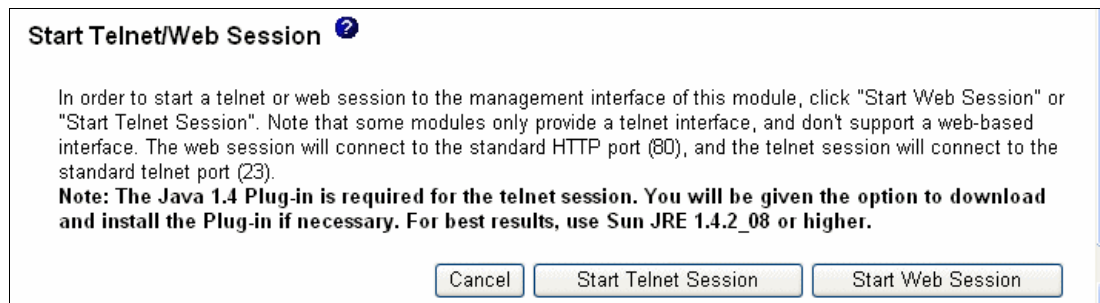


Figure 3-22 Launching Web or Telnet Session from the Management Module

3.5 Firmware update to the latest version

Log on to the FC switch module and check that the latest firmware is installed. Minimum version 5.2.x is required to enable Access Gateway mode.

Note: Version 5.2.1b or later is required to support Access Gateway mode in the Brocade FC switch modules. So before you convert to Access Gateway mode, apply the latest update from the support site.

We used the following sequence to update the firmware from 5.2.1b to 5.3.0.

1. Download the code and unzip the package to an FTP Server.
2. Open a browser and log on to the switch with its IP Address. The main window appears, as shown in Figure 3-23.

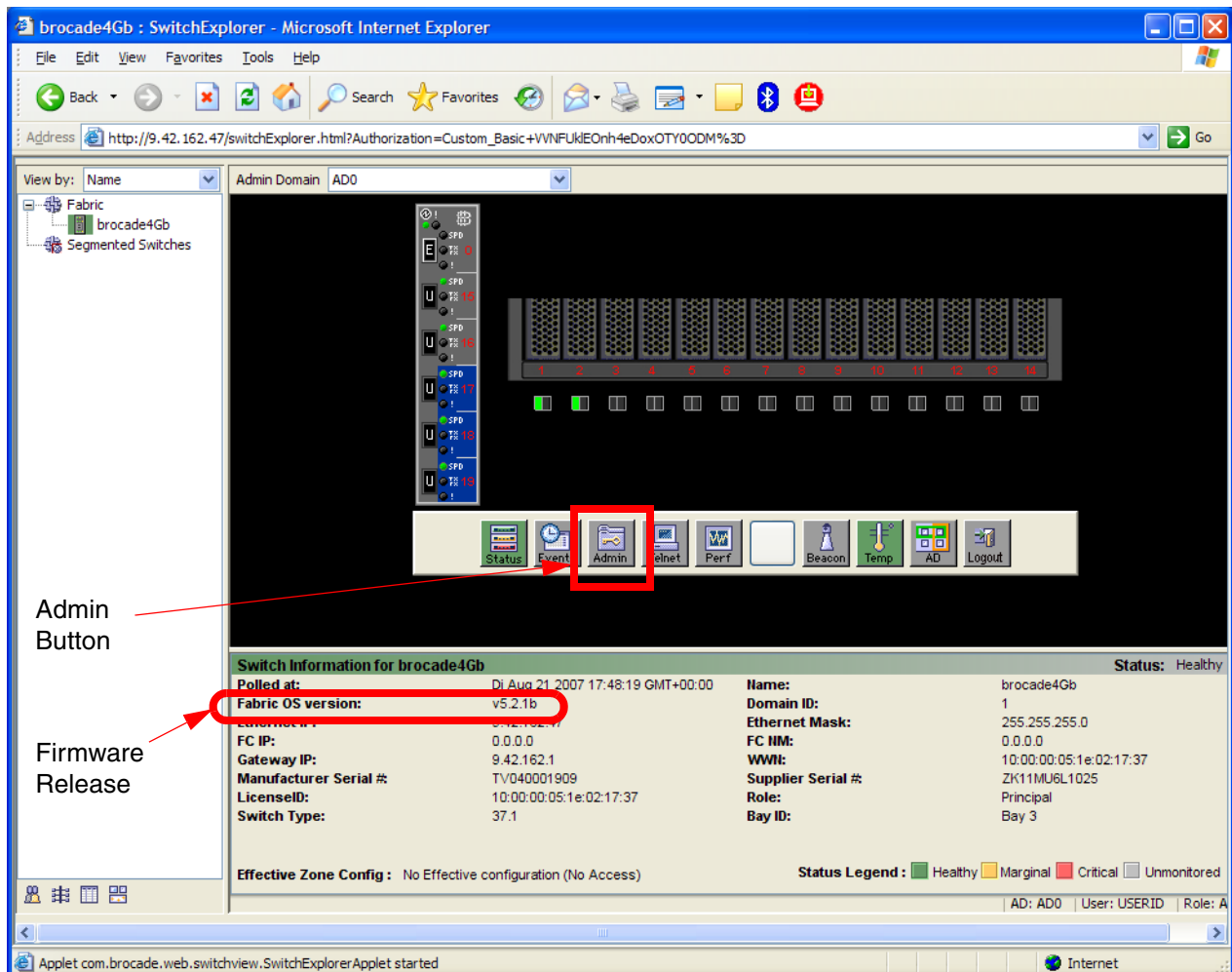


Figure 3-23 Firmware Release

3. Click the Admin button (as indicated in Figure 3-23) to access the Administrator menus as displayed in Figure 3-24 on page 46.

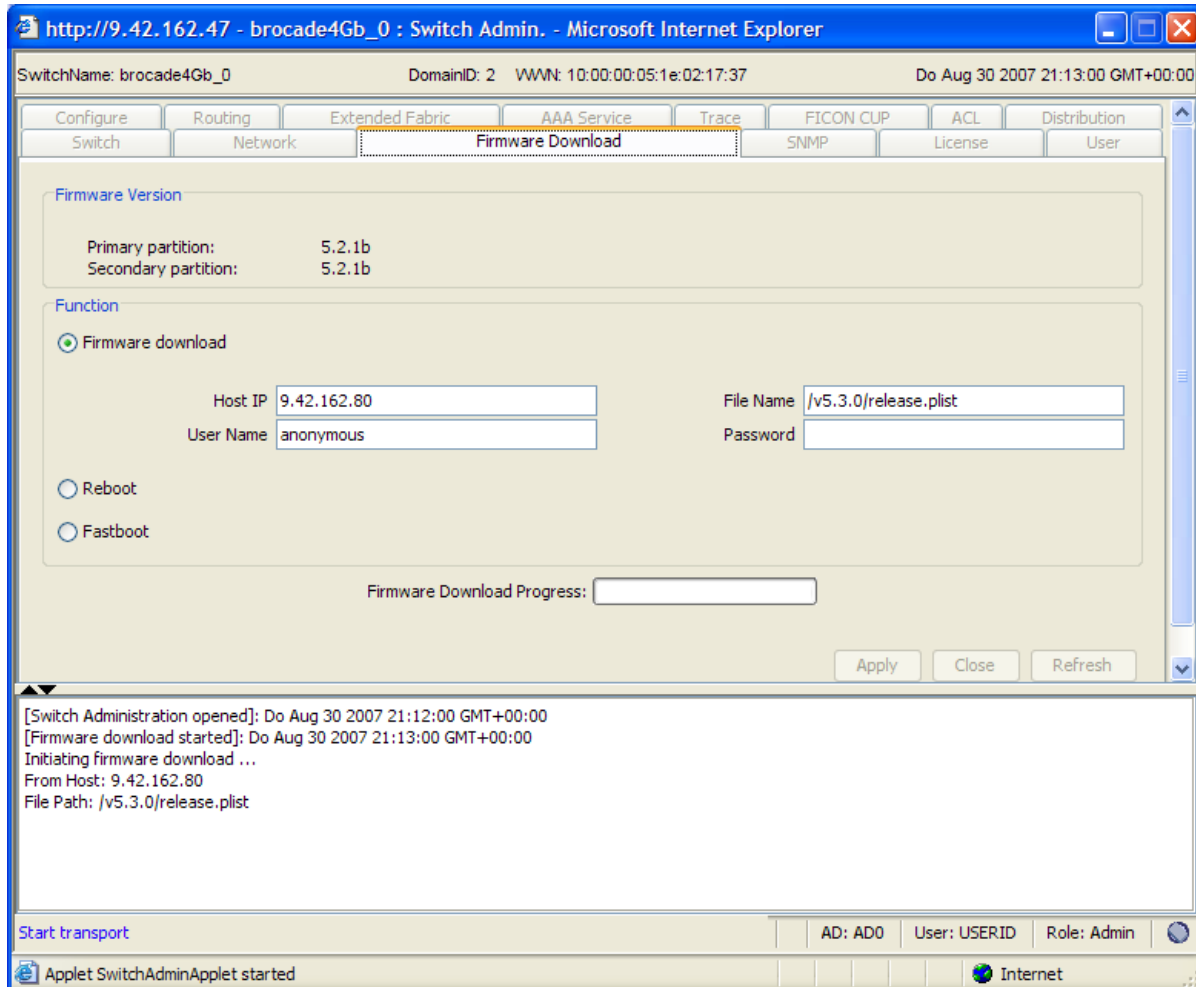


Figure 3-24 Firmware upload

4. Click **Firmware Download** tab as shown in Figure 3-24.
5. Enter IP Address of the FTP server where you have placed the firmware.
6. Enter the path and filename for the new firmware.
7. Enter Username and password for the FTP server.
8. Click **Apply** to begin the download.
9. The switch will download and install the code. The switch reboots when the installation is complete.

You can also use the command line Interface to update the Firmware:

1. Download the code and unzip the package to an FTP Server.
2. Telnet to the IP address of the switch and login with the userid and password.
3. At the prompt run the command:


```
firmwaredownload
```
4. You will be asked to continue; Enter **yes**.
5. Enter the values for the FTP server address, username, password.
6. Enter the path and filename for the new firmware.

