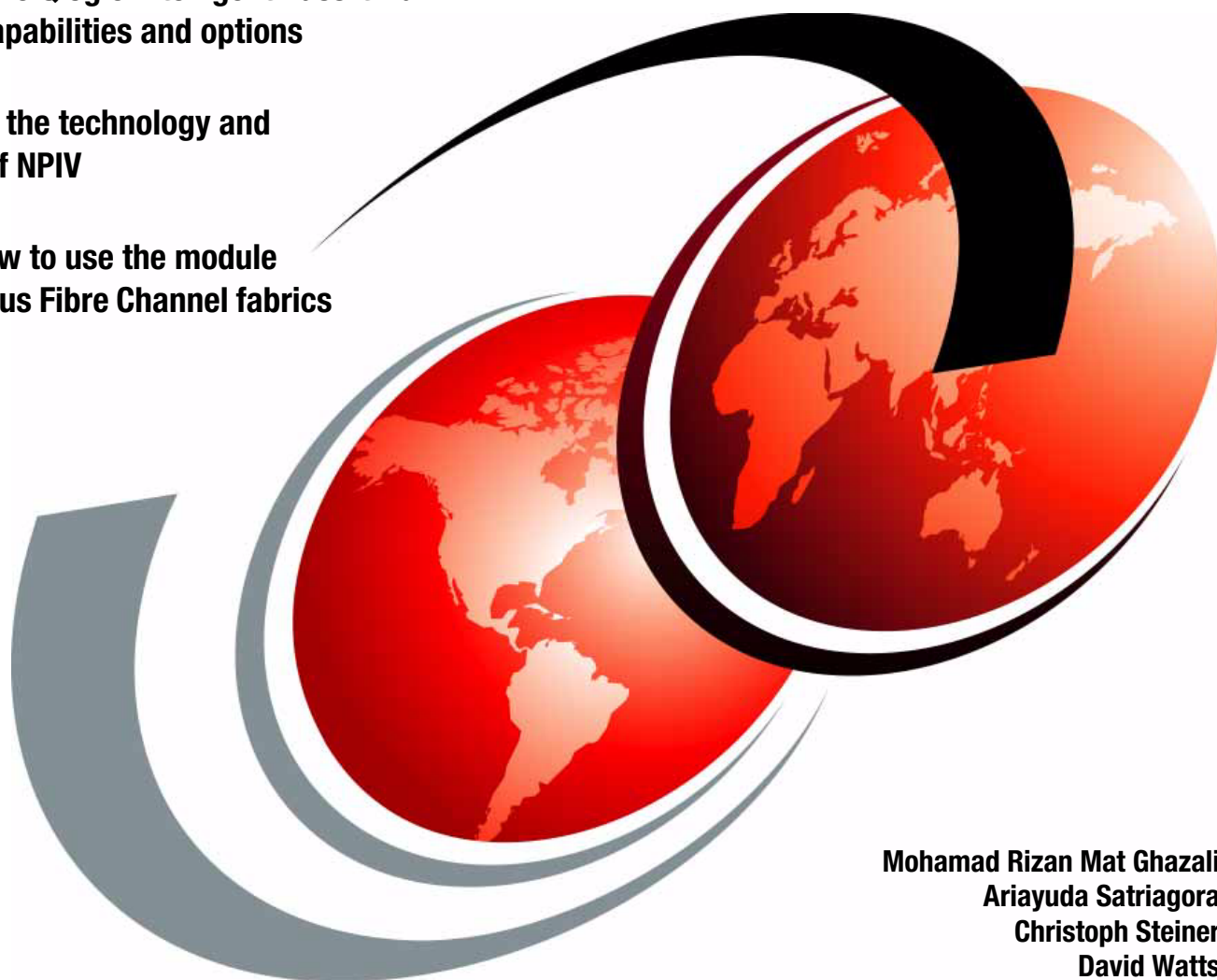


Implementing the QLogic Intelligent Pass-thru Module for IBM BladeCenter

Explains the Qlogic Intelligent Pass-thru Module 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 QLogic Intelligent Pass-thru Module
for IBM BladeCenter**

November 2007

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

First Edition (November 2007)

This edition applies to the QLogic Intelligent Pass-thru Module, part number 43W6723.

This document created or updated on October 30, 2007.

© 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	ix
Comments welcome	ix
Chapter 1. Introduction and technology	1
1.1 Introducing the QLogic 4 Gb Intelligent Pass-thru Module	2
1.1.1 Basic concept	2
1.1.2 Port mapping	4
1.2 N_Port ID Virtualization	6
1.3 Benefits of using the Intelligent Pass-thru Module	8
1.3.1 Interoperability	8
1.3.2 Scalability	9
1.3.3 Simplification	10
1.3.4 Cost reduction	11
1.4 Typical uses of the Intelligent Pass-thru Module	11
1.4.1 Environment with many different fabric vendors	11
1.4.2 Environment where fabric size is becoming a burden	12
1.4.3 Environments with compartmentalized administration	12
1.5 Limitations of the Intelligent Pass-thru Module	12
Chapter 2. Planning	13
2.1 Compatibility	14
2.2 Prerequisites	17
2.3 Additional considerations	19
2.3.1 Switch connection	19
2.3.2 Optical Pass-thru Module connections	20
2.3.3 Using the Intelligent Pass-thru Module	21
2.3.4 Limitations	22
2.4 Failover and fallback policies	23
Chapter 3. Implementation	31
3.1 Tools and environment	32
3.1.1 Tools	32
3.1.2 Environment	33
3.2 Setting up the blade server	34
3.2.1 Install the HBA	34
3.2.2 Manage the HBA	34
3.3 Setting up the Intelligent Pass-thru Module	36
3.3.1 Insert the IPM into the chassis	36
3.3.2 Set up the I/O module IP address	36
3.3.3 Enable module external ports	37
3.3.4 Verify and update module firmware level	38
3.3.5 Verify and modify module port status	43
3.3.6 Verify and modify module port mapping	47

3.4	Setting up the external switch	51
3.4.1	Verify and update switch firmware level	51
3.4.2	Enable NPIV	57
3.5	Configuring the connection	66
3.5.1	Connecting the Intelligent Pass-thru Module to external switch	66
3.5.2	Verify the connection	69
3.5.3	Configure zoning	72
3.5.4	Configure redundancy and load balancing	74
3.5.5	Storage attachment	75
	Abbreviations and acronyms	83
	Related publications	85
	IBM Redbooks	85
	Online resources	85
	Help from IBM	86

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:

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

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

Java, Solaris, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Internet Explorer, 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 QLogic® Intelligent Pass-thru Module 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 machine, through their virtual port provides more granularity to fulfill service level agreements. Finally the ability to tear down a virtual port and reinitialize it on different blade server greatly enhances virtual machine portability for load balancing, portability and incident recovery. In short, NPIV enhances SAN connectivity, flexibility security, resource allocation and recovery.

This IBM Redpapers publication introduces the QLogic Intelligent Pass-thru 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

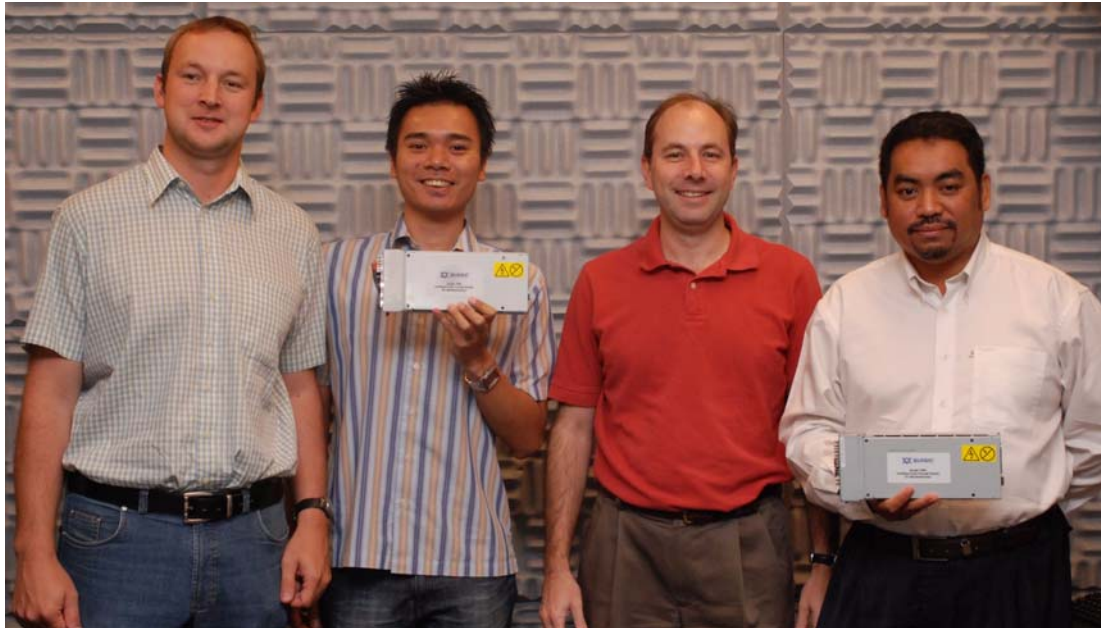
This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Raleigh Center.

Mohammad Rizan M. Ghazali is a 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 advises and provides direction and resolution to customer problems.

Ariayuda Satriagora is a System Support Representative in Indonesia. He has three years of experience in IBM System x and BladeCenter servers field. 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 and 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 U. S. and Australia since 1989. He is an IBM Certified IT Specialist.



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

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

From the ITSO Raleigh Center:

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

From IBM Corporation

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

From QLogic

- ▶ Barbara Craig
- ▶ Ed McGlaughlin
- ▶ Hermal Purohit
- ▶ Michael Walton

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 in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks 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, fabric management complexity increases also. SAN solution demand continues to grow as companies continue to demand more computing resources. One of the recent technologies applied in blade technology that addresses this issue is the *QLogic 4 Gb Intelligent Pass-thru Module*.

In this chapter, we discuss the following topics:

- ▶ 1.1, “Introducing the QLogic 4 Gb Intelligent Pass-thru Module” on page 2
- ▶ 1.2, “N_Port ID Virtualization” on page 6
- ▶ 1.3, “Benefits of using the Intelligent Pass-thru Module” on page 8
- ▶ 1.4, “Typical uses of the Intelligent Pass-thru Module” on page 11
- ▶ 1.5, “Limitations of the Intelligent Pass-thru Module” on page 12

1.1 Introducing the QLogic 4 Gb Intelligent Pass-thru Module

This section discusses the basic concept of the QLogic 4 Gb Intelligent Pass-thru Module, part number 43W6723, and the related technologies.

1.1.1 Basic concept

The QLogic 4 Gb Intelligent Pass-thru Module is a SAN connectivity device built on blade technology that combines the advantages of a switch module and a pass-thru module. The Intelligent Pass-thru Module provides the same connectivity speed that a switch does. At the same time, it does not participate in SAN fabrics as does a Fibre Channel switch. Therefore, it does not have the associated constraints of the Fibre Channel switch, such as domain proliferation and interoperability issues.

Furthermore, the Intelligent Pass-thru Module simplifies blade server deployments in SAN, enables fabric interoperability, and reduces management overhead. Using the Intelligent Pass-thru Module can increase the interoperability, scalability, and manageability of the SAN.

You can also upgrade the Intelligent Pass-thru Module to a full fabric 20-port switch by purchasing and applying the appropriate license. In addition, when operating as a full fabric switch, you can easily revert back to the original Pass-thru Module function as required.

Table 1-1 compares the IBM Optical Pass-thru Module and Fibre Channel Switch Module to the QLogic Intelligent Pass-thru Module.

Table 1-1 Basic comparison of pass-thru modules

	Optical Pass-thru Module	Fibre Channel Switch Module	Intelligent Pass-thru Module
Interoperability	No issue	There are some interoperability issues	No issue
Domain proliferation	No issue	Limited	No issue
TCO (cables, edge switches, SFPs)	Relatively high	Relatively low	Relatively low
Typical speed	Slower	Faster	Faster
SAN management	Simple	Flexible	Simple and Flexible

We use five Fibre Channel port terms in this paper:

- ▶ *N_Port*, node port. A host, HBA, or storage device port that connects to the F_Port of the fabric 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.
- ▶ *TH_Port*, Transparent Host Port, a port of QLogic 4 Gb Intelligent Pass-thru Module which is connected to host.
- ▶ *TF_Port*, Transparent Fabric Port, a port of QLogic 4 Gb Intelligent Pass-thru Module which is connected to fabric.

N_Port, *F Port*, and *E_Port* are commonly used terms in SAN connection. *TH_Port* and *TF_Port* are used especially in the Intelligent Pass-thru Module.

Figure 1-1 shows an example of N_Ports, F_Ports and E_Ports in a Fibre Channel Switch Module connection.

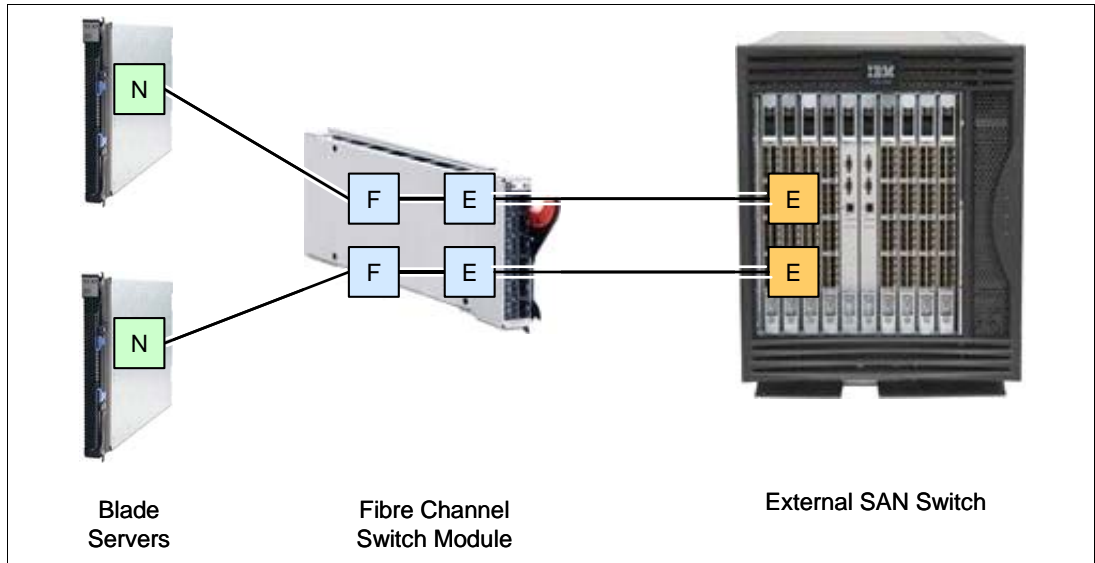


Figure 1-1 An example of port types in a Fibre Channel Switch Module connection

The Intelligent Pass-thru Module multiplexes host connections to the fabrics. It presents an F_Port to the host and an N_Port to fabrics. Using N_Port ID Visualization (NPIV) technology, the Intelligent Pass-thru Module allows multiple FC initiators to access the same physical port. External ports on the Intelligent Pass-thru Module appear to the fabrics as N_Port connections and no domain is added to the fabrics. We discuss NPIV technology in detail in 1.2, “N_Port ID Virtualization” on page 6.

Figure 1-2 illustrates host to fabric connection through the Intelligent Pass-thru Module and how it is compared to Fibre Channel Switch Module connection.