7. The switch will download and install the code. The switch reboots when the installation is complete.

Figure 3-25 shows all of the steps and output of the update sequence with CLI.

```
brocade4Gb:USERID> firmwaredownload
Server Name or IP Address: 9.42.171.80
User Name: anonymous
File Name: /v5.3.0/release.plist
Network Protocol(1-auto-select, 2-FTP, 3-SCP) [1]: 2
Password:+++++
Checking system settings for firmwaredownload...
Protocol selected: FTP
Trying address-->AF_INET IP: 9.42.171.80, flags : 2
System settings check passed.

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

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

Do you want to continue [Y]: y
Firmware is being downloaded to the switch. This step may take up to 30 minutes.
Preparing for firmwaredownload...
Start to install packages...
dir #####
ldconfig #####
glibc #####

sysstat #####
ipv6 #####
Removing unneeded files, please wait ...
Finished removing unneeded files.

All packages have been downloaded successfully.
Firmware has been downloaded to the secondary partition of the switch.
HA Rebooting ...
```

Figure 3-25 Firmware upgrade with CLI

After the successful firmware upgrade you get the new Brocade Web Tools window shown in Figure 3-26 on page 48.

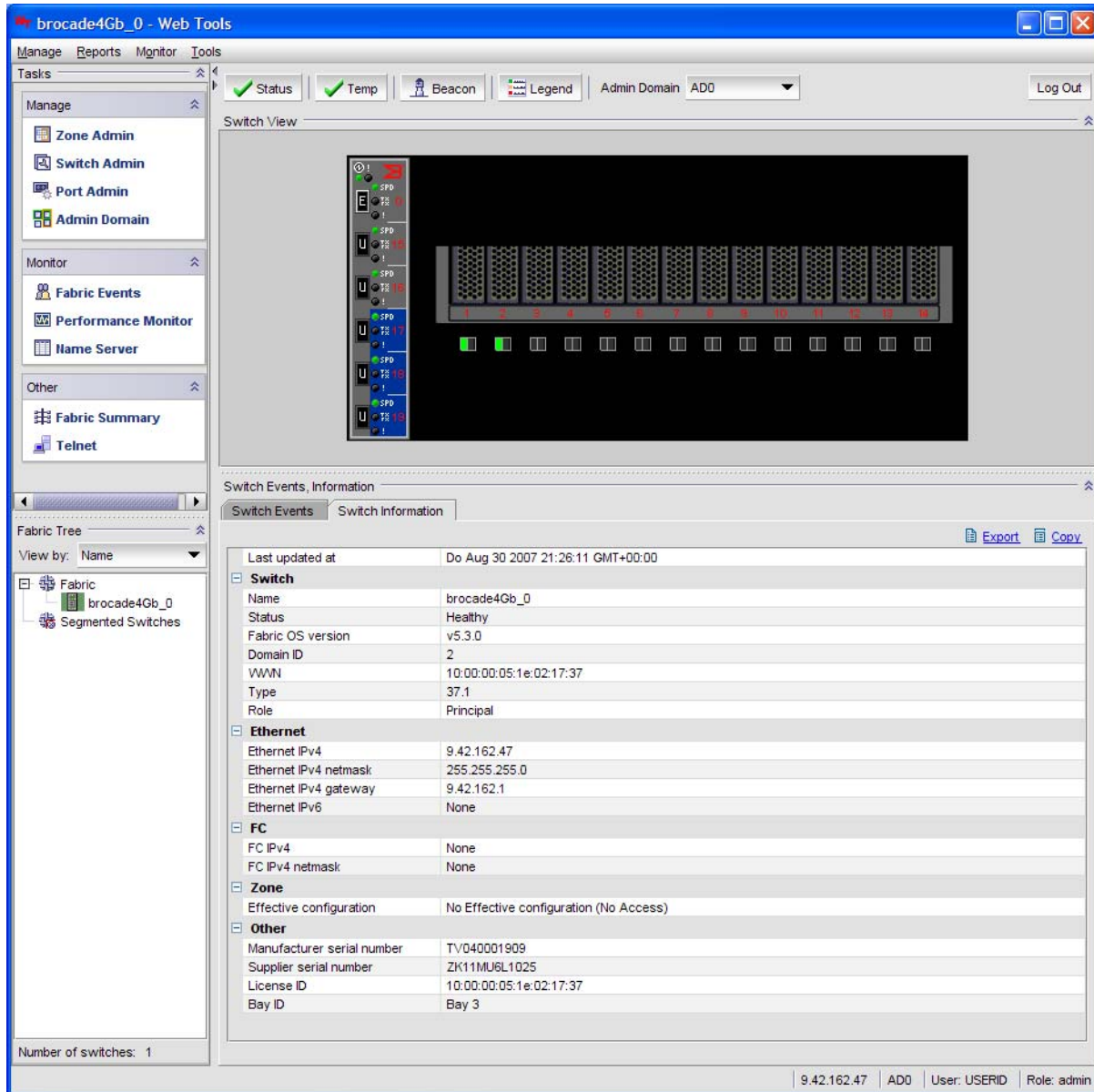


Figure 3-26 Web Tools 5.3

3.6 Converting to Access Gateway mode

You can change from the Fabric switch mode to the Access Gateway Mode using either of the following:

- ▶ Command Line Interface
- ▶ Brocade Web Tools

Once converted, the switch operates as a transparent device in the fabric.

3.6.1 Command line interface

Follow these steps:

1. Log on to the switch.
2. Use the **switchShow** command to display the current configuration, as shown in Figure 3-27. A value of Native as shown indicates the switch is in full fabric mode.

```
brocade4Gb:USERID> switchShow
switchName:   brocade4Gb
switchType:   37.1
switchState:  Online
switchMode:   Native
switchRole:   Principal
switchDomain: 1
switchId:     fffc01
switchWwn:    10:00:00:05:1e:02:80:81
zoning:       OFF
switchBeacon: OFF
...
```

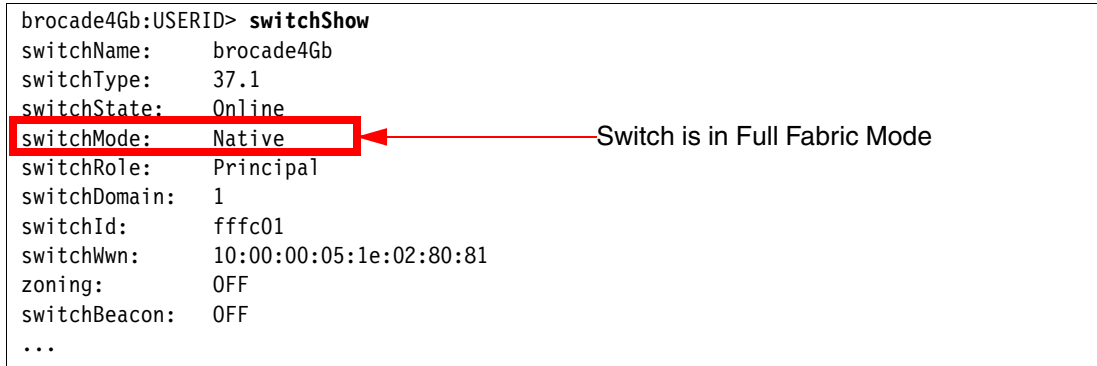


Figure 3-27 switchShow

3. Enter **switchDisable** to disable the switch.

Note: You should save the switch configuration using the **configUpload** command before proceeding with step 4.

4. Use the command **ag --modeEnable** to enable Access Gateway mode as shown in Figure 3-28. The device will be rebooted after the command completes.

```
brocade4Gb:USERID> ag --modeenable
WARNING: Enabling agmode will remove all the configuration data on the switch
including zoning configuration and security database. Please backup your
configuration using configupload.
This operation will reboot the switch.
Do you want to continue? (yes, y, no, n): [no] y
```

Figure 3-28 Enable Access Gateway Mode

At this point, the device will be in Access Gateway Mode with the default port mapping shown in Table 2-8 on page 23. This can be verified by issuing the **ag --modeShow** command as shown in Figure 3-29.

```
brocade4Gb:USERID> ag --modeshow
Access Gateway mode is enabled.
```

Figure 3-29 ag --modeshow

Access Gateway mode can also be verified using the **switchShow** command as shown in Figure 3-30 on page 50.

```
brocade4Gb:USERID> switchshow
switchName:    brocade4Gb
switchType:    37.1
switchState:   Online
switchMode:    Access Gateway Mode
switchWwn:     10:00:00:05:1e:02:80:81
switchBeacon:  OFF
...
```

Figure 3-30 switchshow

3.6.2 Brocade Web Tools

Follow these steps to activate Access Gateway mode using the GUI tools.

1. Connect through a browser to the IP address of the Brocade switch module. After authentication you will get the Switch view window (Figure 3-31 on page 51).

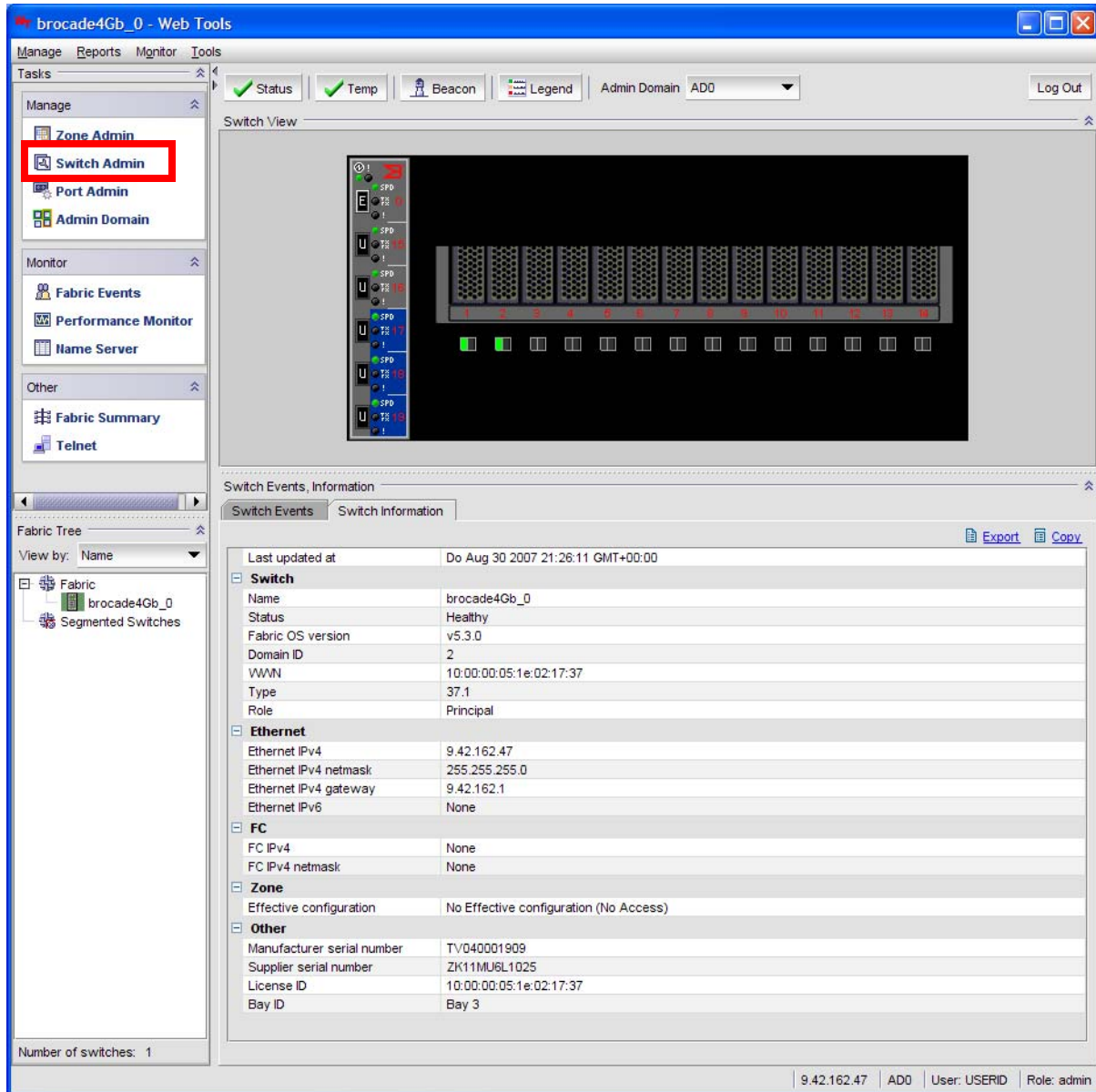


Figure 3-31 initial window

2. Click **Switch Admin** in the left upper corner of the window (see Figure 3-31).

3. Save current configuration as per Figure 3-32. Go to the **Configure** → **Upload/Download** subtab for saving and proceed with the next step.

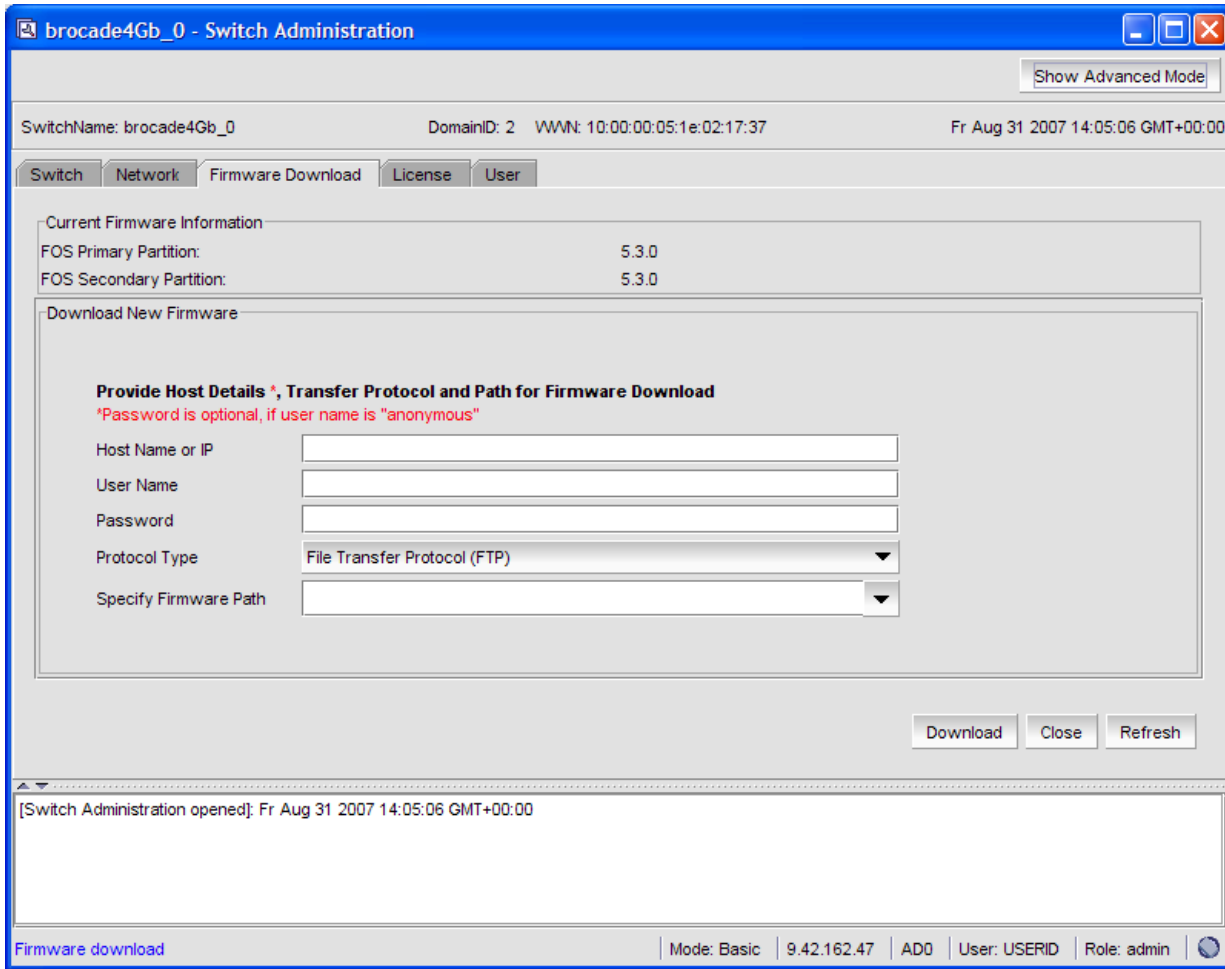


Figure 3-32 Save config

4. In the Switch Status portion of Figure 3-33 on page 53, click **Disable** to disable switch mode.
You must disable the switch before enabling Access Gateway Mode. If you do not, you will get an error message reminding you of this fact.

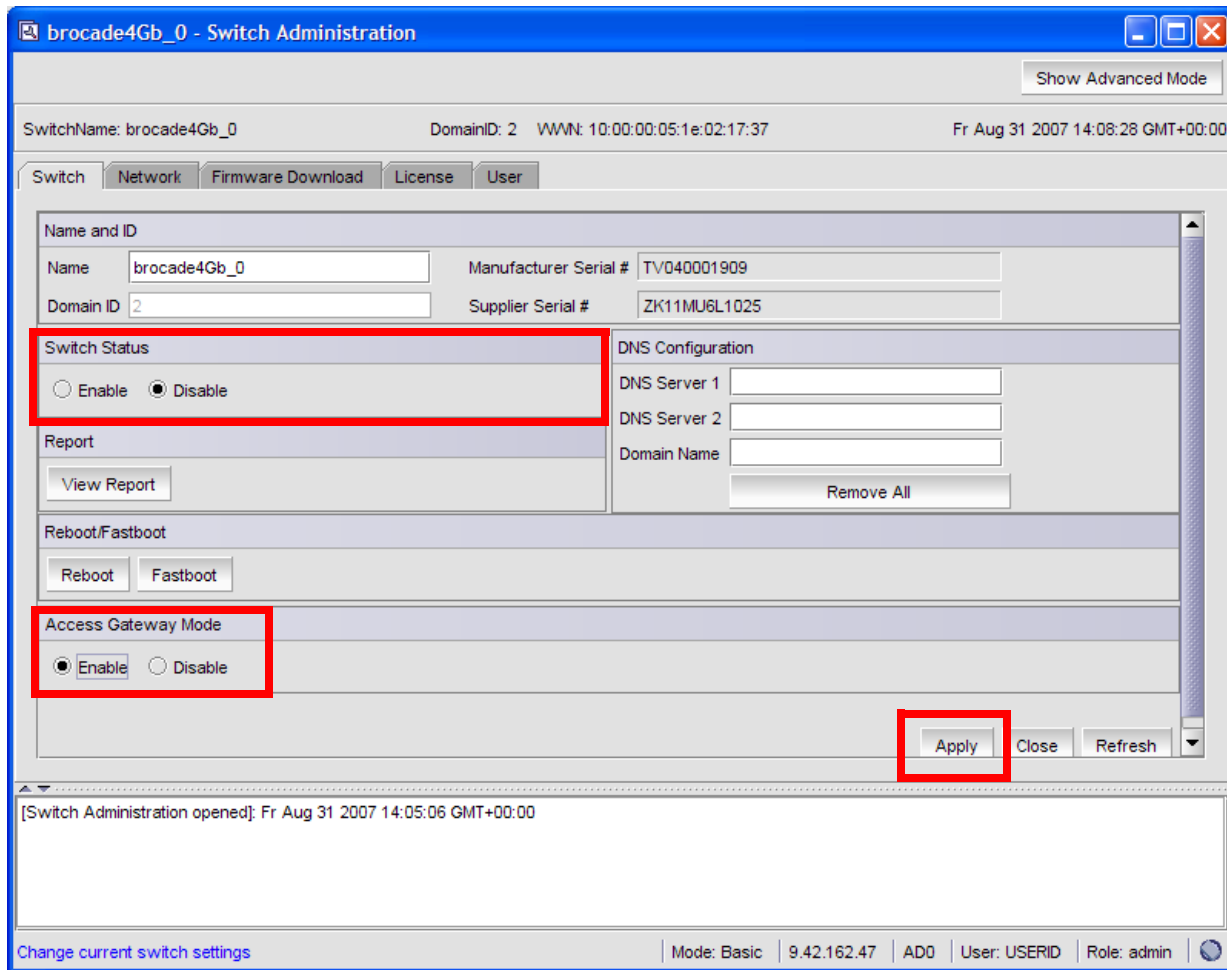


Figure 3-33 Enable Access Gateway mode

5. In the Access Gateway Mode section, click **Enable**.
6. After clicking **Apply** and **Yes** the switch proceeds with the change. After the switch reboots, it will restart in Access Gateway mode.

Note that in Access Gateway Mode, the fabric management features are grayed out and there are only few switch menus available. Compare Figure 3-34 on page 54 (Access Gateway mode) with Figure 3-31 on page 51 (Switch mode).