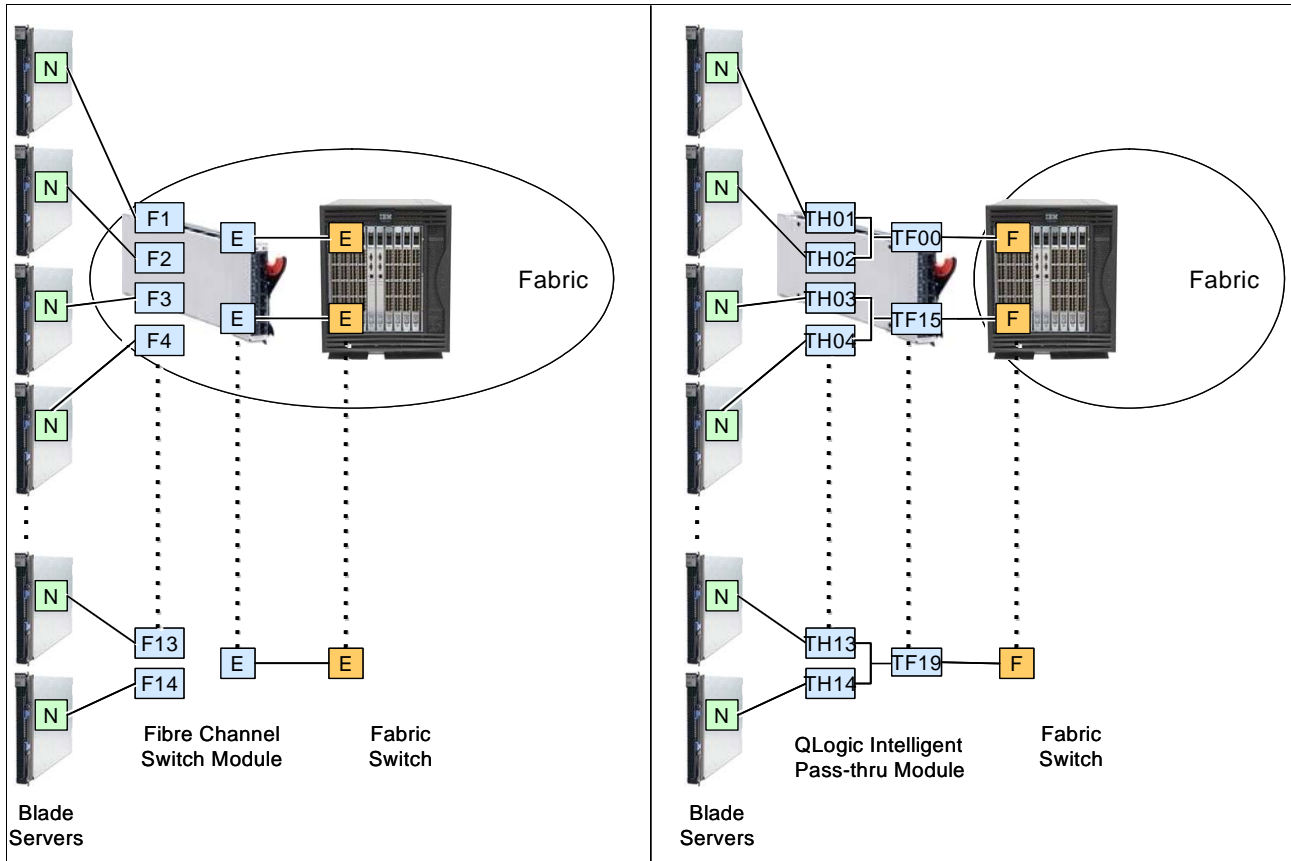


Figure 1-2 Comparison of port types used by Intelligent Pass-thru Module and those used by a FC Switch Module

1.1.2 Port mapping

To manage traffic between hosts and the fabric, the Intelligent Pass-thru Module uses *port mapping*. TH_Ports must be mapped to TF_Ports so that servers have a path to external SAN fabric. This mapping builds static routes between specific TH_Port to specific TF_Port.

There is a default port mapping that predefines the routes between the TF_Ports and the TH_Ports. By default, all external ports of a Intelligent Pass-thru Module (Port 0, 15-19) are configured as TF_Ports and all internal ports are configured as TH_Ports and mapped to the TF_Ports. This default mapping can be changed if required.

Figure 1-3 illustrates a port mapping example of a Intelligent Pass-thru Module that connects blade servers to the external fabric.

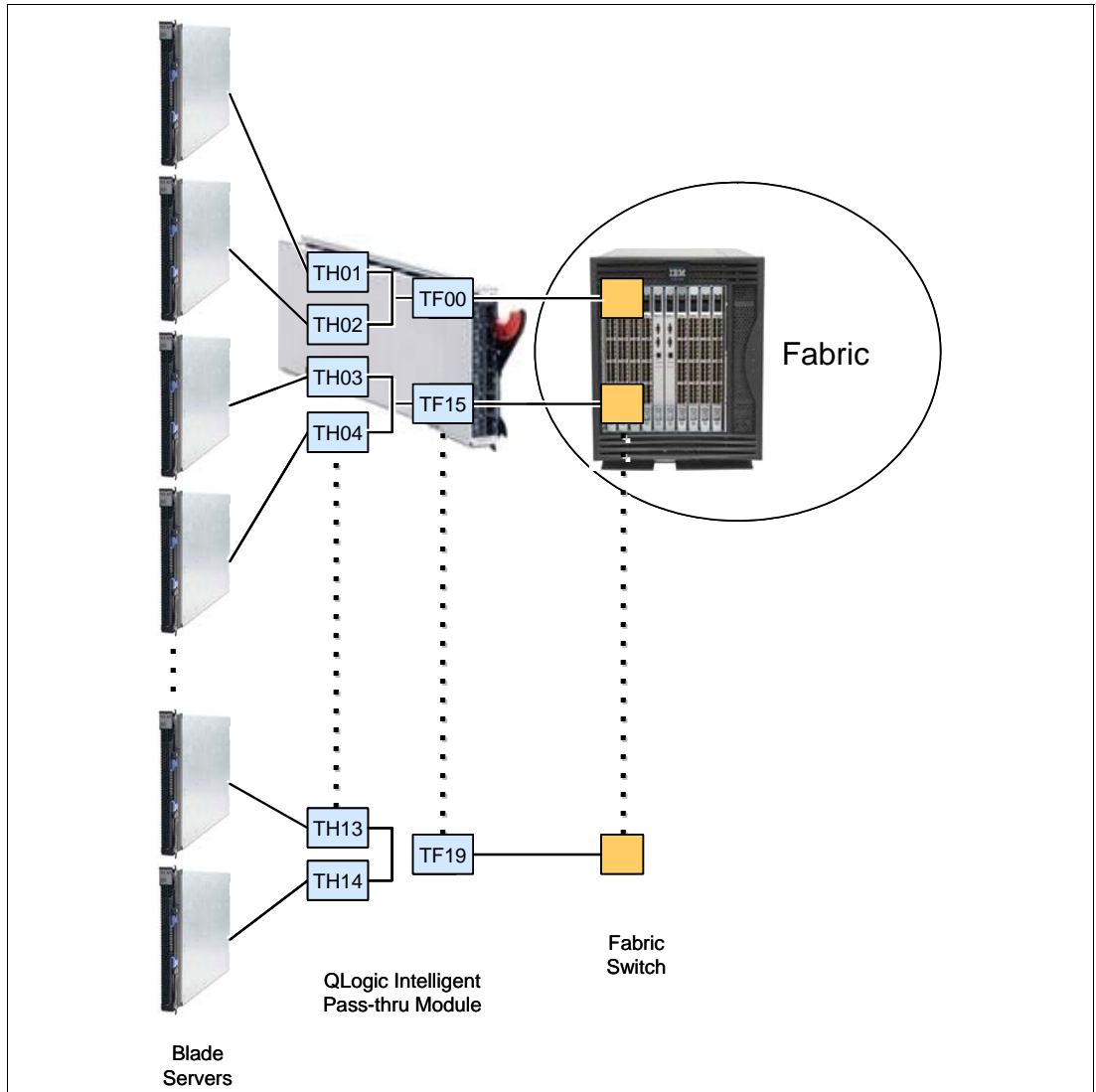


Figure 1-3 An example of port mapping

Table 1-2 summarizes the mapping example shown in Figure 1-3.

Table 1-2 An example of port mapping table

TH_Ports	TF_Ports
P01	P00
P02	P00
P03	P15
P04	P15
P13	P19
P14	P19

1.2 N_Port ID Virtualization

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, thereby allowing multiple, distinguishable entities on the same physical ports. In other words, it makes a single Fibre Channel port appear as multiple virtual ports, each having its own N-Port ID and virtual worldwide name (WWN). The NPIV protocol requires an N_Port (typically a host bus adapter any device that acts as an NPIV gateway) and a fabric (generally an FC switch) so that the N_Port can request and acquired multiple addresses from the fabric.

An NPIV implementation requires two participating ports:

- ▶ An N_Port that communicates with a Fibre Channel fabric for requesting port addresses and subsequently registering with the fabric.
- ▶ An F_Port that assigns the addresses and provides fabric services.

NPIV enables several possible solutions, such as HBAs and server virtualization and gateway connectivity for multiple servers, without adding an additional Fibre Channel Domain to an existing Fibre Channel Fabric.

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 a host bus adapter (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 illustrates how a single HBA shares its single physical N_Port to some VMs virtual N_Ports.

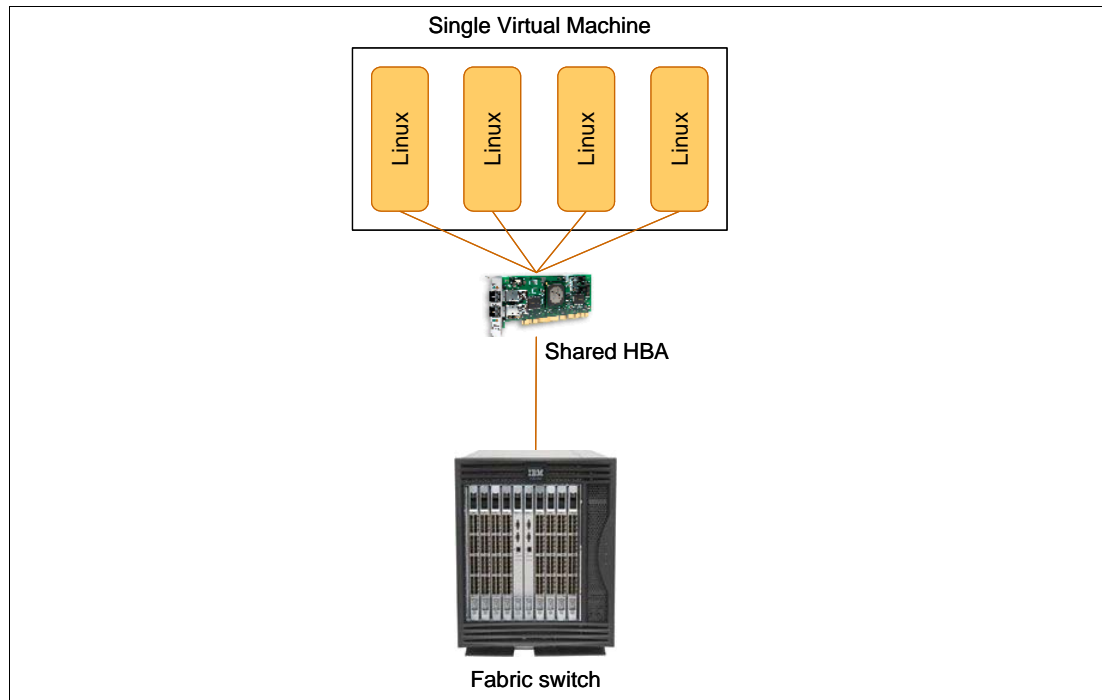


Figure 1-4 Illustration of NPIV

The benefits of NPIV and the Intelligent Pass-thru Module is that the NPIV pre-requisites are handled by the module, which means:

- ▶ You do not need to change any settings on the HBA when implementing the Intelligent Pass-thru Module.
- ▶ An NPIV-capable HBA is not required, although one that is NPIV-capable is supported.
- ▶ The operating system on the blades is not required to recognize or take advantage of NPIV technology, although it is supported if present. The NPIV connection is fully handled by the module.

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 partition 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. Because zoning is based on WWN, the separate virtual hosts have controlled access to the allocated storage.

1.3 Benefits of using the Intelligent Pass-thru Module

We describe the benefits of using the Intelligent Pass-thru Module in the following sections.

1.3.1 Interoperability

Using the Intelligent Pass-thru Module 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 Intelligent Pass-thru Module presents the hosts transparently as N_Port devices to the fabric, management of the fabric is unaffected.

Figure 1-5 and Figure 1-6 show connections between blade servers and the fabric through a Intelligent Pass-thru Module and how they are represented in the fabric.

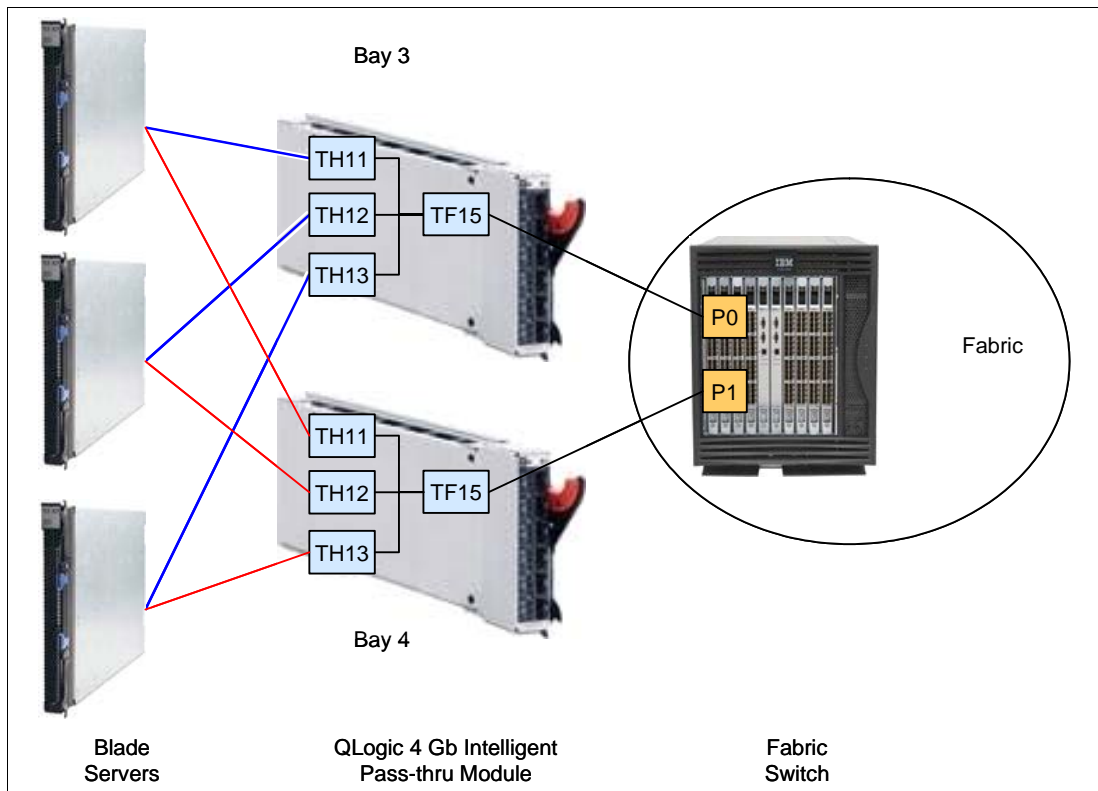


Figure 1-5 Blade server to fabric connection through QLogic 4 Gb Intelligent Pass-thru Module

swd77 : Name Server Table. - Microsoft Internet Explorer

Name Server

Auto Refresh Auto-Refresh Interval: 15 seconds Number of Devices: 12

All Devices

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	NPIV(...)	Host vs. Target
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	NPIV	Initiator
1	15	010f00	N	20:25:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	5	010500	N	20:14:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
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	NPIV	Initiator
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 (...)	NPIV	Initiator
1	4	010400	N	20:24:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	14	010e00	N	20:15:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	1	010100	N	20:00:00:c0:dd:0d:35:8f	10:00:00:c0:dd:0d:35:8f		Physical	Unknown(Initia...
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 (...)	NPIV	Initiator
1	0	010000	N	20:00:00:c0:dd:0d:35:a3	10:00:00:c0:dd:0d:35:a3		Physical	Unknown(Initia...
1	1	010101	N	21:00:00:1b:32:18:1a:0b	20:00:00:1b:32:18:1a:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	NPIV	Initiator
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	NPIV	Initiator

Detail View Accessible Devices Refresh Print Close

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

Figure 1-6 Brocade Silksworm Web Tools Name Server table

The blue boxes in Figure 1-6 indicate all HBA WWNs that connected to Port 0 of the fabric switch. The red boxes indicates those HBA WWNs that connected to Port 1 of the fabric switch.