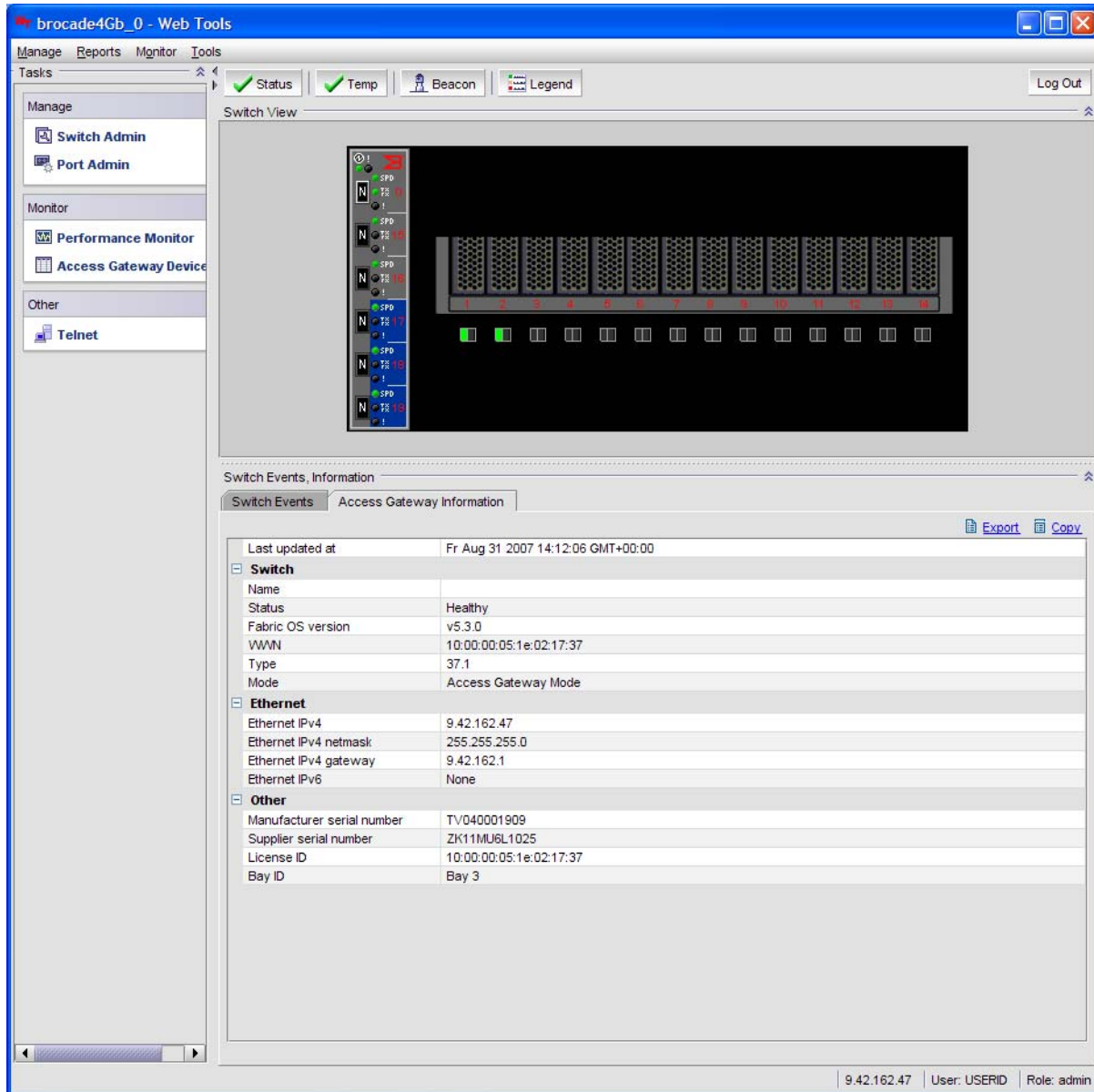


Figure 3-34 Access Gateway Mode

3.7 Connecting to the fabric

The commands below describe how you can check the installation. The World-Wide Names (WWNs) of the host bus adapters (HBAs) are recognized by the edge switches and can be used for further configuration (for example, zoning).

In our labs, we used the following WWNs:

LS20:

- ▶ 21:00:00:e0:8b:9d:a8:d7
- ▶ 21:01:00:c0:8b:bd:a8:d7

HS20:

- ▶ 21:00:00:11:25:93:af:4a
- ▶ 21:00:00:11:25:93:af:4b

3.7.1 Cisco MDS

In Cisco environments, the CLI is almost always used. However you can also use the Device Manager through a browser for displaying information and settings.

The **show tech support** command collects a large amount of information about the switch configuration which is helpful in case of troubleshooting.

The following examples show the output of the subcommands which are useful for getting information about our configuration.

The **show interface brief** command displays a quick overview of all configured Interfaces. We used fc1/1 and fc1/2 and can see that both are up as per Figure 3-35.

```
~show interface brief ~
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/1	100	auto	on	up	sw1	F	2	--
fc1/2	100	auto	on	up	sw1	F	2	--
fc1/3	100	auto	on	sfpAbsent	--	--	--	--
fc1/4	100	auto	on	sfpAbsent	--	--	--	--
fc1/5	100	auto	on	notConnected	sw1	--	--	--
fc1/6	100	auto	on	sfpAbsent	--	--	--	--
fc1/7	100	auto	on	sfpAbsent	--	--	--	--
fc1/8	100	auto	on	sfpAbsent	--	--	--	--
fc1/9	100	auto	on	notConnected	sw1	--	--	--
fc1/10	100	auto	on	notConnected	sw1	--	--	--
fc1/11	100	auto	on	sfpAbsent	--	--	--	--
fc1/12	100	auto	on	sfpAbsent	--	--	--	--
fc1/13	100	auto	on	notConnected	sw1	--	--	--
fc1/14	100	auto	on	sfpAbsent	--	--	--	--
fc1/15	100	auto	on	sfpAbsent	--	--	--	--
fc1/16	100	auto	on	sfpAbsent	--	--	--	--

Figure 3-35 show interface brief

The **show flogi** command displays all devices that have successfully logged in to the fabric as per Figure 3-36 on page 56.

```

~show flogi database vsan 100 ~
-----
INTERFACE  VSAN   FCID          PORT NAME          NODE NAME
-----
fc1/1      100    0x610002     20:00:00:05:1e:02:17:37  10:00:00:05:1e:02:17:37
fc1/1      100    0x610700     21:00:00:11:25:93:af:4a  20:00:00:11:25:93:af:4a
fc1/1      100    0x610800     21:00:00:e0:8b:9d:a8:d7  20:00:00:e0:8b:9d:a8:d7
fc1/2      100    0x610001     20:00:00:05:1e:02:80:81  10:00:00:05:1e:02:80:81
fc1/2      100    0x610500     21:00:00:11:25:93:af:4b  20:00:00:11:25:93:af:4b
fc1/2      100    0x610600     21:01:00:e0:8b:bd:a8:d7  20:01:00:e0:8b:bd:a8:d7
Total number of flogi = 6.

```

Figure 3-36 show flogi database vsan 100

The **show fcns** command shows the name server database which stores the name entries for all hosts in the Fibre Channel switch as per Figure 3-37.

```

~show fcns database vsan 100~
-----
VSAN 100:
-----
FCID          TYPE  PWWN          (VENDOR)          FC4-TYPE:FEATURE
-----
0x610001     N     20:00:00:05:1e:02:80:81
0x610002     N     20:00:00:05:1e:02:17:37
0x610500     N     21:00:00:11:25:93:af:4b
0x610600     N     21:01:00:e0:8b:bd:a8:d7 (Qlogic)
0x610700     N     21:00:00:11:25:93:af:4a
0x610800     N     21:00:00:e0:8b:9d:a8:d7 (Qlogic)
Total number of entries = 6

```

Figure 3-37 show fcns database vsan 100

If Cisco Device Manager is used, clicking **FC** → **Name Server** shows the Name Server Table of the switch as per Figure 3-38.

VSAN Id, ...	Type	PortName	NodeName	Fc...	FabricPortName
100, 0x610001	N	Brocade 20:00:00:05:1e:02:80:81	Brocade 10:00:00:05:1e:02:80:81		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610002	N	Brocade 20:00:00:05:1e:02:17:37	Brocade 10:00:00:05:1e:02:17:37		Cisco 20:01:00:0d:ec:01:ac:c0
100, 0x610500	N	IBM 21:00:00:11:25:93:af:4b	IBM 20:00:00:11:25:93:af:4b		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610600	N	Qlogic 21:01:00:e0:8b:bd:a8:d7	Qlogic 20:01:00:e0:8b:bd:a8:d7		Cisco 20:02:00:0d:ec:01:ac:c0
100, 0x610700	N	IBM 21:00:00:11:25:93:af:4a	IBM 20:00:00:11:25:93:af:4a		Cisco 20:01:00:0d:ec:01:ac:c0
100, 0x610800	N	Qlogic 21:00:00:e0:8b:9d:a8:d7	Qlogic 20:00:00:e0:8b:9d:a8:d7		Cisco 20:01:00:0d:ec:01:ac:c0

Figure 3-38 Name Server Table

3.7.2 Brocade

The **switchshow** command on the fabric switch displays the NPIV links logged into the fabric as shown in Figure 3-39 on page 57.

```

swd77:admin> switchshow
switchName:    swd77
switchType:    46.2
switchState:   Online
switchMode:    Native
switchRole:    Principal
switchDomain:  1
switchId:      fffc01
switchWwn:     10:00:00:05:1e:38:9d:e9
zoning:        ON (Test1)
switchBeacon:  OFF
FC Router:     OFF
FC Router BB Fabric ID: 1

Area Port Media Speed State      Proto
=====
  0  0  id  N4  Online      F-Port  4 NPIV public
  1  1  id  N4  Online      F-Port  4 NPIV public
  2  2  id  N4  Online      F-Port  3 NPIV public
  3  3  id  N4  Online      F-Port  3 NPIV public
  4  4  id  2G  Online      F-Port 20:24:00:a0:b8:26:1c:30
  5  5  id  2G  Online      F-Port 20:14:00:a0:b8:26:1c:30
  6  6  id  N4  No_Light
  7  7  id  N4  No_Light

```

Ports 2 and 3 are used in our test environment

Figure 3-39 Output of the switchshow command

You can also use the **portshow** command to get more information about the ports as shown in Figure 3-40 (port 2) and Figure 3-41 on page 58 (port 3).