The Intelligent Pass-thru Module does not appear like a switch to fabrics. It avoids the reduced feature set that is likely to be required when someone connects a switch to multivendor networks.

1.3.2 Scalability

By eliminating the switch domain, the Intelligent Pass-thru Module directly addresses an important SAN scalability constraint: the number of domains in a fabric.

Adding a Fibre Channel Switch Module, which has fewer ports, significantly increases the number of domains in a fabric compared to the addition of the nodes. With a limited total number of domains which can be supported in a fabric, this becomes undesirable situation, especially for enterprise with a large BladeCenter infrastructure. Because the Intelligent Pass-thru Modules do not participate as a switch in the fabric, they do not require domains and do not impair the SAN scalability.

For example, consider that an enterprise is connecting 32 BladeCenter chassis to 4 switches in the fabric. With Fibre Channel switch modules, they need at least 36 domain IDs in that fabric. With the Intelligent Pass-thru Module, they need only 4 domain IDs instead of 36. Figure 1-7 illustrates this example.

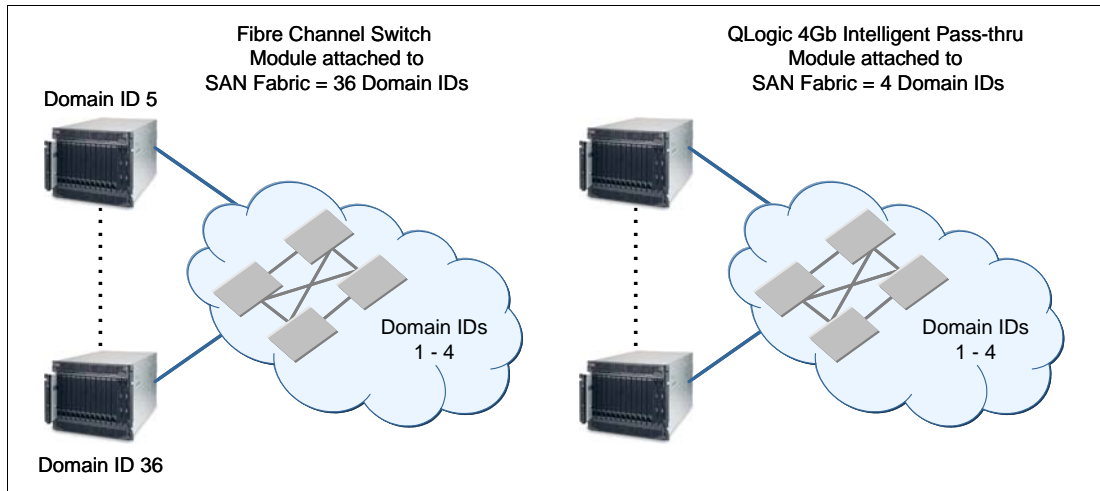


Figure 1-7 Intelligent Pass-thru Module implementation reduces the number of domain IDs in a fabric

1.3.3 Simplification

A massive scale blade system with its Fibre Channel switch implementation sometimes creates an undesirable situation. With a lot of Fibre Channel switch modules added in the existing SAN environment, the topology becomes more complex. At the same time, these switches embedded into the chassis also create a potential device management issue with administrators who are responsible for managing these Fibre Channel switch modules.

By not adding switching devices to the existing SAN environment regarding the blade system implementation, the Intelligent Pass-thru Module simplifies the topology. It provides fewer switches and simpler connection with the same number of nodes in topology. Because the Intelligent Pass-thru Module does not participate in the fabric as a switch, switch standard management activities, such as zoning, are no longer needed in this device.

From an administration perspective, using the Intelligent Pass-thru Modules gives clearer perspective of administrator responsibility, because they are not considered fabric domains.

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

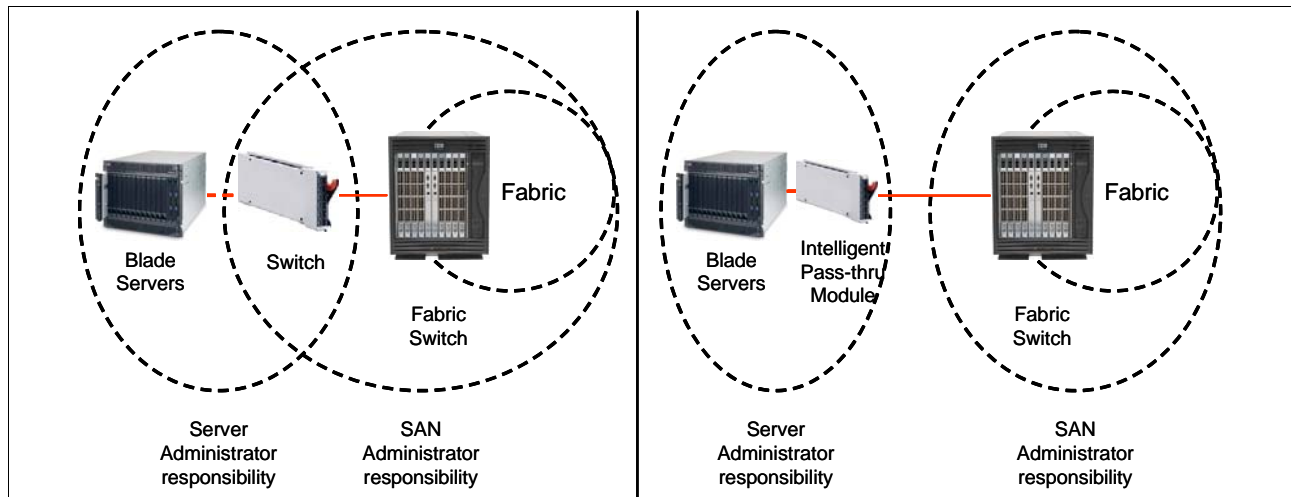


Figure 1-8 Comparison of administration perspective in a typical blade environment

1.3.4 Cost reduction

The existing pass-through solution, Optical Pass Through Module, uses dedicated cabling to connect each blade server to a port on an external switch. Dedicated cabling makes pass-through solutions expensive to maintain. Each blade server requires dedicated connectivity hardware and a dedicated port on the external switch. Using the QLogic 4 Gb Intelligent Pass-thru Modules reduces the number of SAN ports, SFP, and cables required.

Compared to using a Fibre Channel switch module, using an Intelligent Pass-thru Module is also financially compelling. The purchase price of an Intelligent Pass-thru Module is typically lower than that of a Fibre Channel switch module with the same number of ports.

1.4 Typical uses of the Intelligent Pass-thru Module

Based on the benefits that we have discussed previously, we present in this section some typical cases where the QLogic 4 Gb Intelligent Pass-thru Module can be a solution.

1.4.1 Environment with many different fabric vendors

This case happens typically in enterprises with large scale and wide variety of SAN devices or in growing companies that implement devices that are provided by many different vendors in terms of cost saving. For example, a small company was set up with very limited SAN environment using low-budgeted and limited featured switches from certain vendor. As it grows, its SAN environment adds more advanced switches from many other vendors. Then, the company begins to experience interoperability issues.

By making the switches transparent to the fabric, the Intelligent Pass-thru Module reduces interoperability issue significantly in maintaining a huge SAN environment with multivendor fabric. It includes a reduced feature set and a more complex multi vendor fabric administration.

1.4.2 Environment where fabric size is becoming a burden

This situation happens typically in enterprises with large scale SAN. Today, many enterprises have implemented a large SAN environment with many domains in a fabric, some with more than 30 domains in their fabric. Unfortunately, most vendors support many fewer than the total domains in a fabric defined in the Fibre Channel Standards (237), typically 24 to 55. Therefore, a solution for this issue is very desirable.

By eliminating the switch domain, the Intelligent Pass-thru Module addresses this scalability constraint directly.

1.4.3 Environments with compartmentalized administration

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

For example, to support the company's enterprise, the company might hire people to function as the server administrator, the network administrator, and the SAN administrator. While the complex SAN topology remains, this situation of having several different administrators sometimes creates a grey area in terms of administrative authority and responsibility. In the case of the blade environment, this kind of situation typically happens regarding the switch module management. Operating as a switch, a Fibre Channel Switch Module is sometimes managed by both the SAN administrator and a server administrator (because it is considered a part of BladeCenter).

By implementing transparent switching, the Intelligent Pass-thru Module reduces the complexity of SAN topology. Also, because they do not appear as switching devices, this solution can give a clearer perspective of administrator authority and responsibility.

1.5 Limitations of the Intelligent Pass-thru Module

There are some limitations of implementing Intelligent Pass-thru Module as follows:

- ▶ Direct connection to SAN targets

The Intelligent Pass-thru Module does not support direct connection to SAN targets, such as tape or disk enclosure for examples.

- ▶ Number of devices in connection

There is no theoretical maximum of the Intelligent Pass-thru Module that can be connected into a single fabric. The maximum number of devices that can be connected to a fabric via the Intelligent Pass-thru Module depends on the maximum number of local devices that are supported in the fabric. Up to 16 NPIV WWNs can be allocated to one external SFP port in transparent mode. The number becomes 256 in the full-fabric mode.

- ▶ Cascading devices

Cascading between the Intelligent Pass-thru Modules is only supported in full-fabric mode.

- ▶ Switch features

With the Intelligent Pass-thru Module, some switch features are not applicable. For examples FICON®, ISL Trunking, and Management Services. These features are available in full fabric mode.



Planning

This chapter provides information about the planning and installation of the Intelligent Pass-thru Module. Although the hardware is equal to the existing Fibre Channel Switch, there are few things to consider when you install the Intelligent Pass-thru Module, such as prerequisites, compatibility matrixes, and failover matrixes before you begin deployment.

In this chapter, we discuss the following topics:

- ▶ 2.1, “Compatibility” on page 14
- ▶ 2.2, “Prerequisites” on page 17
- ▶ 2.3, “Additional considerations” on page 19
- ▶ 2.4, “Failover and failback policies” on page 23

2.1 Compatibility

The implementation process of an Intelligent Pass-thru Module (IPM) is fast and simple. In the case of setting up new systems, you can install the necessary hardware in a relatively short amount of time.

As listed in the Table 2-1, the IPM is supported in all available BladeCenter chassis.

Table 2-1 BC Chassis Support matrix

Part	I/O Module	BCE	BCT	BCH	BCHT
43W6723	QLogic 4 Gb Intelligent Pass-thru Module	Yes	Yes	Yes	Yes

You must install Intelligent Pass-thru Modules only in I/O-module bays 3 and 4 (see Figure 2-1) of the BladeCenter unit. Installing two provides redundancy. At least one IPM is required when you install the BladeCenter Fibre Channel Expansion Card in the blade server. Installing an IPM 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 IPM enables a second connection to a Fibre Channel expansion card in the BladeCenter unit. Adding a second IPM provides a redundant path and a separate Fibre Channel connection from the blade server to the external Fibre Channel network and SAN.

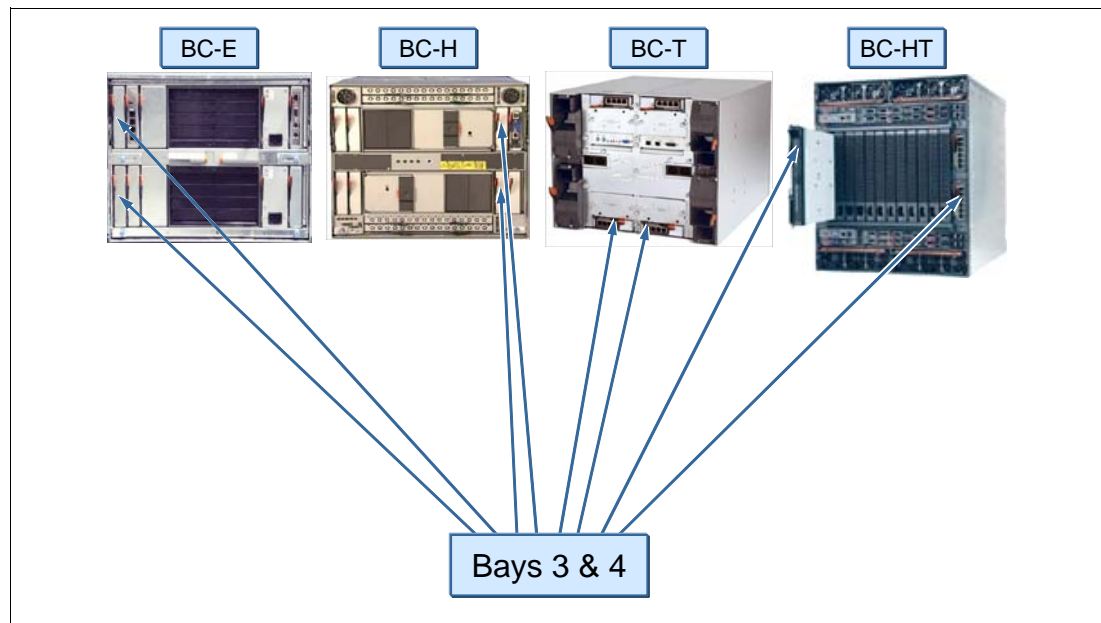


Figure 2-1 Bays 3 and 4 of the BladeCenter chassis

Table 2-2 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 Intelligent Pass-thru Module. 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.

Table 2-2 BladeCenter 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 Intelligent Pass-thru Modules in a Multi-Switch Interconnect Module (MSIM, see Figure 2-2), provided that 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 Table 2-2.



Figure 2-2 Multi-Switch Interconnect Module

The ports on the CFFh expansion cards in each server are hardwired to specific bays in the switch modules in each MSIM. Refer to Table 2-3 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 operates only in the left-hand I/O Slot of the MSIM. The OPM works in both of the two 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)

Table 2-4 shows the compatibility between HBAs with the respective chassis.

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 4Gb Standard FC Expansion Card	Yes	Yes	Yes	Yes
26R0890	QLogic 4Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
39Y9186	Emulex 4Gb SFF Fibre Channel Expansion Card	Yes	Yes	Yes	Yes
41Y8527	QLogic 4Gb Fibre Channel Expansion Card (CFFv)	Yes	Yes	Yes	Yes
43W6859	Emulex 4Gb 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 & 4Gb 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 that we cover in 2.1, “Compatibility” on page 14, 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 IPM requires the NPIV functionality to be enabled on the edge switch. An IPM 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
Brocade ^a	SilkWorm 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4100, 4900, 7500, 24000, 48000	v5.1.0 or later
Cisco ^b	MDS9120, MDS9140, MDS9216, MDS9506, MDS9509	SAN-OS 2.1(2b) or later
QLogic ^c	SANbox® 5200, 5202, 5600, 5602, SANbox 9000	v6.0 or later
McDATA ^d	Sphereon 3016, 3032, 3216, 3232, 4300, 4500 Intrepid 6064, 6140, 10000	E/OS 8.0 or later

a. Brocade models 3014, 3250, 3850, 3900, and 24000 have NPIV support defaulted OFF and it 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 NPIV license after E/OS 9.6.x as the license is included.

Firmware updates

You can download the latest firmware from these URLs:

► Brocade:

<http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/supportresources?brandind=5000031&familyind=5329725&taskind=2>

► Cisco:

<http://www.cisco.com/public/sw-center/>

► QLogic:

SANbox 9000:

http://support.qlogic.com/support/product_resources.asp?id=1006&type=switch

SANbox 5600/2:

http://support.qlogic.com/support/product_resources.asp?id=929&type=switch

SANbox 5200/2:

http://support.qlogic.com/support/product_resources.asp?id=540&type=switch

► McDATA:

<http://www.mcdata.com/filecenter/template?page=index>

Zoning

Use zoning to create a segmentation of the fabric and the different environments so that only members in the same zone can communicate. Because all zoning features are removed in the IPM, you have to set up the zoning configuration on the fabric switch outside of the BladeCenter.

There are two zoning methods:

► *Port zoning*

This method 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*

This method 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 (WWNs). 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 still remains 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 full switch mode requires no changes to the zoning configuration.

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

Licensing

An upgrade to a full fabric switch is possible through the purchase of the following keys:

► QLogic 10-port and 20-port 4 Gb San Switch Modules for IBM BladeCenter.

The QLogic 4 Gb San Switch Modules are full-fabric Fibre Channel switches and are available in both 10 and 20-port active configurations, which enables high-performance 1, 2, and 4 Gb per second SAN solutions. The 10-port model can also be upgraded to 20 ports through the purchase of a license key (QLogic 10-port upgrade for IBM BladeCenter)

The 10-port switch provides the ability to connect up to seven internal blade server ports, and three external ports, while the 20-port switch provides all 14 internal ports and six external ports. Table 2-6 shows the product and order information for these modules.

► QLogic 20-port Full Fabric License for IBM BladeCenter.

The 20-port full fabric upgrade license is used to upgrade the QLogic 4 Gb Intelligent Pass-thru Module to a full fabric, 20 port switch.

Table 2-6 Product and order information

Description	Order number
QLogic 10-port 4 Gb Upgrade for IBM BladeCenter (10-port upgrade to 20-ports)	32R1912
QLogic 4 Gb Intelligent Pass-thru Module for IBM BladeCenter (IPM upgrade to 20-ports full fabric)	43W4413

Tip: It is also possible to convert a Fibre Channel Switch Module that was previously upgraded from IPM back to an IPM.

2.3 Additional considerations

Previously, there were two possibilities for connecting BladeCenter to a SAN: using a switch connection or using an Optical Pass-thru Module. Now, you can also use the Intelligent Pass-thru Module. This section discusses some additional considerations for these possible connections.

2.3.1 Switch connection

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

- ▶ Six external autosensing Fibre Channel ports that operate at a maximum of 4 Gbps
- ▶ 14 internal fixed-speed Fibre Channel ports that operate at a maximum of 4 Gbps
- ▶ Two internal full-duplex 100 Mbps Ethernet interfaces
- ▶ External ports that can be configured as F_Ports (fabric ports), FL_ports (fabric loop ports), or E_Ports (expansion ports)
- ▶ Internal ports that are configured as F_Ports at 2 Gbps or 4 Gbps
- ▶ Power on diagnostics and status reporting
- ▶ Fabric security for controlling management access
- ▶ Support for Non-Disruptive Code Load Activation (NDCLA)
- ▶ Simple name server implementation
- ▶ Registered State Change Notification (RSCN)
- ▶ Support for standards based FC-SW2 interoperability
- ▶ Error detection
- ▶ Frame bundling
- ▶ Configurable Fabric Address Notification (FAN)
- ▶ Support up to 239 switches depending on configuration
- ▶ Optional small form-factor pluggable (SFP) modules

Figure 2-3 shows a configuration using Fibre Channel switch modules.

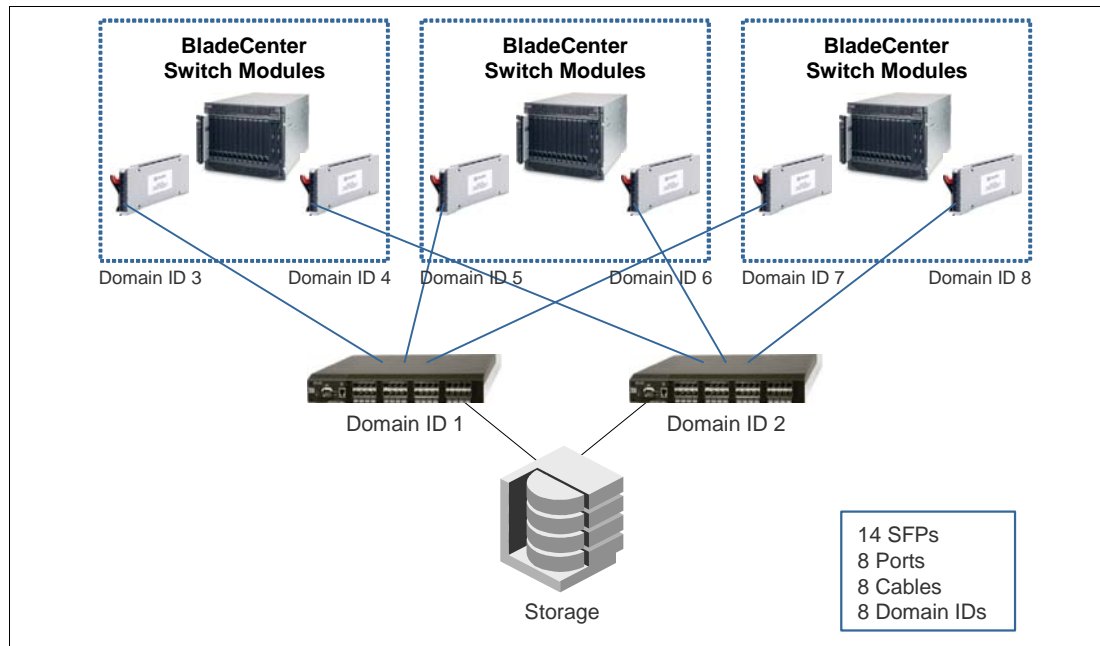


Figure 2-3 Switch connectivity

2.3.2 Optical Pass-thru Module connections

The Optical Pass-thru Module (OPM) provides an unswitched or 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:

- ▶ Confirms 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

Figure 2-4 shows a configuration using OPMs.

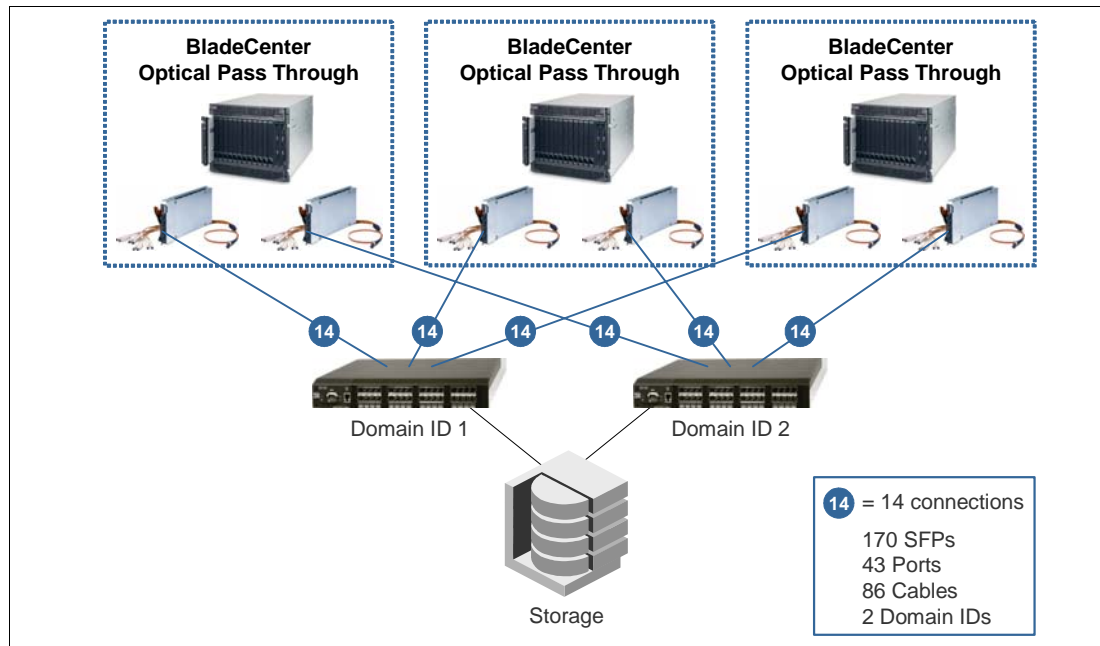


Figure 2-4 OPM connectivity

2.3.3 Using the Intelligent Pass-thru Module

If you have large Fibre Channel fabrics, choosing the switch or OPM connections can yield one of the following situations:

- ▶ A lot of domain administration, where each switch gets its own domain ID with the use of Fibre Channel switch modules
- ▶ A lot of cables, SFPs, and physical ports (28 for each BladeCenter) if you choose the use of OPMs

The Intelligent Pass-thru Module offers a new way to connect to a SAN without these drawbacks:

- ▶ IPM 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 costly switch port licenses are no longer required.
- ▶ Due to the implementing of transparent switching, all standard management features, such as name server table, zoning, and domain ID administration, are fully removed from the switch. This transparency enables easy administration by either a SAN or a server administrator.

Figure 2-5 shows a sample Fibre Channel fabric with the smaller hardware requirements.

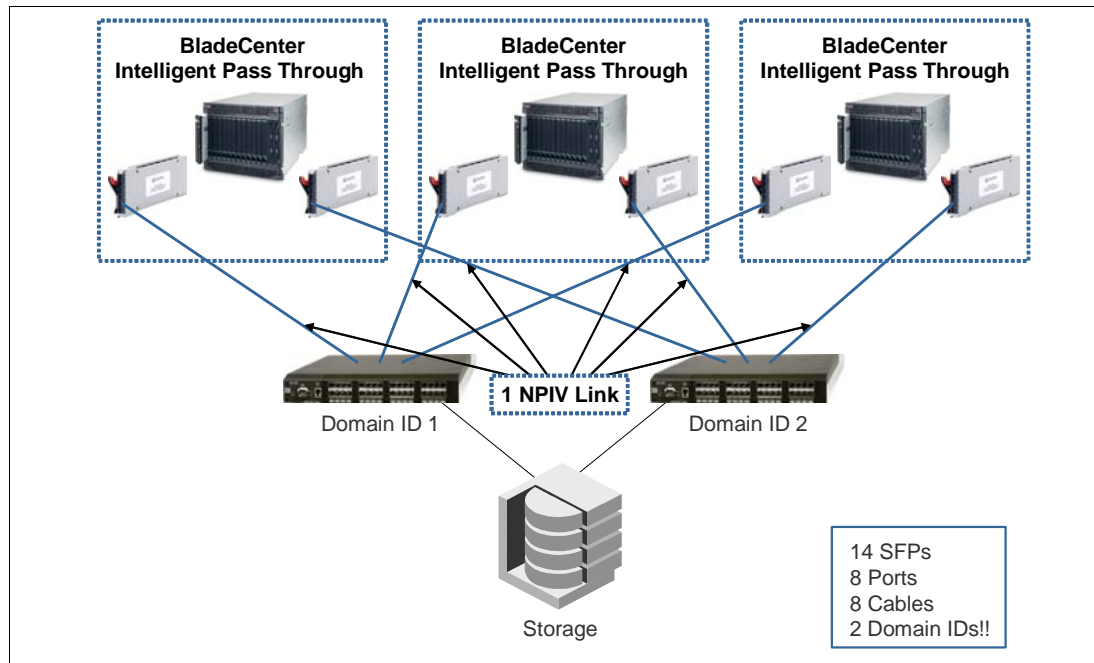


Figure 2-5 Sample with Intelligent Pass-thru Module

2.3.4 Limitations

If you plan to implement an IPM, consider the following limitations:

- ▶ There is no physical-port or virtual-port limitation on the Intelligent Pass-thru Module, which means that all of the 14 internal Ports can be mapped to one physical external Port. The only limit that you need to consider is the edge switches, which depends 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 cannot have 255 virtual PIDs because of the limit on the maximum number virtual PIDs a switch can have.

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

Note: By default all external ports present N_Ports to the edge fabric switch.

- ▶ IPM can be connected to multiple fabrics.

2.4 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 port are distributed among all the online N_Ports in a sequence as described in the following scenario.

Figure 2-6 displays a simple configuration with two hosts (blades) for explaining the failover and failback policies. The solid green line shows the default mapping according to Table 2-8 on page 24.

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

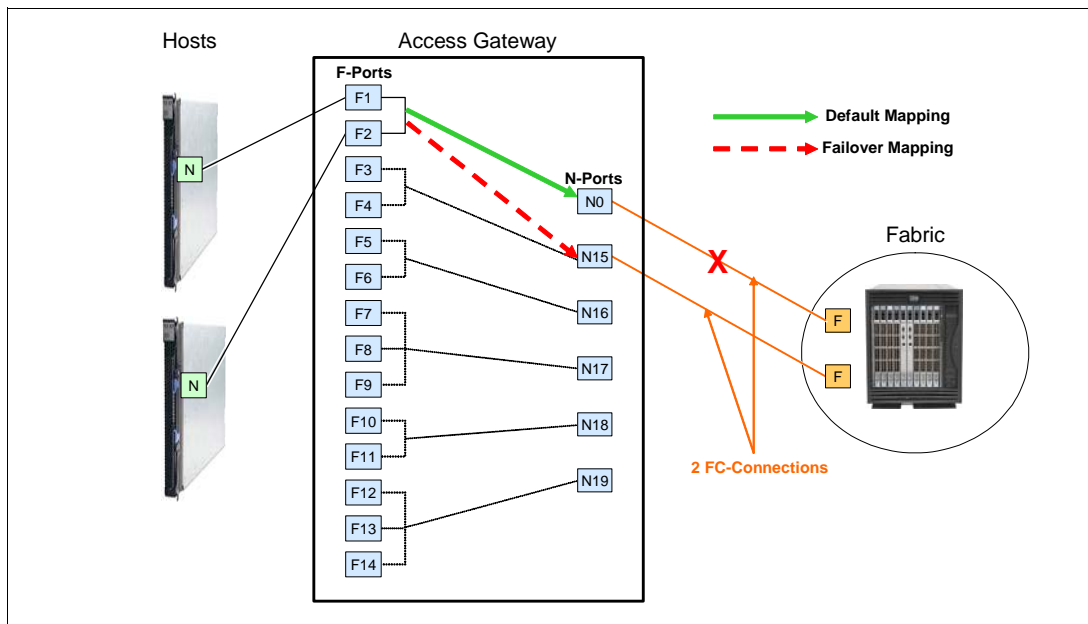


Figure 2-6 Failover scenario

IPM uses a TH_Port (internal ports) to TF_Port (external ports) mapping. Table 2-8 lists the default port mapping, which can be changed manually by the CLI or Quick Tools, if required.