```

swd77:admin> portshow 2
portName:
portHealth: No Fabric Watch License

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x24b03      PRESENT ACTIVE F_PORT G_PORT U_PORT NPIV LOGICAL_ONLINE
  LOGIN NOELP LED ACCEPT
portType: 10.0
portState: 1 Online
portPhys: 6 In_Sync
portScn: 32 F_Port
port generation number: 44
portId: 010200
portIfId: 4302080d
portWwn: 20:02:00:05:1e:38:9d:e9
portWwn of device(s) connected:
  21:00:00:e0:8b:9d:a8:d7
  21:00:00:11:25:93:af:4a
  20:00:00:05:1e:02:17:37
Distance: normal
portSpeed: N4Gbps

```

LS21
 HS21
 Access Gateway node

Figure 3-40 The portshow command displaying data about device port 2

```

swd77:admin> portshow 3
portName:
portHealth: No Fabric Watch License

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x24b03      PRESENT ACTIVE F_PORT G_PORT U_PORT NPIV LOGICAL_ONLINE
  LOGIN NOELP LED ACCEPT
portType: 10.0
portState: 1   Online
portPhys: 6   In_Sync
portScn: 32   F_Port
port generation number: 46
portId: 010300
portIfId: 4302080c
portWwn: 20:03:00:05:1e:38:9d:e9
portWwn of device(s) connected:
  21:00:00:11:25:93:af:4b
  21:01:00:e0:8b:bd:a8:d7
  20:00:00:05:1e:02:80:81
Distance: normal
portSpeed: N4Gbps

```

Figure 3-41 The portshow command displaying data about device port 3

The nsshow command can also show the connected virtual WWNs as shown in Figure 3-42.