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 command **show config port** lists the current mapping as shown in Figure 2-7. The entries PrimaryTFPortMap and BackupTFPortMap indicate whether the FO or FB policies are enabled or disabled.

```
IBM4GbT: admin> show config port 1

Configuration Name: config_test
-----

Port Number: 1
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap 0
BackupTFPortMap 15
SymbolicName   Port1

IBM4GbT: admin> show config port 2

Configuration Name: config_test
-----

Port Number: 2
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap 0
BackupTFPortMap 15
SymbolicName   Port2
```

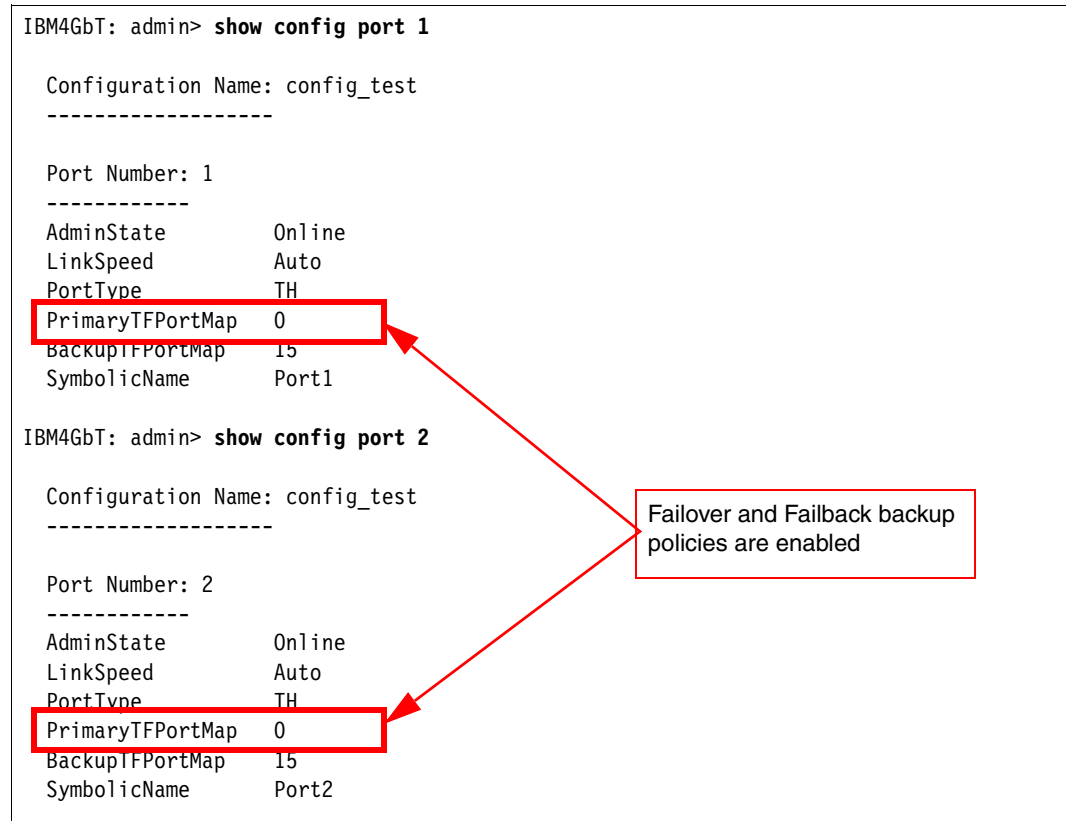


Figure 2-7 The show config port command

To enable or disable those two settings, use the commands shown in Figure 2-8 to Figure 2-11.

Specifying the value 0 or 15 in this example enables the policies, but putting the character N disables the value as shown in the red box in Figure 2-8.

```
IBM4GbT: admin> admin start

IBM4GbT (admin): admin> config edit

The config named config_test is being edited.

IBM4GbT (admin-config): admin> set config ports internal

A list of attributes with formatting and current values for the port
number or port type specified at the command line will follow.
Each value that is changed will be set for ALL INTERNAL PORTS.
If you wish to terminate this process before reaching the end of the
list press 'q' or 'Q' and the ENTER key to do so.

Configuring all internal ports (displaying values from port number: 1)
-----

AdminState      (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
LinkSpeed       (2=2Gb/s, 4=4Gb/s, A=Auto)             [Auto ]
PrimaryTFPortMap (decimal value for port, N=no mapping)           [0   ] N
BackupTFPortMap  (decimal value for port, N=no mapping)       [15  ] N

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

IBM4GbT (admin-config): admin> config save

The config named config_test has been saved.

IBM4GbT (admin): admin> config activate

The currently active configuration will be activated.
Please confirm (y/n): [n] y

IBM4GbT (admin): admin> admin end
```

Set the value to N to disable the policies.

Figure 2-8 Disable the FO and FB policies

Figure 2-9 shows the result of disabling the FO and FB policies.

```
IBM4GbT: admin> show config port 1

Configuration Name: config_test
-----

Port Number: 1
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap None
BackupTFPortMap None
SymbolicName   Port1

IBM4GbT: admin> show config port 2

Configuration Name: config_test
-----

Port Number: 2
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap None
BackupTFPortMap None
SymbolicName   Port2
```

The image shows two terminal outputs for 'show config port 1' and 'show config port 2'. In both outputs, the lines 'PrimaryTFPortMap None' and 'BackupTFPortMap None' are enclosed in red rectangular boxes. Red arrows originate from a central box on the right labeled 'Result from disable the FO and FB policies' and point to these two lines in both configurations.

Figure 2-9 Actual result of disabling the FO and FB policies

To make sure that the FO and FB policies are enabled, see the commands shown in Figure 2-10.

```
IBM4GbT: admin> admin start

IBM4GbT (admin): admin> config edit

The config named config_test is being edited.

IBM4GbT (admin-config): admin> set config ports internal

A list of attributes with formatting and current values for the port
number or port type specified at the command line will follow.
Each value that is changed will be set for ALL INTERNAL PORTS.
If you wish to terminate this process before reaching the end of the
list press 'q' or 'Q' and the ENTER key to do so.

Configuring all internal ports (displaying values from port number: 1)
-----

AdminState      (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
LinkSpeed       (2=2Gb/s, 4=4Gb/s, A=Auto) [Auto ]
PrimaryTFPortMap (decimal value for port, N=no mapping) [None ] 0
BackupTFPortMap (decimal value for port, N=no mapping) [None ] 15

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

IBM4GbT (admin-config): admin> config save

The config named config_test has been saved.

IBM4GbT (admin): admin> config activate

The currently active configuration will be activated.
Please confirm (y/n): [n] y

IBM4GbT (admin): admin> admin end
```

Set the value to 0 and 15 to enable the policies

Figure 2-10 Enable the FO and FB policies

Figure 2-11 shows the actual result of enabling the FO and FB policies.

```
IBM4GbT: admin> show config port 1

Configuration Name: config_test
-----

Port Number: 1
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap 0
BackupTFPortMap 15
SymbolicName   Port1

IBM4GbT: admin> show config port 2

Configuration Name: config_test
-----

Port Number: 2
-----
AdminState      Online
LinkSpeed      Auto
PortType       TH
PrimaryTFPortMap 0
BackupTFPortMap 15
SymbolicName   Port2

IBM4GbT: admin>
```




Figure 2-11 Actual result of enabling the FO and FB policies

2. We disconnected 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 are distributed among the remaining online N_Ports.

The show port command in Figure 2-12 shows the mapping after the failover.

```
IBM4GbT: admin> show port 0

Port Number: 0
-----
ActiveTHPortList None
AdminState Offline
AsicNumber 0
AsicPort 0
ConfigType TF
DiagStatus Passed
EpConnState None
EpIsoReason NotApplicable
Licensed True
LinkSpeed 2Gb/s
LinkState Inactive
LoginStatus NotLoggedIn
MaxCredit 8
MediaSpeeds 1Gb/s, 2Gb/s
OperationalState Offline
PerfTuningMode Normal
PortWWN 20:00:00:c0:dd:0d:35:bc
RunningType TF
MediaPartNumber JSP-21S0AA1
MediaRevision
MediaType 200-M5-SN-I
MediaVendor JDS UNIPHASE
MediaVendorID 0000019c
SymbolicName Port0
SyncStatus SyncAcquired
XmitterEnabled True

IBM4GbT: admin> show port 15

Port Number: 15
-----
ActiveTHPortList 1,2,3
AdminState Online
AsicNumber 0
AsicPort 1
ConfigType TF
DiagStatus Passed
EpConnState None
EpIsoReason NotApplicable
Licensed True
LinkSpeed 2Gb/s
LinkState Active
LoginStatus LoggedIn
MaxCredit 8
MediaSpeeds 1Gb/s, 2Gb/s
OperationalState Online
PerfTuningMode Normal
PortWWN 20:0f:00:c0:dd:0d:35:bc
RunningType TF
MediaPartNumber JSP-21S0AA1
MediaRevision
MediaType 200-M5-SN-I
MediaVendor JDS UNIPHASE
MediaVendorID 0000019c
SymbolicName Port15
SyncStatus SyncAcquired
XmitterEnabled True
```

Figure 2-12 The show port command

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

Note: The failover and failback processes are 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.



Implementation

IBM BladeCenter technology is designed to deliver great performance along with simplicity, flexibility and scalability. All related technologies, including the QLogic 4 Gb Intelligent Pass-thru Module, are built in the same fashion. The Intelligent Pass-thru Module is designed to be implemented in a simple, flexible, and scalable way.

This chapter explains how to implement the Intelligent Pass-thru Module in a typical SAN environment. The implementation steps are delivered in samples taken from our labs.

In this chapter, we discuss the following topics:

- ▶ 3.1, “Tools and environment” on page 32
- ▶ 3.2, “Setting up the blade server” on page 34
- ▶ 3.3, “Setting up the Intelligent Pass-thru Module” on page 36
- ▶ 3.4, “Setting up the external switch” on page 51
- ▶ 3.5, “Configuring the connection” on page 66

3.1 Tools and environment

This section discusses the tools that we used and the environment that we set up in our lab to test the Intelligent Pass-thru Module implementation.

3.1.1 Tools

We used two types of tools to implement the Intelligent Pass-thru Module: the graphical user interface (GUI) and command-line interface (CLI). We demonstrate the use of both of these tools in most steps.

GUI tools

We use the GUI tools in the following tasks:

- ▶ Setting up and configuring the BladeCenter chassis through the BladeCenter Advance Management Module (AMM) Web interface
- ▶ Setting up and configuring IPM through QuickTools™
- ▶ Setting up and configuring external switches through the Web interface (for example, Web Tools for Brocade switch)

Workstation requirements for all GUI tools that we used in our example are usually basic. Table 3-1 lists the requirements for fabric management workstation running QuickTools.

Table 3-1 QuickTools workstation requirements

Items	Requirements
Operating System	Windows 2003 and XP SP1/SP2
	Solaris™ 9, 10, and 10 x86
	Red Hat Enterprise Linux 3, 4
	SUSE Linux Enterprise Server 9 and 10
Memory	256 MB or more (512MB or more recommended)
Disk Space	150 MB per installation
Processor	1 GHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet Browser	Microsoft® Internet Explorer® 5.0 and later
	Netscape Navigator 6.0 and later
	Mozilla 1.5 and later
	Firefox 1.0 and later
	Java™ 2 Standard Edition Runtime Environment 1.4.2

CLI tools

We used the CLI tools to set up and configure the IPM and external switches as well as to update the firmware. Telnet is a commonly used tool. SSH can be used only to manage external switches that support serial port management connection. Figure 3-1 displays the IPM status that is shown initially after logging in to IPM using Telnet.

```
QLOGIC4GbT login: admin
Password:

Establishing connection... Please wait.

*****
*                                     *
*      Command Line Interface SHell  (CLISH)      *
*                                     *
*****

SystemDescription  QLogic(R) 4Gb Intelligent Pass Through Module for IBM
BladeCenter(R)
EthNetworkAddress  9.42.162.42 (use 'set setup system' to update)
MACAddress         00:c0:dd:0d:35:8f
WorldWideName     10:00:00:c0:dd:0d:35:8f
ChassisSerialNumber 11S43W6726YK10NY73P525
SymbolicName      QLOGIC4GbT
ActiveSWVersion   V6.5.0.15.0
ActiveTimestamp   Wed May 2 14:43:36 2007
DiagnosticsStatus Passed
LicensedExternalPorts 6
LicensedInternalPorts 14
SwitchMode        Transparent

The alarm log is empty.

Warning: Your user account password has not been changed
         It is strongly recommended that you do so before proceeding
```

Figure 3-1 Initial CLi shell after logging in

3.1.2 Environment

We set up a simple environment in our lab to represent a typical SAN environment at a customer site. Our lab environment consisted of the following devices:

- ▶ BladeCenter chassis
We used a BladeCenter H chassis.
- ▶ BladeCenter servers
We used one HS21 and two LS21 blade servers.
- ▶ Multi-Switch Interconnect Modules
We used two Multi-Switch Interconnect Modules attached to Bay 8 and Bay 10 of the BladeCenter H.
- ▶ QLogic 4 Gb Intelligent Pass-thru Modules
We attached one module to each Multi-Switch Interconnect Module.

- ▶ External switches
 - We used Brocade 7500, Cisco MDS 9216 and McDATA M6140. We used three different external switches to test the interoperability and manageability of the IPM.
- ▶ Workstation management console

Figure 3-2 shows the environment topology that we built in our lab.

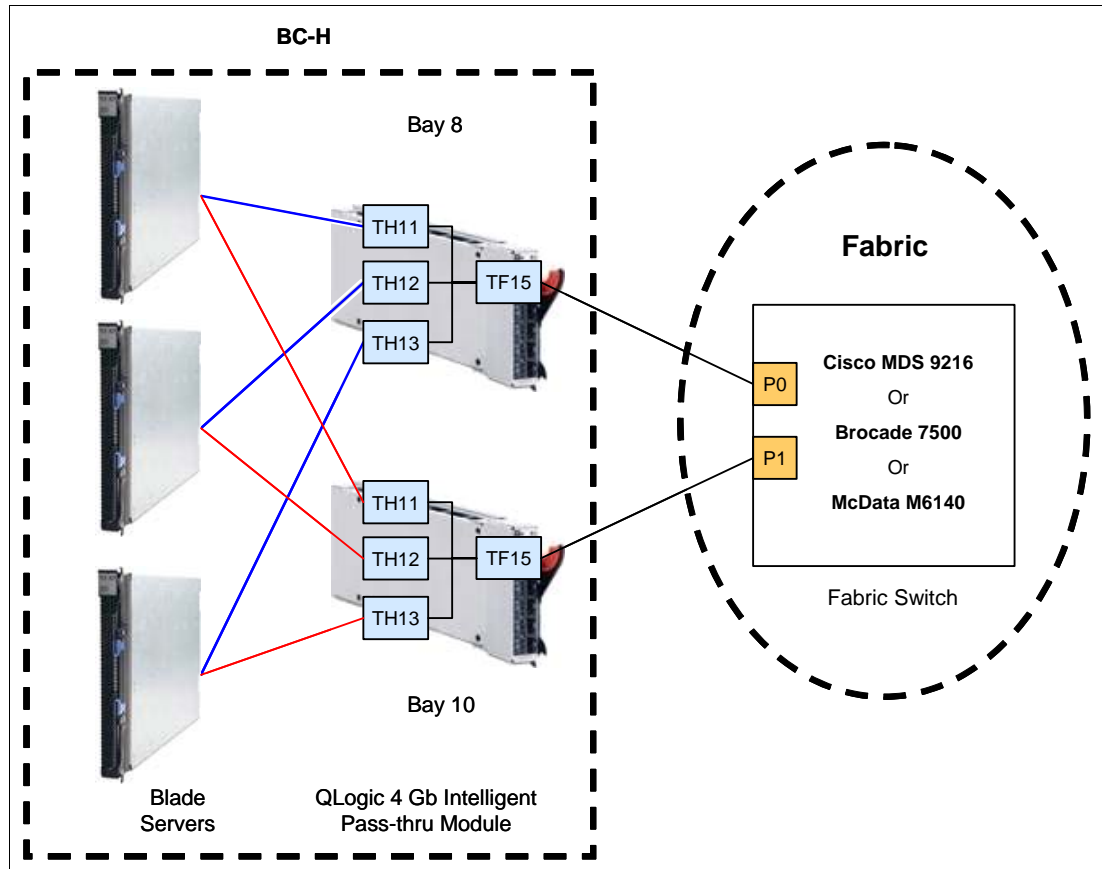


Figure 3-2 Environment topology in our lab

3.2 Setting up the blade server

This section discusses the steps that are required to set up blade servers regarding the IPM implementation.

3.2.1 Install the HBA

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

3.2.2 Manage the HBA

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

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

1. Record the World Wide Port Name (WWPN) of the HBA.

The WWPN is needed to define the storage group, host, and host port in the storage subsystem. It is also needed to configure the zone in the external switches, as shown in Figure 3-3.

```
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 3-3 HBA BIOS

2. Configure the Host Adapter BIOS.

The default value is *Disable*. If you need to configure a Boot from SAN, you have to change the value to *Enabled*, as shown in Figure 3-4.

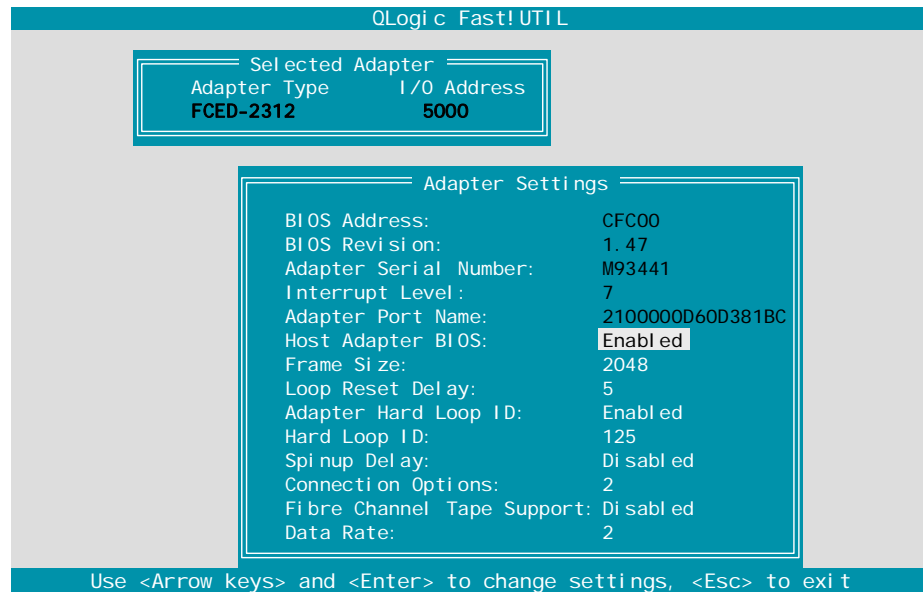


Figure 3-4 Manage the Host Bus Adapter BIOS

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

3.3 Setting up the Intelligent Pass-thru Module

This section discusses the steps required to set up the Intelligent Pass-thru Module.

3.3.1 Insert the IPM into the chassis

You need to attach the module to the correct bay in the BladeCenter chassis. The bay that you choose depends upon the types of chassis and the connectivity devices that you use. Refer to 2.1, “Compatibility” on page 14 for the supported I/O bay and configuration requirements.

3.3.2 Set up the I/O module IP address

We used the BladeCenter AMM Web interface to set up the module IP address. To open the BladeCenter AMM Web interface:

1. On your work station, open a supported browser window. Then, enter the IP address of the AMM in the address field.
2. When prompted, enter the user name and password. By default, the IBM BladeCenter AMM user name is *USERID* and the password is *PASSWORD* (where the “0” here is a *zero*). Both the user name and password defaults are all upper case and both are case sensitive.

There are default IP addresses for the modules, which are based on the bays where they are installed. To change the module IP address:

1. In the I/O Module Task tab, click **Configuration**.
2. Select the bay where you installed the IPM, and change the IP address (Figure 3-5). Then, click **Save**.

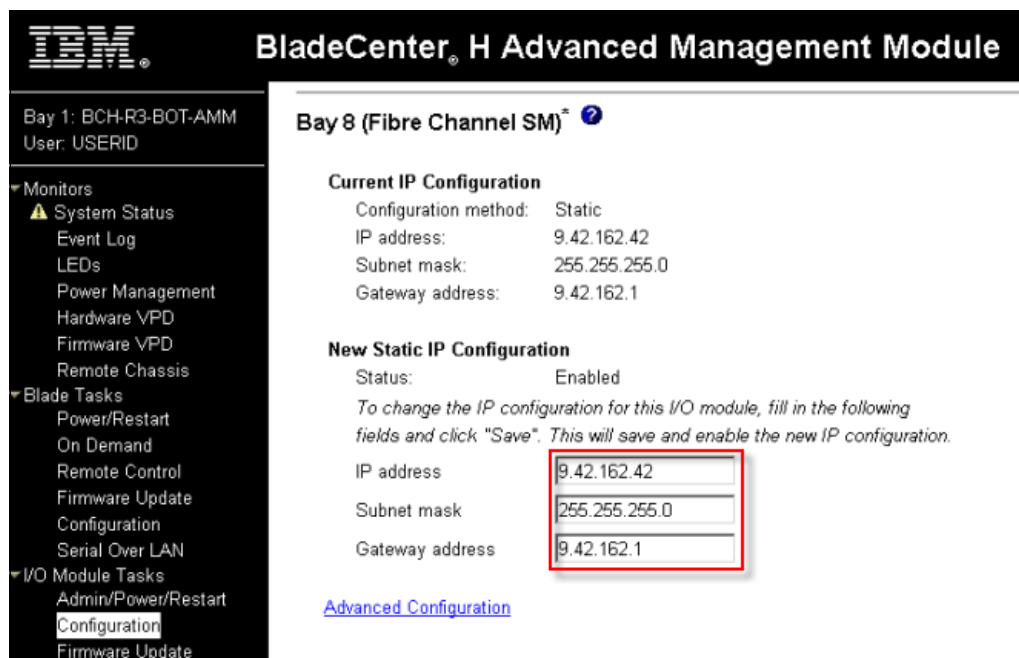


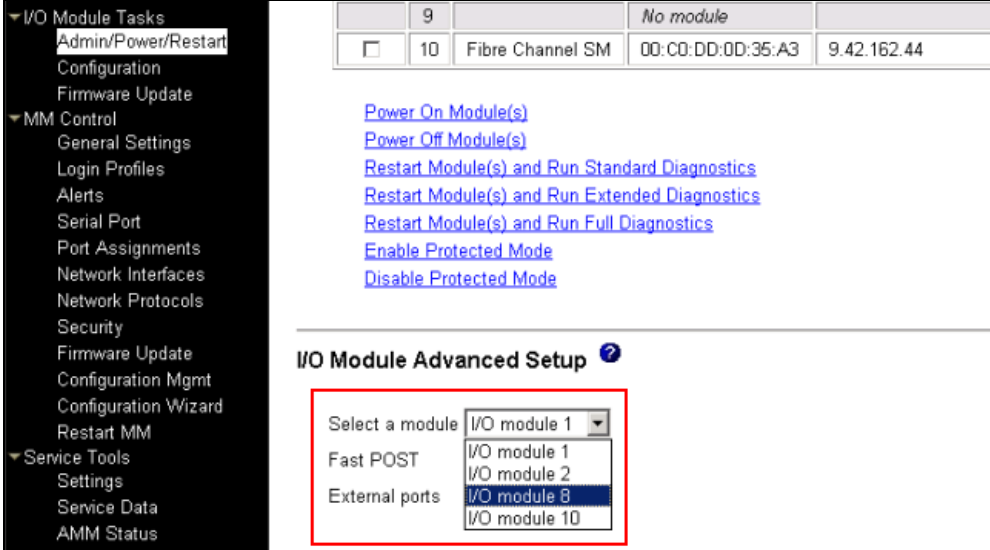
Figure 3-5 Setting the IPM IP address through the BladeCenter AMM

Note: The IP address of the module must be in the same subnet as the IP address of BladeCenter AMM Web interface for communications to be successful.

3.3.3 Enable module external ports

Next, you use the BladeCenter AMM Web interface to enable external ports of the module. Follow these steps:

1. In the I/O Module Task tab, click **Admin/Power/Restart** and select the module based on the bay where you attached the module (Figure 3-6).
2. Ensure that the external ports are set to *Enabled* and click **Save**.



The screenshot displays the BladeCenter AMM web interface. On the left is a navigation menu with categories: I/O Module Tasks, MM Control, and Service Tools. The 'Admin/Power/Restart' option is selected under I/O Module Tasks. The main content area shows a table with columns for checkboxes, module numbers (9, 10), module types (Fibre Channel SM), MAC addresses (00:00:DD:0D:35:A3), and IP addresses (9.42.162.44). Below the table are several blue hyperlinks for power and diagnostic actions. The 'I/O Module Advanced Setup' section is visible, featuring a dropdown menu for 'Select a module' with 'I/O module 1' selected. A red box highlights the 'External ports' dropdown menu, which is open and shows 'I/O module 8' as the selected option.

Figure 3-6 Enable module external port through BladeCenter AMM

3.3.4 Verify and update module firmware level

It is recommended that you run modules on the latest firmware level. To verify and update the module firmware, you can use either a Telnet session (CLI) or QuickTools (GUI).

Using Telnet (CLI) session

To open a Telnet session and update the IPM firmware through a CLI:

1. From a command line, open a Telnet session with the IP address of the IPM.
2. Enter the user name and password at the login prompt. By default, the login name is *USERID* and the password is *PASSWORD* (where the "0" here is a *zero*).

Figure 3-7 shows the initial display after logging in to the module successfully.

```
QLOGIC4GbT login: admin
Password:

Establishing connection... Please wait.

*****
*
*      Command Line Interface SHell  (CLISH)
*
*****

SystemDescription  QLogic(R) 4Gb Intelligent Pass Through Module for IBM
BladeCenter(R)
EthNetworkAddress  9.42.162.42 (use 'set setup system' to update)
MACAddress         00:c0:dd:0d:35:8f
WorldWideName      10:00:00:c0:dd:0d:35:8f
ChassisSerialNumber 11S43W6726YK10NY73P525
SymbolicName       QLOGIC4GbT
ActiveSWVersion    V6.5.0.15.0
ActiveTimestamp    Wed May 2 14:43:36 2007
DiagnosticsStatus  Passed
LicensedExternalPorts 6
LicensedInternalPorts 14
SwitchMode         Transparent

The alarm log is empty.

Warning: Your user account password has not been changed
         It is strongly recommended that you do so before proceeding
```

Figure 3-7 Initial CLI display after login to the Intelligent Pass-thru Module

- To verify the firmware version of the module, enter the **show version** command to display a summary of I/O module identity information including the firmware version (Figure 3-8).

```

QLOGIC4GbT: admin> show version

*****
*                                     *
*      Command Line Interface SHell   (CLISH)   *
*                                     *
*****

SystemDescription  QLogic(R) 4Gb Intelligent Pass Through Module for IBM
BladeCenter(R)
EthNetworkAddress  9.42.162.42 (use 'set setup system' to update)
MACAddress         00:c0:dd:0d:35:8f
WorldWideName     10:00:00:c0:dd:0d:35:8f
ChassisSerialNumber 11S43W6726YK10NY73P525
SymbolicName      QLOGIC4GbT
ActiveSWVersion   V6.5.0.15.0
ActiveTimestamp   Wed May  2 14:43:36 2007
DiagnosticsStatus Passed
LicensedExternalPorts 6
LicensedInternalPorts 14
SwitchMode        Transparent

```

Figure 3-8 The show version command

To upgrade the firmware version of the module:

- Enter the **admin start** command and continue with the **firmware install** command (Figure 3-9).

```

IBM4GbT: USERID> admin start

IBM4GbT (admin): USERID> firmware install

The switch will be reset. This process will cause a disruption
to I/O traffic.

Continuing with this action will terminate all management sessions,
including any Telnet sessions. When the firmware activation is complete,
you may log in to the switch again.

Do you want to continue? [y/n]: y

Press 'q' and the ENTER key to abort this command.

```

Figure 3-9 The firmware install command

- Enter your choice for the file transfer protocol (FTP) with which to download the firmware image file. FTP requires a user account and password, while TFTP does not (Figure 3-10).

```

FTP or TFTP      : ftp

```

Figure 3-10 Choosing the file transfer protocol

3. Enter your account name on the remote host (FTP only) and the IP address of the remote host. When prompted for the source file name, enter the path of the firmware image file (Figure 3-11).

```
User Account      : rizan
IP Address       : 9.42.170.200
Source Filename  : 6.5.0.17.00_ipc
```

Figure 3-11 Account name and source file name

Tip: If you do not have an FTP server, there are a number of simple TFTP servers available at no charge. An example is tftpd32, which is available from:

<http://tftpd32.jounin.net/>

4. When prompted to install the new firmware, enter yes to continue or no to cancel. Entering yes disrupts the traffic (Figure 3-12).

```
About to install image. Do you want to continue? [y/n] y
Connected to 9.42.170.200 (9.42.170.200).
220 Microsoft FTP Service
```

Figure 3-12 Confirmation to install the new firmware version

5. Enter the password of your account name (FTP only), as shown in Figure 3-13.