```

swd77:admin> nsshow
{
  Type Pid   COS   PortName                                     NodeName                                     TTL(sec)
  N   010201;  3;21:00:00:11:25:93:af:4a;20:00:00:11:25:93:af:4a; na
    Fabric Port Name: 20:02:00:05:1e:38:9d:e9
    Permanent Port Name: 21:00:00:11:25:93:af:4a
    Port Index: 2
    Share Area: No
    Device Shared in Other AD: No
  N   010202;  3;21:00:00:e0:8b:9d:a8:d7;20:00:00:e0:8b:9d:a8:d7; na
    Fabric Port Name: 20:02:00:05:1e:38:9d:e9
    Permanent Port Name: 21:00:00:e0:8b:9d:a8:d7
    Port Index: 2
    Share Area: No
    Device Shared in Other AD: No
  N   010301;  3;21:01:00:e0:8b:bd:a8:d7;20:01:00:e0:8b:bd:a8:d7; na
    Fabric Port Name: 20:03:00:05:1e:38:9d:e9
    Permanent Port Name: 21:01:00:e0:8b:bd:a8:d7
    Port Index: 3
    Share Area: No
    Device Shared in Other AD: No
  N   010302;  3;21:00:00:11:25:93:af:4b;20:00:00:11:25:93:af:4b; na
    Fabric Port Name: 20:03:00:05:1e:38:9d:e9
    Permanent Port Name: 21:00:00:11:25:93:af:4b
    Port Index: 3
    Share Area: No
    Device Shared in Other AD: No
  The Local Name Server has 18 entries }

```

Figure 3-42 The nsshow command

The Brocade Web Tools application also shows the connected ports as shown in Figure 3-43.

Name Server

Auto Refresh Auto-Refresh Interval: 15 seconds Number of Devices: 17

All Devices

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	FDMI Host
1	0	010001	N	21:01:00:1b:32:38:1a:0b	20:01:00:1b:32:38:1a:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	
1	15	010f00	N	20:25:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTt 0916	
1	0	010002	N	21:01:00:1b:32:37:40:de	20:01:00:1b:32:37:40:de	QMI3472 FW:v4.00.23 DVR:v9.1.2.19 (w...	
1	0	010003	N	21:01:00:1b:32:38:15:0b	20:01:00:1b:32:38:15:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	
1	2	010200	N	20:00:00:05:1e:02:80:81	10:00:00:05:1e:02:80:81		
1	3	010302	N	21:00:00:e0:8b:9d:a8:d7	20:00:00:e0:8b:9d:a8:d7		
1	4	010400	N	20:24:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTt 0916	
1	2	010202	N	21:01:00:e0:8b:bd:a8:d7	20:01:00:e0:8b:bd:a8:d7		
1	1	010103	N	21:00:00:1b:32:18:15:0b	20:00:00:1b:32:18:15:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	
1	5	010500	N	20:14:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTt 0916	
1	3	010301	N	21:00:00:11:25:93:af:4a	20:00:00:11:25:93:af:4a		
1	2	010201	N	21:00:00:11:25:93:af:4b	20:00:00:11:25:93:af:4b		
1	3	010300	N	20:00:00:05:1e:02:17:37	10:00:00:05:1e:02:17:37		
1	14	010e00	N	20:15:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTt 0916	
1	1	010100	N	20:00:00:c0:dd:0d:35:8f	10:00:00:c0:dd:0d:35:8f		
1	0	010000	N	20:00:00:c0:dd:0d:35:a3	10:00:00:c0:dd:0d:35:a3		
1	1	010102	N	21:00:00:1b:32:17:40:de	20:00:00:1b:32:17:40:de	QMI3472 FW:v4.00.23 DVR:v9.1.2.19 (w...	

Detail View Accessible Devices Refresh Print Close

Refreshing Name Server Information... done AD: AD0 User: admin Role: Admin

Applet com.brocade.web.zoning.NameServerApplet_SS started Internet

Figure 3-43 Name Server

3.7.3 McDATA

In a McDATA environment, viewing the Name Server table can be done through the EFCM GUI as shown in Figure 3-44.

EFCM™ Basic Edition

Model Name: Intrepid 6140
Switch Name: McData Core_ID5 (.57)
IP Address: 9.42.164.57
Domain ID: 1

Login: Administrator Logout
Status: Minor Failure
State: Online

Fabric Product Configure Security Logs Maintenance Upgrade Help Last Updated 8/27/07 [16:04:00] Refresh

Product > Node List

Port	FC Address	Node Type	Port WWN	Node WWN	COS	BB Credit	Rx Field Size
0	610413	N_Port	200000051E021737	100000051E021737	Class 3	8	2112
0	610414	N_Port	210000112593AF4A	200000112593AF4A	Class 3	3	2048
0	610415	N_Port	210000E08B9DA8D7	200000E08B9DA8D7	Class 3	3	2048
1	610513	N_Port	200000051E028081	100000051E028081	Class 3	8	2112
1	610514	N_Port	210000112593AF4B	200000112593AF4B	Class 3	3	2048
1	610515	N_Port	210100E08BBD8A87	200100E08BBD8A87	Class 3	3	2048

Figure 3-44 Name Server table

You can also use the **show nameserver** command in the CLI as shown in Figure 3-45.

DID	Type	PortId	Port Name	Node Name	COS	FC4	
1	N	610413	20:00:00:05:1E:02:17:37	10:00:00:05:1E:02:17:37	3	N/A	← Node name of the Access Gateway
1	N	610414	21:00:00:11:25:93:AF:4A	20:00:00:11:25:93:AF:4A	3	N/A	← HS21
1	N	610415	21:00:00:E0:8B:9D:A8:D7	20:00:00:E0:8B:9D:A8:D7	3	N/A	← HS21
1	N	610513	20:00:00:05:1E:02:80:81	10:00:00:05:1E:02:80:81	3	N/A	← Node name of the Access Gateway
1	N	610514	21:00:00:11:25:93:AF:4B	20:00:00:11:25:93:AF:4B	3	N/A	← HS21
1	N	610515	21:01:00:E0:8B:BD:A8:D7	20:01:00:E0:8B:BD:A8:D7	3	N/A	← LS21

FC4 types decode information can be viewed via the ShownameserverFC4types CLI command

Figure 3-45 Output of the show nameserver command

3.7.4 Storage attachment