```
331 Password required for rizan.
Password:
230 User rizan logged in.
```

Figure 3-13 Entering the account name password

6. Wait until the new firmware is downloaded successfully from the remote host, installed, and activated.

Using the QuickTools GUI

To use QuickTools to check and update the IPM firmware:

1. On your workstation, open a supported browser window, and enter the module IP address in the address field.
2. Enter a login name and password, as shown in Figure 3-14. By default, the login name is *USERID* and the password is *PASSWORD* (where the “0” here is a *zero*).



Figure 3-14 Add New Fabric dialog box

After the Add New Fabric dialog box, QuickTools opens, as shown in Figure 3-15.

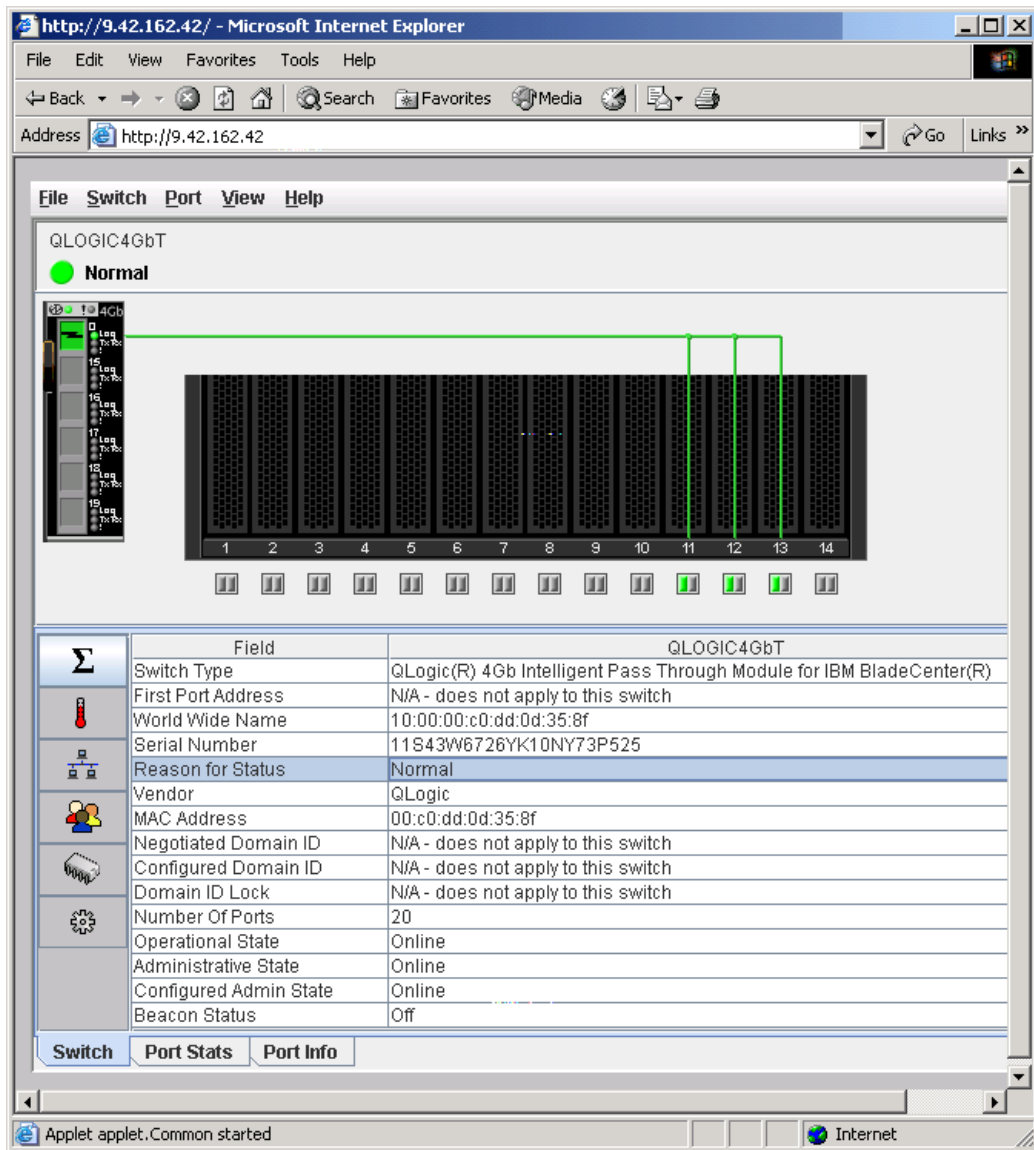


Figure 3-15 QuickTools initial interface

To verify the firmware version using QuickTools:

1. In main window, go to the Switch tab.
2. Click the **Firmware** icon (a chip). The firmware version displays as shown in Figure 3-16.

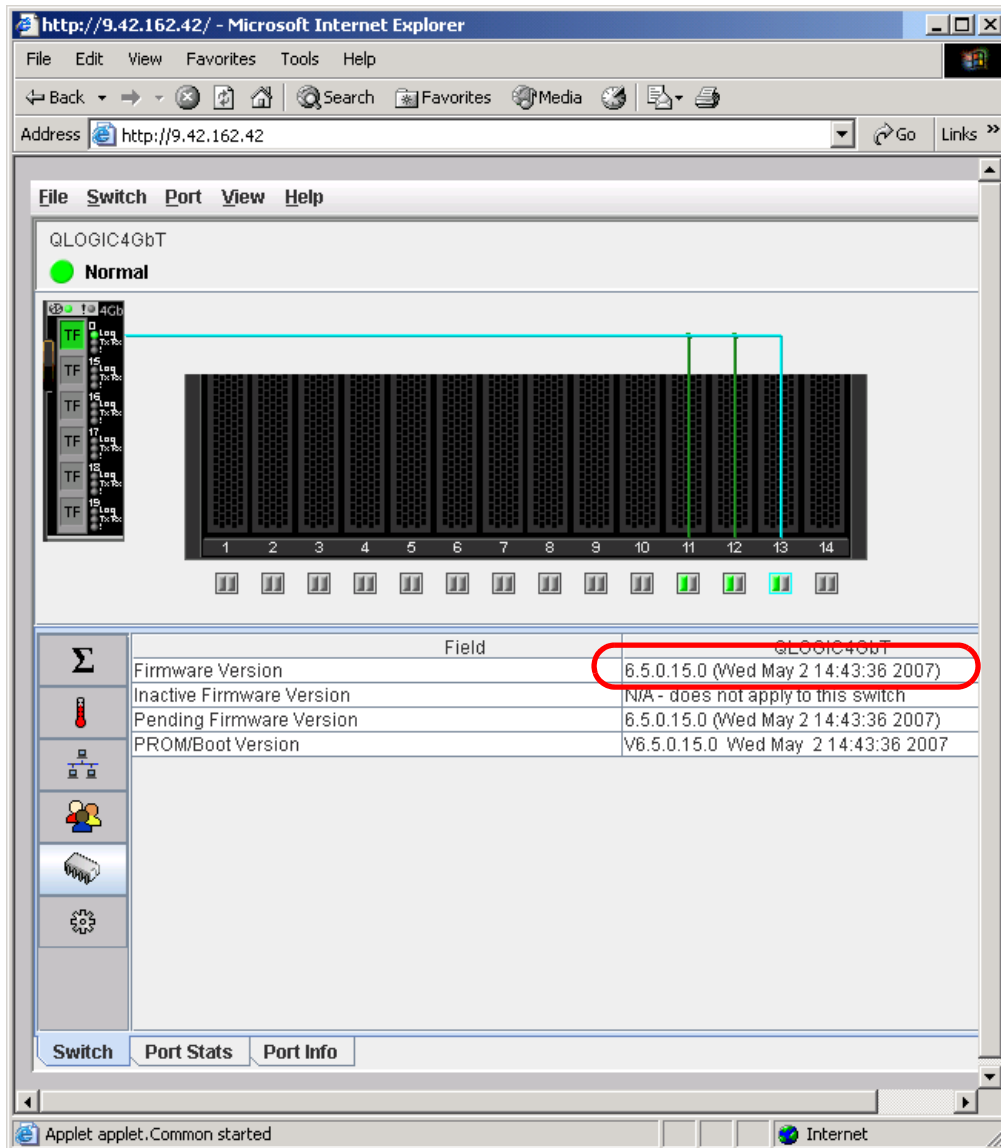


Figure 3-16 Verify firmware version using QuickTools

To upgrade the firmware using QuickTools:

1. Click **Switch** → **Load Firmware**.
2. In the Firmware Upload dialog box, shown in Figure 3-17, browse the firmware image and click **Start**.

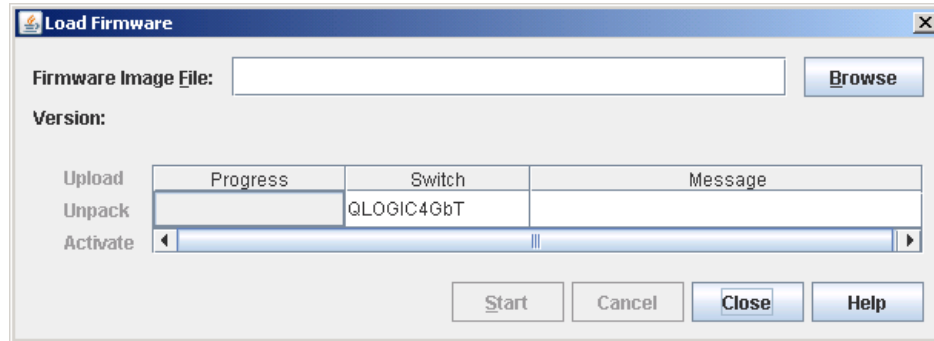


Figure 3-17 Browse the firmware image and start loading

3. Click **OK** to reset the module and activate the new firmware. QuickTools prompts you to activate the new firmware using the hot (nondisruptive) reset, if possible.

3.3.5 Verify and modify module port status

To verify and modify the port status, you can use either a Telnet session (CLI) or QuickTools (GUI).

Note: Server bay ports always be TH_Ports. External ports must be configured as TF_Ports when connect to fabric ports and as TH_Ports when connect to external hosts. By default, all external ports are TF_Ports.

Using Telnet (CLI) session

Enter the **show config port** command to display the port configuration parameters. For example, Figure 3-18 shows the configuration parameter of Port 0.

```
IBM4GbT (admin): admin> show config port 0

Configuration Name: config_test
-----

Port Number: 0
-----

AdminState      Online
LinkSpeed       Auto
PortType        TF
SymbolicName    Port0
```

Figure 3-18 The show config port command

Enter the **show port** command to display port operational information. For example, Figure 3-19 shows the port operational information of Port 0.

```

IBM4GbT (admin): admin> show port 0

Port Number: 0
-----
ActiveTHPortList None           MediaSpeeds      Unknown
AdminState      Online           OperationalState Offline
AsicNumber      0               PerfTuningMode   Normal
AsicPort        0               PortWWN          20:00:00:c0:dd:0d:35:bc
ConfigType      TF              RunningType      TF
DiagStatus      Passed          MediaPartNumber  Unknown
EpConnState     None            MediaRevision    Unknown
EpIsoReason     NotApplicable  MediaType        NotInstalled
Licensed        True            MediaVendor      Unknown
LinkSpeed       Auto            MediaVendorID    Unknown
LinkState       Inactive        SymbolicName     Port0
LoginStatus     NotLoggedIn    SyncStatus       SyncLost
MaxCredit       8              XmitterEnabled   True

ALInit          0               LIP_F8_F7       0
ALInitError     0               LinkFailures     0
BadFrames       0               Login            0
BBCR_FrameFailures 0           Logout           0
BBCR_RRDYFailures 0           LongFramesIn     0
Class2FramesIn  0               LoopTimeouts     0
Class2FramesOut 0               LossOfSync       0
Class2WordsIn   0               LostFrames       0
Class2WordsOut  0               LostRRDYs        0
Class3FramesIn  0               PrimSeqErrors    0
Class3FramesOut 0               RxLinkResets     0
Class3Toss      0               RxOfflineSeq     0
Class3WordsIn   0               ShortFramesIn    0
Class3WordsOut  0               TotalErrors      0
DecodeErrors    0               TotalLinkResets  0
EpConnects     0               TotalLIPsRecvd   0
FBusy          0               TotalLIPsXmitd   0
FlowErrors      0               TotalOfflineSeq  1
FReject         0               TotalRxFrames    0
InvalidCRC      0               TotalRxWords     0
InvalidDestAddr 0               TotalTxFrames    0
LIP_AL_PD_AL_PS 0               TotalTxWords     0
LIP_F7_AL_PS    0               TxLinkResets     0
LIP_F7_F7       0               TxOfflineSeq     1
LIP_F8_AL_PS    0

```

Figure 3-19 The show port command

You can modify the port status by either making permanent changes or temporary changes. Use the **set config port** command to make permanent changes. These changes are saved in the active configuration and are preserved across I/O module or port resets. The **set port** command makes temporary changes that apply until the next port or I/O module reset, or until you activate a configuration.

To modify the port status:

1. Enter the **admin start** command and continue.
2. Enter the **config edit** command.
3. Enter the **set port command** or the **set config port** command.
4. Enter the new value or press Enter to accept the current value.
5. Enter the **config save** command.
6. Enter the **config activate** command.

Figure 3-20 shows how to configure the Port 0 permanently.

```
QLogic4GbT #> admin start
QLogic4GbT (admin) #> config edit
QLogic4GbT (admin-config) #> set config port 0
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number: 0
  -----
  AdminState (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online] offline
  LinkSpeed (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto) [Auto ]
  PortType (TH / TF) [TF ]
  SymPortName (string, max=32 chars) [Port0 ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
  QLogic4GbT (admin-config) #> config save
  QLogic4GbT (admin-config) #> config activate

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
  QLogic4GbT (admin-config) #> config save
  QLogic4GbT (admin-config) #> config activate
```

Figure 3-20 The set config port command

Using the QuickTools GUI

To verify the port status:

1. From main menu, go to the Port Info tab, then go to the Summary tab.
2. Click the port to view.

Figure 3-21 shows the status of Port 13 of the module. It shows that the Port 13 is currently online and configured as a TH_Port.

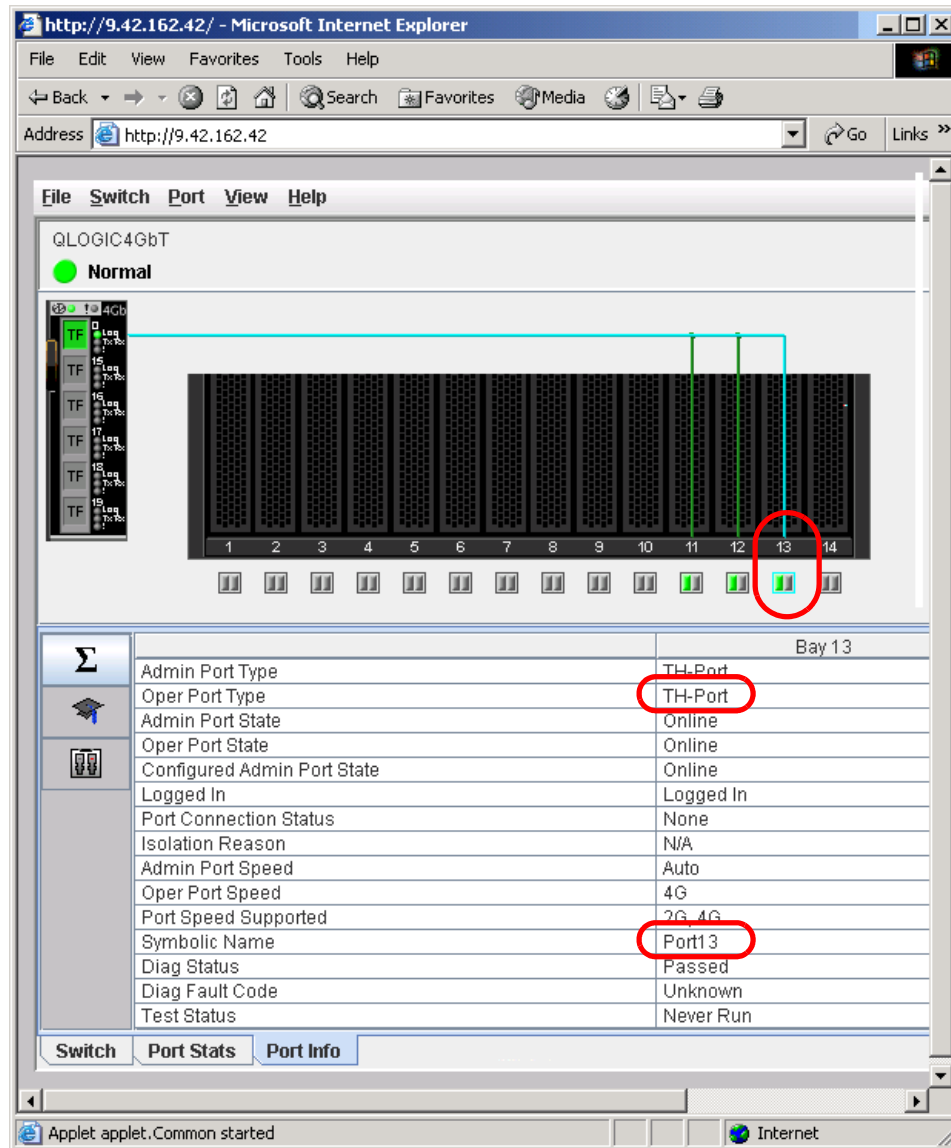


Figure 3-21 Verify port status through QuickTools

To modify the port status:

1. From the main menu, click the port to modify.
2. Click **Port** → **Port Properties**.
3. From Port Properties dialog box, you can modify Port States, Port Speed, and Port Type from three different pull-down menus as shown in Figure 3-22.

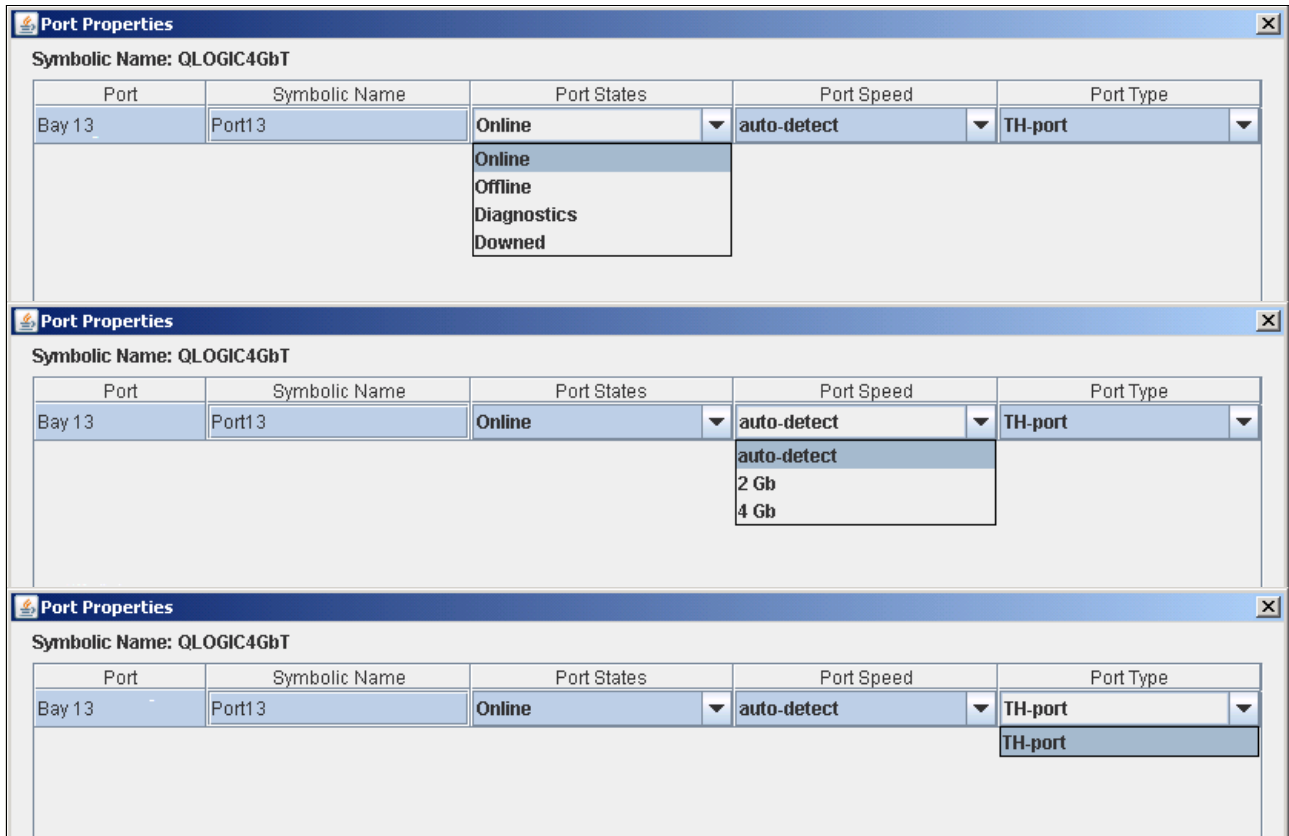


Figure 3-22 Configure the port state, port speed, and port type

3.3.6 Verify and modify module port mapping

Using mapping, you can assign a TH_Port to multiple TF_Ports. For redundancy purposes, a backup port mapping can also be specified. A TH_Port can be mapped to multiple primary and secondary ports. A port designated as primary will be the first path chosen. If there are multiple primary ports, the TH_Ports are distributed (using algorithm) across the TF_Ports. Backup ports only become active when all primary ports fail.

Tip: Leaving a TH_Port unmapped has the same effect as unplugging a Fibre Channel cable.

To verify and modify the port mapping, you can use either Telnet session (CLI) or QuickTools (GUI).

Using Telnet (CLI) session

Enter the **show config port** command to display the port mapping. Figure 3-23 shows that Port 1 is mapped to Port 0 as primary map and to Port 15 as backup map.