In this section we describe how the Access Gateway can be used in a clustering environment. We are using the IBM System Storage™ DS4300 as the basis of our SAN.

In this lab we set up an environment which consists of:

- ▶ A BladeCenter E chassis
- ▶ Three BladeCenter HS21 servers
- ▶ Two Brocade 4 Gb Fiber Switch Module in Access Gateway mode
- ▶ One IBM System Storage DS4300
- ▶ One IBM 2005-H16 External SAN Switch
- ▶ Windows Server® 2003 Standard Edition and Enterprise Edition

We were able to successfully implement an MSCS cluster using the Access Gateway and the redundant paths we configured, meaning the data continued to be available even after a path failure.

We do not describe how to set up MSCS in this paper. Instead, refer to the following link for details:

<http://www.microsoft.com/windowsserver2003/enterprise/clustering.mspx>

To set up the configuration, do the following:

1. Define the zoning of each blade server that you intend to have in the MSCS environment. Figure 3-46 on page 61 shows the initial zoning stage.

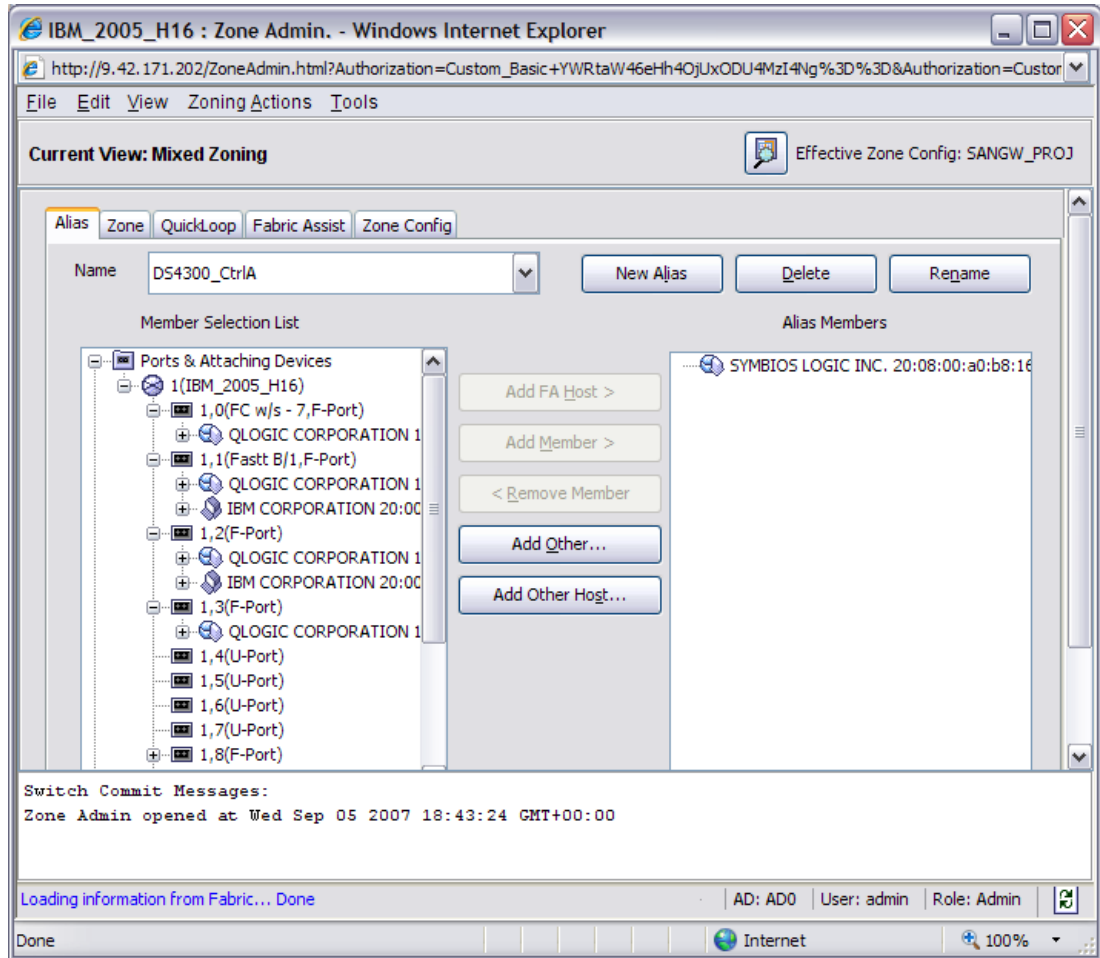


Figure 3-46 Initial stage setup on defining the alias name

2. Once you have created the alias name based on the WWN, you may proceed to define the zoning of each alias that you had created earlier. This is shown in Figure 3-47 on page 62.

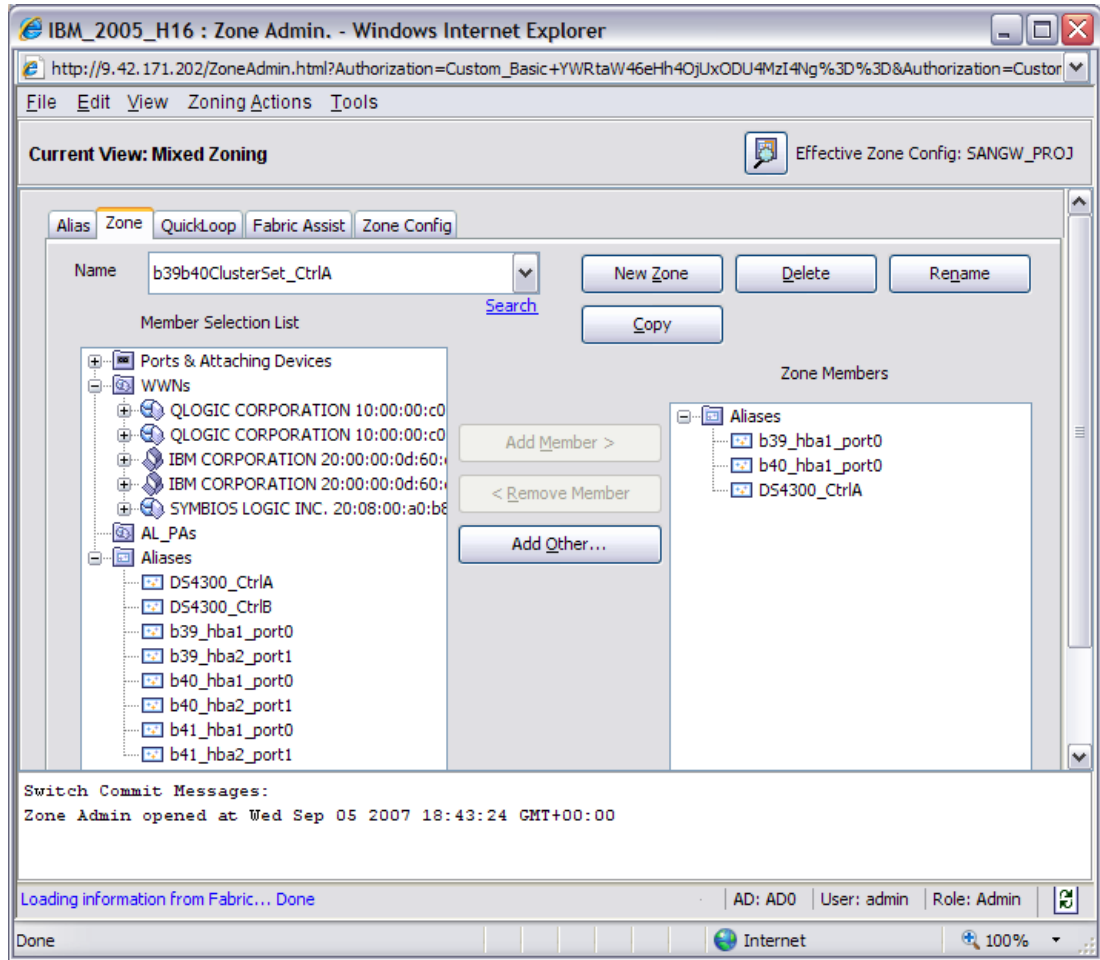


Figure 3-47 Define a Zone

3. Save the configuration that you have made in the SAN switch to activate the configuration as shown in Figure 3-48.

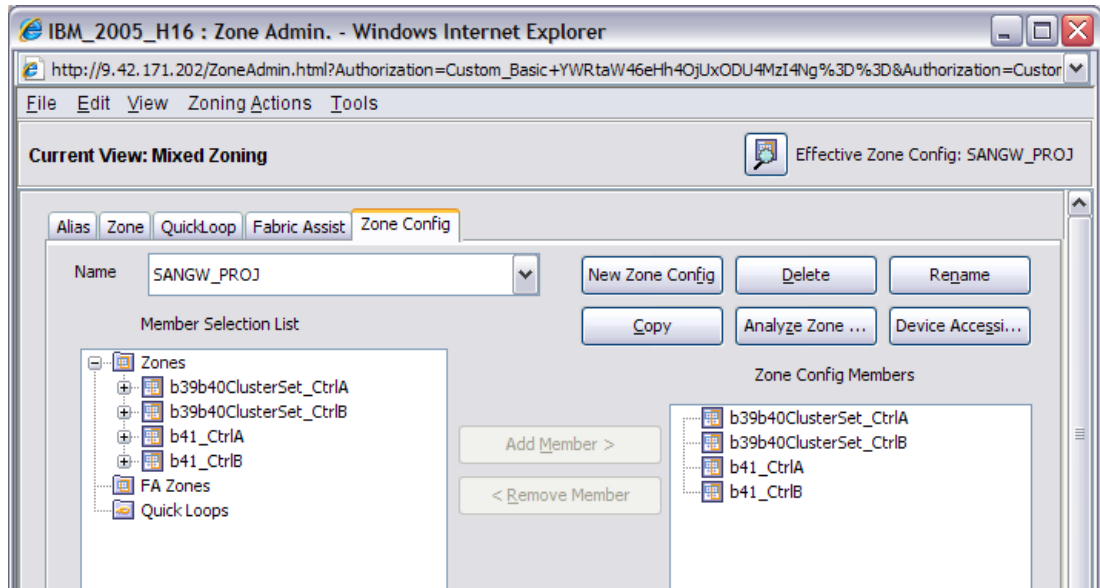


Figure 3-48 Complete the zoning configuration

4. After you have completed the HBA assigning and zoning, proceed to define the storage partition based on your current needs and environment.
In our lab example, we assigned 68 GB disk array with RAID 1 (for quorum) and 137 GB disk array with RAID 5 (for data). This is shown in Figure 3-49.

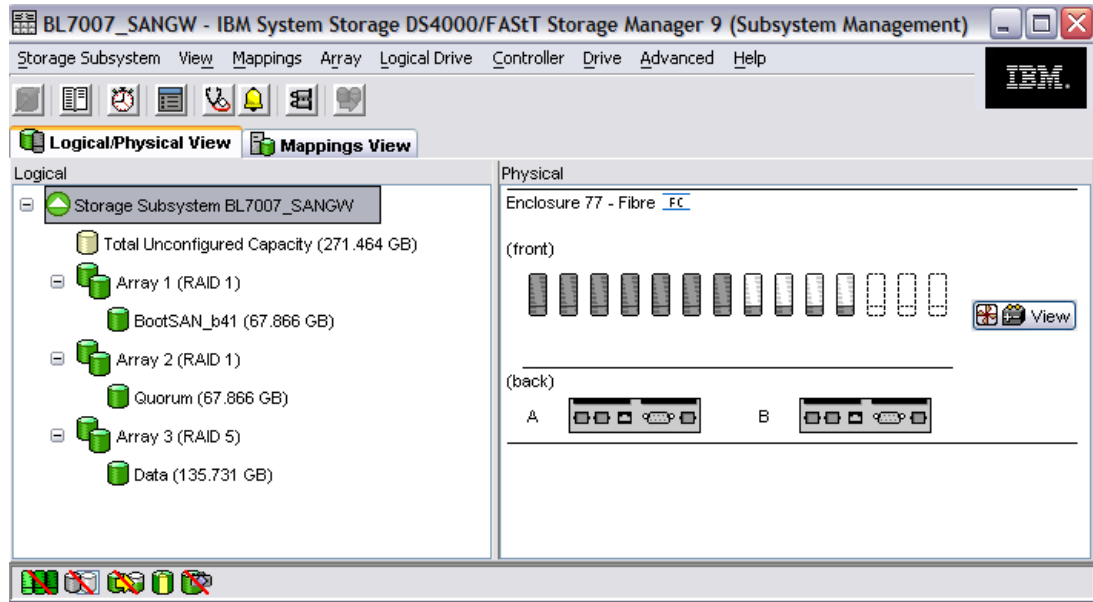


Figure 3-49 Storage Partition Assigning

5. During the synchronizing of the array, proceed with the disk mapping for your server to identify the new partitions on the operating systems. See Figure 3-50 on page 64.

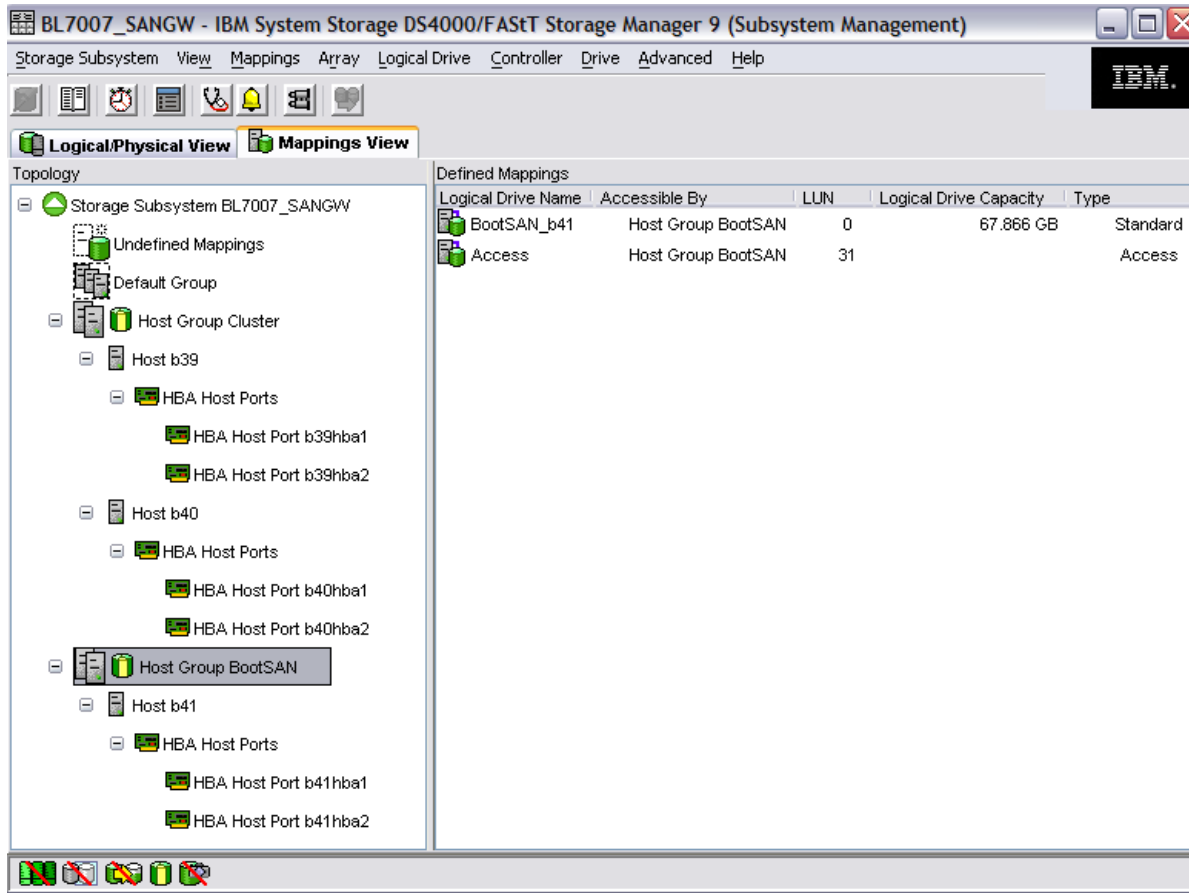


Figure 3-50 Storage Mapping

- Now you have completed the storage assigning for the blade server. Now you may proceed with setting up MSCS. We don't cover this in the paper.

Note: During the disk mapping, ensure the host type is defined to Windows as clustered in order to support the MSCS settings.

Now you have completed the initial setup of blade server, SAN storage, SAN switch, and operating systems. You may proceed with the test cases that we initiate in this test lab. Since Access Gateway works similar to the SAN Switch Module, setting up the MSCS is straight forward.

In order to test the port redundancy we disable port 0 whereby the settings of port 0 are "PrimaryTFport" and port 15 are "BackupTFport". Initiating the disable port can be done through GUI or CLI; the result is still the same. In this example we use the GUI to have a clearer picture of the failover initiating automatically without any interruption at the cluster server sets as shown in Figure 3-51 on page 65 for the Access Gateway and the MSCS result in Figure 3-52 on page 65.

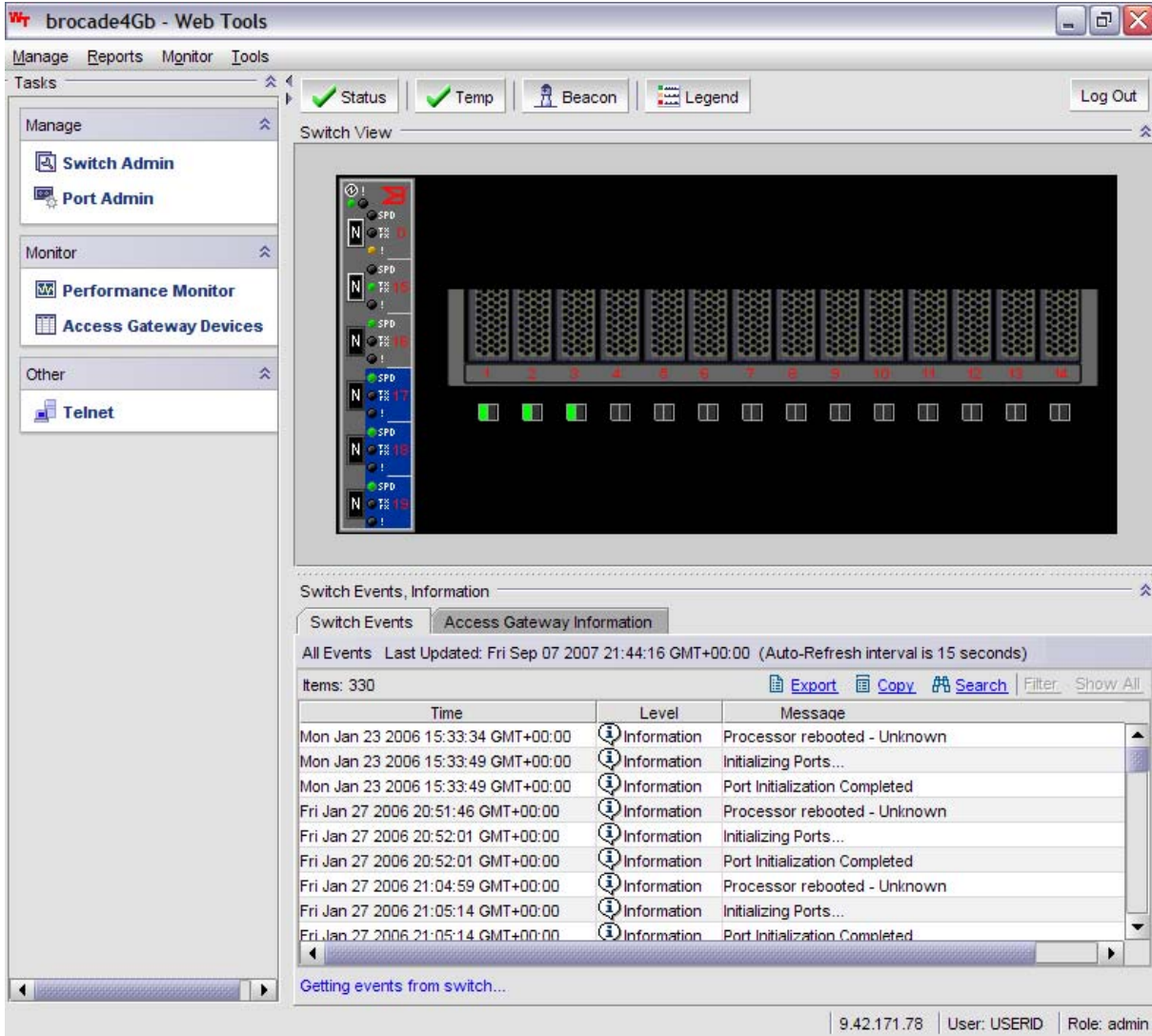


Figure 3-51 Indicate actual result port failover between port 0 and port 15

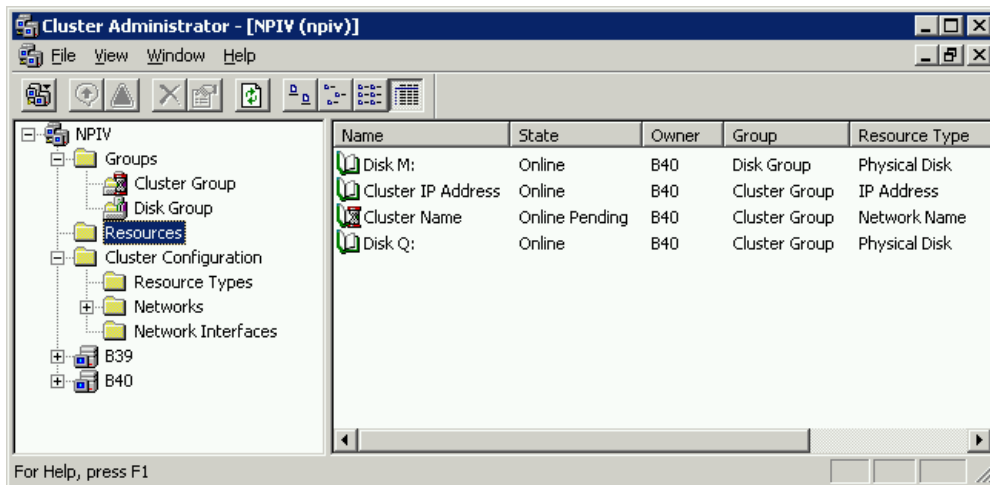


Figure 3-52 MSCS Failover

Either you disable the port on the Access Gateway or totally power off the Access Gateway; the result will still remain the same for the clustered environment, where users are still able to access the data or continue working without having any interruptions. The results are shown in Figure 3-53.

I/O Module Power/Restart ?

Select one or more module(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

<input type="checkbox"/>	Bay	Type	MAC Address	IP Address	Pwr	POST Status
<input type="checkbox"/>	1	Ethernet SM	00:05:5D:89:81:B4	192.168.70.127	On	POST results available: FF: Module completed POST s
<input type="checkbox"/>	2	Ethernet SM	00:05:5D:71:82:04	192.168.70.128	On	POST results available: FF: Module completed POST s
<input type="checkbox"/>	3	Fibre SM	00:05:1E:35:AC:59	9.42.171.78	Off	POST results not complete: 00
<input type="checkbox"/>	4	Fibre SM	00:05:1E:35:AC:7B	9.42.171.79	On	POST results available: FF: Module completed POST s

Figure 3-53 Indicate actual result Power Off the Access Gateway in Bay 3

3.8 Command reference

This section lists commands that are useful to SAN administrators.

3.8.1 Switch commands

Commands for the Brocade 4 Gb SAN Switch Module:

switchshow

The `switchshow` command displays switch properties, such as WWNs, switch mode.

Example 3-1 The switchshow command

```
brocade4Gb:USERID> switchshow
switchName:    brocade4Gb
switchType:    37.1
switchState:   Online
switchMode:    Access Gateway Mode
switchWwn:     10:00:00:05:1e:02:80:81
switchBeacon:  OFF
```

Area	Port	Media	Speed	State	Proto
0	0	id	N4	Online	N-Port 10:00:00:05:1e:38:9d:e9 0x010200
1	1	cu	2G	Online	F-Port 21:01:00:e0:8b:bd:a8:d7 0x010202
2	2	cu	2G	Online	F-Port 21:00:00:11:25:93:af:4b 0x010201
3	3	cu	AN	No_Sync	
4	4	cu	AN	No_Sync	
5	5	cu	AN	No_Sync	
6	6	cu	AN	No_Sync	
7	7	cu	AN	No_Sync	
8	8	cu	AN	No_Sync	
9	9	cu	AN	No_Sync	
10	10	cu	AN	No_Sync	
11	11	cu	AN	No_Sync	
12	12	cu	AN	No_Sync	

```

13 13  cu  AN  No_Sync
14 14  cu  AN  No_Sync
15 15  --  N4  No_Module
16 16  --  N4  No_Module
17 17  --  N4  No_Module
18 18  --  N4  No_Module
19 19  --  N4  No_Module

```

portshow

The **portshow** command displays properties about the specified port.

Syntax: **portshow <Portnumber>**

Example 3-2 The portshow command

```

brocade4Gb:USERID> portshow 0
portName: Ext0
portHealth: No Fabric Watch License

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x24b03      PRESENT ACTIVE F_PORT G_PORT LOGICAL_ONLINE LOGIN NOEL
LED ACCEPT
portType: 11.0
POD Port: Port is licensed
portState: 1  Online
portPhys: 6  In_Sync
portScn: 1  Online
port generation number: 0
portId: 010200
portIfId: 43020012
portWwn: 20:00:00:05:1e:02:80:81
portWwn of device(s) connected:
      20:02:00:05:1e:38:9d:e9
Distance: normal
portSpeed: N4Gbps

LE domain: 0
Interrupts:      6      Link_failure: 0      Frjt:      0
Unknown:        0      Loss_of_sync: 1      Fbsy:      0
Lli:            6      Loss_of_sig: 2
Proc_rqrd:     2672    Protocol_err: 0
Timed_out:      0      Invalid_word: 0
Rx_flushed:     0      Invalid_crc: 0
Tx_unavail:     0      Delim_err: 0
Free_buffer:    0      Address_err: 0
Overrun:        0      Lr_in:      1
Suspended:      0      Lr_out:     0
Parity_err:     0      Ols_in:     0
2_parity_err:  0      Ols_out:    1
CMI_bus_err:    0

Port part of other ADs: No
brocade4Gb:USERID>

```

portcfgshow

The portcfgshow command displays port configuration information (speed, NPIV status, and so on).

Example 3-3 The portcfgshow command

```
brocade4Gb:USERID> portcfgshow
Ports of Slot 0  0  1  2  3   4  5  6  7   8  9 10 11   12 13 14 15
-----+---+---+---+-----+---+---+---+-----+---+---+---+-----+---+---+---+-----
Speed           AN 2G 2G AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Locked N_Port   ON .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ON
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

Ports of Slot 0  16 17 18 19
-----+---+---+---+-----
Speed           AN AN AN AN
Locked N_Port   ON ON ON ON
Persistent Disable.. .. .. ..
NPIV capability ON ON ON ON
```

where AN:AutoNegotiate, ..:OFF, ?:INVALID,
SN:Software controlled AutoNegotiation.

portcfgnport

Syntax: **portcfgnport <Slot>/<Port> LockRequest**

where LockRequest is 0 for unlock and 1 for lock.

By default all external ports of the Access Gateway Module are locked in N_Port Mode. Use this command to unlock or lock the external port in order to configure additional F_Ports. See Figure 2-10 on page 25 for an example.

3.8.2 Access Gateway commands

ag --modenable

Enables Access Gateway Mode

ag --modedisable

Disables Access Gateway Mode

ag --modeshow

Displays which mode is currently active (Access Gateway or Switch Mode). See Example 3-4.

Example 3-4 ag --modeshow

```
brocade4Gb:USERID> ag --modeshow
Access Gateway mode is enabled.
brocade4Gb:USERID>
```

ag --show

Displays name, node name, IP Address, Firmware, online N- and F-Ports and their mapping, failover and failback policies as per Example 3-5 on page 69.

Example 3-5 The ag --show command

```
brocade4Gb:USERID> ag --show
Name           : brocade4Gb
NodeName       : 10:00:00:05:1e:02:17:37
Number of Ports : 20
IP Address(es) : 9.42.162.47
Firmware Version : v5.2.1b
N_Ports        : 1
F_Ports        : 2
Attached N_Port information :
  Port  PortID      PortWWN              F0  FB  IP_Addr  F_Ports
-----
   0  0x010200  20:02:00:05:1e:38:9d:e9  1  1  9.42.162.117  1;2;
-----
Attached F_Port information :
  Port  PortID      Port WWN              N_Port
-----
   1  0x010202  21:00:00:e0:8b:9d:a8:d7  0
   2  0x010201  21:00:00:11:25:93:af:4a  0
-----
brocade4Gb:USERID>
```

ag --mapset

Maps a F_Port to a specific N_Port of the fabric.

Syntax: **ag --mapset <N_Port F_Port>**

ag --mapadd

Adds an F_Port to an existing N_Port. An F_Port can be mapped to only one N_Port.

Syntax: **ag --mapadd <N_Port> <F_Port>**

ag --mapdel

Deletes the F_Port from an N_Port mapping.

Syntax: **ag --mapdel <N_Port> <F_Port>**

ag --mapshow

Displays the F_Ports that are currently connected to an N_Port. Example 3-6 shows an example of the command.

Syntax: **ag --mapshow <N_Port>**

Example 3-6 ag --mapshow

```
brocade4Gb:USERID> ag --mapshow
N_Port  Configured_F_Ports  Current_F_Ports  Failover  Failback
-----
   0    1;2;              1;2;             1         1
  15    3;4;              None              1         1
  16    5;6;7;          None              1         1
  17    8;9;              None              1         1
  18   10;11;          None              1         1
  19   12;13;14;       None              1         1
-----
```

Failover and failback policy commands

Commands that enable and disable failover/failback policies:

- ag --failbackenable <N_Port>** : Enables the failback policy for an N_Port
- ag --failbackdisable <N_Port>**: Disables the failback policy for the <N_Port>
- ag --failbackshow <N_Port>** : Displays the failback policy for the <N_Port>
- ag --failoverenable <N_Port>** : Enables the failover policy for the <N_Port>
- ag --failoverdisable <N_Port>** : Disables the failover policy for the <N_Port>
- ag --failovershow <N_Port>** : Displays the failover policy for the <N_Port>

3.8.3 Commands on the external Switch

agshow

Displays all active Brocade Access Gateways in the SAN as per Example 3-7 shown below.

Example 3-7 agshow

```
swd77:admin> agshow
Worldwide Name          Ports  Enet IP Addr  Firmware  Local/Remote  Name
-----
10:00:00:05:1e:02:17:37  20    9.42.162.47  v5.2.1b  local         brocade4Gb_0
10:00:00:05:1e:02:80:81  20    9.42.162.48  v5.2.1b  local         brocade4Gb_1
```

agshow

Displays properties of the dedicated Access Gateway as per Example 3-8.

Syntax: **agshow <name of an Access Gateway>**

Example 3-8 agshow <name>

```
swd77:admin> agshow brocade4Gb_0
Name                : brocade4Gb_0
NodeName            : 10:00:00:05:1e:02:17:37
N-Port ID(s)       : 0x010300
Number of Ports    : 20
IP Address(es)     : 9.42.162.47
Firmware Version   : v5.2.1b
N-Ports            : 1
F-Ports            : 2
Attached F-Port information :
  PortID    Port WWN
  -----
  0x010300  20:00:00:05:1e:02:17:37
  0x010302  21:00:00:11:25:93:af:4a
  0x010301  21:00:00:e0:8b:9d:a8:d7
```

Abbreviations and acronyms

AMM	Advanced Management Module	POD	Ports on Demand
BC	BladeCenter	RAID	redundant array of independent disks
BIOS	basic input output system	RBAC	Role Based Access Control
CLI	command-line interface	SAN	storage area network
DPOD	Dynamic Ports on Demand	SFP	small form-factor pluggable
DPS	Dynamic Path Selection	SMI-S	Role Based Access Control
EFCM	Enterprise Fabric Connectivity Manager	SNS	Secure Name Service
FB	fallback	SSH	Secure Shell
FC	Fibre Channel	UI	user interface
FCSM	Fibre Channel Switch Module	VM	virtual machine
FICON	Fibre Connection	VSAN	virtual SAN
FO	failover	WWN	World Wide Name
FOS	Fabric Operating System	WWPN	World Wide Port Name
FTP	File Transfer Protocol		
GB	gigabyte		
GUI	graphical user interface		
HBA	host bus adapter		
HT	Hyper-Threading		
HW	hardware		
I/O	input/output		
IBM	International Business Machines Corporation		
ID	identifier		
IOS	Internetwork Operating System		
IP	Internet Protocol		
ISL	Inter-Switch Link		
IT	information technology		
ITSO	International Technical Support Organization		
LE	low end		
LED	light emitting diode		
LUN	logical unit number		
MAC	media access control		
MDS	Multilayer Director Switch		
MSCS	Microsoft® Cluster Server		
MSIM	Multi-Switch Interconnect Module		
NPIV	N_Port ID Virtualization		
OPM	Optical Pass-thru Module		
OS	operating system		
PID	process ID		

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

You can search for, view, or download books, papers, Technotes, draft publications and additional materials, as well as order hardcopy IBM Redbooks publications, at the IBM Redbooks Web site:

ibm.com/redbooks

Related IBM Redbooks publications include the following:

- ▶ *IBM BladeCenter Products and Technology*, SG24-7523
- ▶ *IBM BladeCenter 4Gb SAN Solution*, SG24-7313

Online resources

These Web sites are also relevant as further information sources:

- ▶ IBM ServerProven:
<http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html>
- ▶ IBM Configuration and Options Guide:
<http://www.ibm.com/support/docview.wss?rs=1201&uid=psg1SC0D-3ZVQ5W>
- ▶ IBM BladeCenter support:
<http://www.ibm.com/systems/bladecenter/support>
- ▶ Cisco Technical Assistance Center:
<http://www.cisco.com/tac>
- ▶ Windows Server 2003 R2 Enterprise Edition – Server Cluster:
<http://www.microsoft.com/windowsserver2003/enterprise/clustering.msp>

Help from IBM

IBM Support and downloads: ibm.com/support

IBM Global Services: ibm.com/services