```
IBM4GbT: USERID> show config port 1
```

```
Configuration Name: config_test
```

```
-----
```

```
Port Number: 1
```

```
-----
```

```
AdminState      Online
```

```
LinkSpeed       Auto
```

```
PortType        TH
```

```
PrimaryTFPortMap 0
```

```
BackupTFPortMap 15
```

```
SymbolicName    Port1
```

Figure 3-23 Display port mapping using show config port command

To modify the port mapping:

1. Enter the **admin start** command.
2. Enter the **config edit** command.
3. Enter the **set config ports** command.
4. Enter the new value or press Enter to accept the current value.
5. Enter the **config save** command.
6. Enter the **config activate** command.

Figure 3-24 shows how to map all internal ports to Port 0 and Port 16 as primary map and to Port 17, Port 18, and Port 19 as backup map.

```
IBM4GbT: USERID> admin start

IBM4GbT (admin): USERID> config edit

The config named config_test is being edited.
IBM4GbT (admin-config): USERID> set config ports internal

A list of attributes with formatting and current values for the port
number or port type specified at the command line will follow.
Each value that is changed will be set for ALL INTERNAL PORTS.
If you wish to terminate this process before reaching the end of the
list press 'q' or 'Q' and the ENTER key to do so.

Configuring all internal ports (displaying values from port number: 1)
-----

AdminState      (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
LinkSpeed       (2=2Gb/s, 4=4Gb/s, A=Auto)                [Auto ]
  PrimaryTFPortMap (decimal value for port, N=no mapping) [0    ] 0,16
  BackupTFPortMap (decimal value for port, N=no mapping) [15   ] 17,18,19

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

IBM4GbT (admin-config): USERID> config save

The config named config_test has been saved.

IBM4GbT (admin): USERID> config activate

The currently active configuration will be activated.
Please confirm (y/n): [n] y

IBM4GbT (admin): USERID> admin end
```

Figure 3-24 Modify the port mapping

Using the QuickTools GUI

You can verify the working port mapping by clicking the TF port in the main menu and looking at the connection line in graphical representation of the switch.

Figure 3-25 shows that Port 11, Port 12, and Port 13 are currently mapped to Port 0.

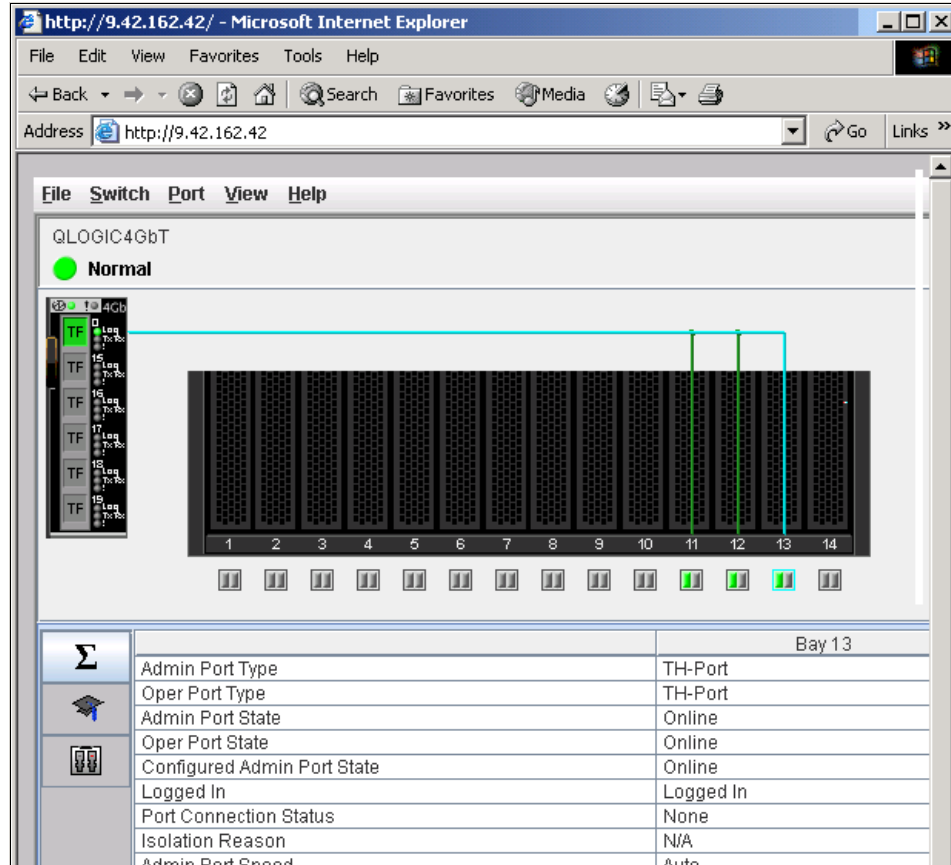


Figure 3-25 Main menu displays the working port mapping

You can also use Map Ports dialog box to verify and modify the port mapping by following these steps:

1. From the main menu, click **Port** and then select **Map Ports**.
2. Look at the table to verify the port mapping. Then, change the value of the table cell to modify the port mapping.

Figure 3-26 shows a step to modify the mapping of Port 13.

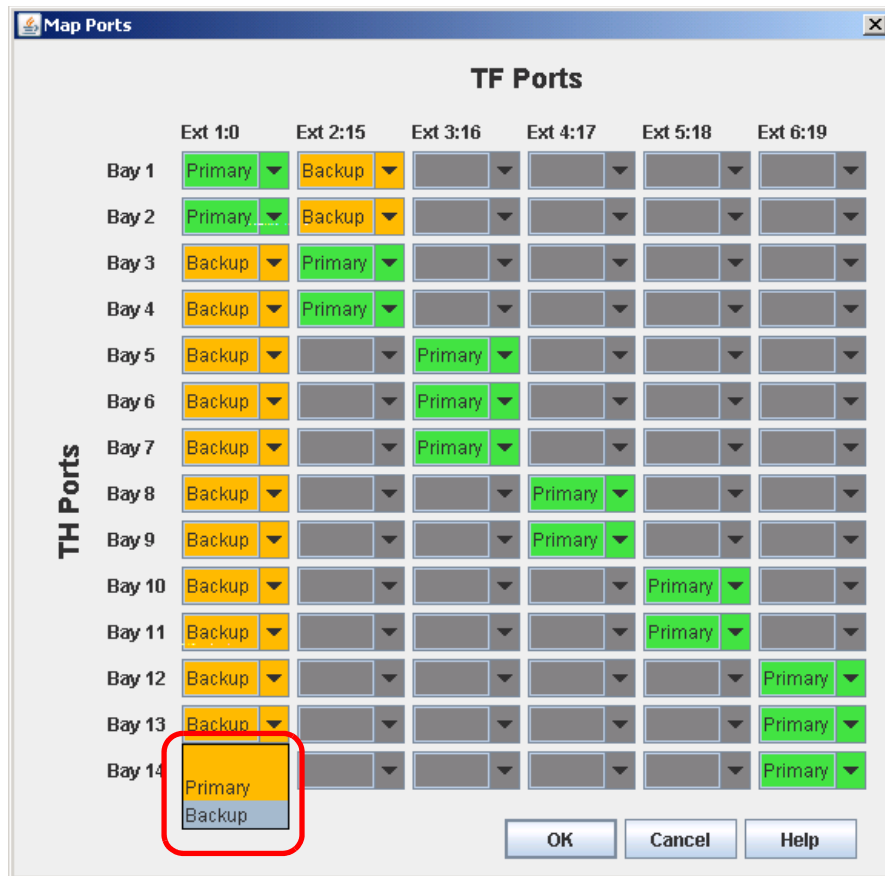


Figure 3-26 Modify the port mapping using Map Ports dialog box

3.4 Setting up the external switch

There are two basic steps to do with the external switch in order to implement the Intelligent Pass-thru Module solution. They ensure that it runs in required firmware version and ensuring that all ports connected to the Intelligent Pass-thru Module are NPIV enabled.

As previously discussed, in our lab we used Cisco MDS 9216, Brocade 7500, and McDATA 6140 Fibre Channel switches to test the interoperability and manageability. This section covers the step to set up those three external switch using both GUI and CLI.

3.4.1 Verify and update switch firmware level

There is minimum requirement of external switch firmware version to communicate with a Intelligent Pass-thru Module. Refer to “Firmware of the Fabric (edge) Switches” on page 17 for information about required firmware versions.

To update the firmware of the external switch, refer to the related documentation of the external switch.

To verify firmware version of the external switch, you can use either a Telnet session (CLI) or a GUI. We describe the steps we took using the switches in our lab.

Using Telnet (CLI) session

You can use a Telnet session to manage all of the switches. There are different login names and passwords applicable for each switch type. Refer to the related switch documentation.

Cisco MDS 9216

Enter the **show version** command to display the firmware version (Figure 3-27).

```
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 3-27 Displaying firmware version of the Cisco MDS 9216

Brocade

Enter the **version** command to display the firmware version (Figure 3-28).

```
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 3-28 Displaying firmware version of the Brocade switch

McDATA

Enter the **show system** command to display the firmware version (Figure 3-29).

```
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 3-29 Displaying firmware version of the McDATA 6140

Using a GUI

You can use a supported browser to manage all of the switches. Refer to the related documentation for detail requirements of browser and other application.

There are different login names and passwords applied on the different switch types. Refer to the related switch documentation for more detail information.

Cisco MDS 9216

To display the firmware version:

1. On your workstation, open a supported browser window, and enter the switch management IP address in the address field.
2. Enter a login name and password, and the Cisco Device Manager opens, as shown in Figure 3-30.

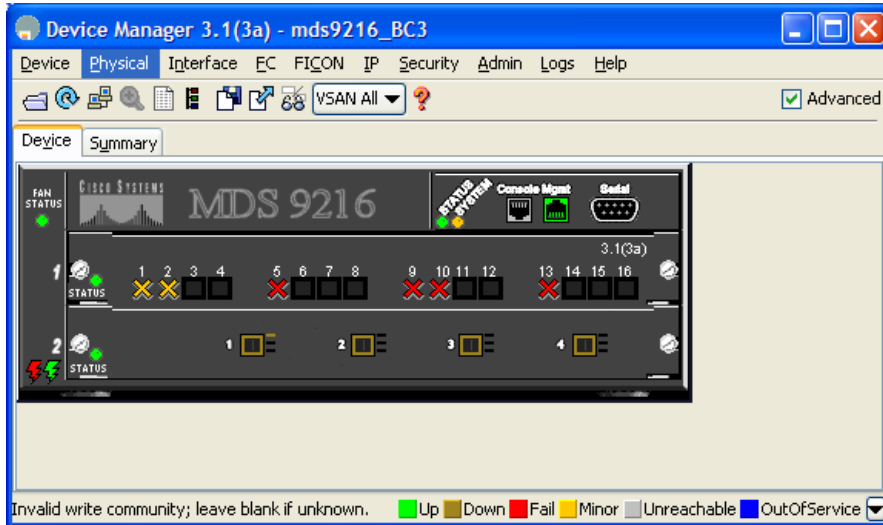


Figure 3-30 Cisco Device Manager main interface

3. From the main menu, click **Physical** → **System**. The firmware version displays in the Description field as shown in Figure 3-31.

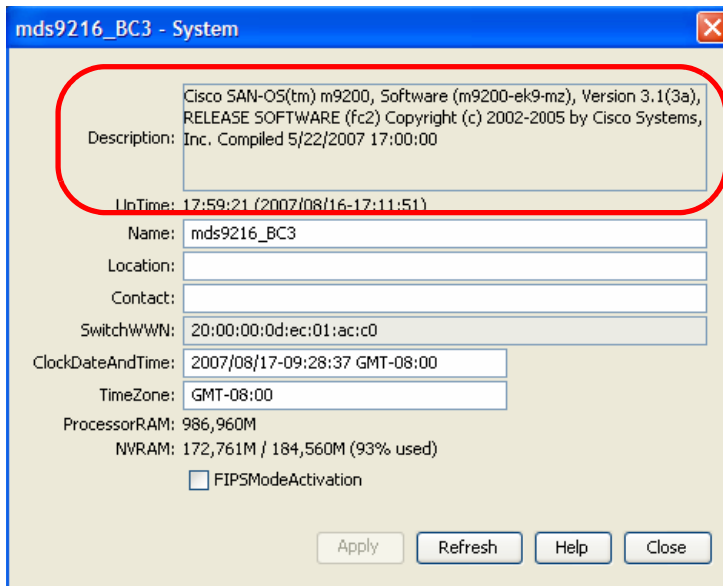


Figure 3-31 Displaying the firmware version of the Cisco MDS 9216

Brocade

To display the firmware version:

1. On your workstation, open a supported browser window, and enter the switch management IP address in the address field.
2. Enter a login name and password.
3. The firmware version displays as the **Fabric OS version** in the main interface, as shown in Figure 3-32.

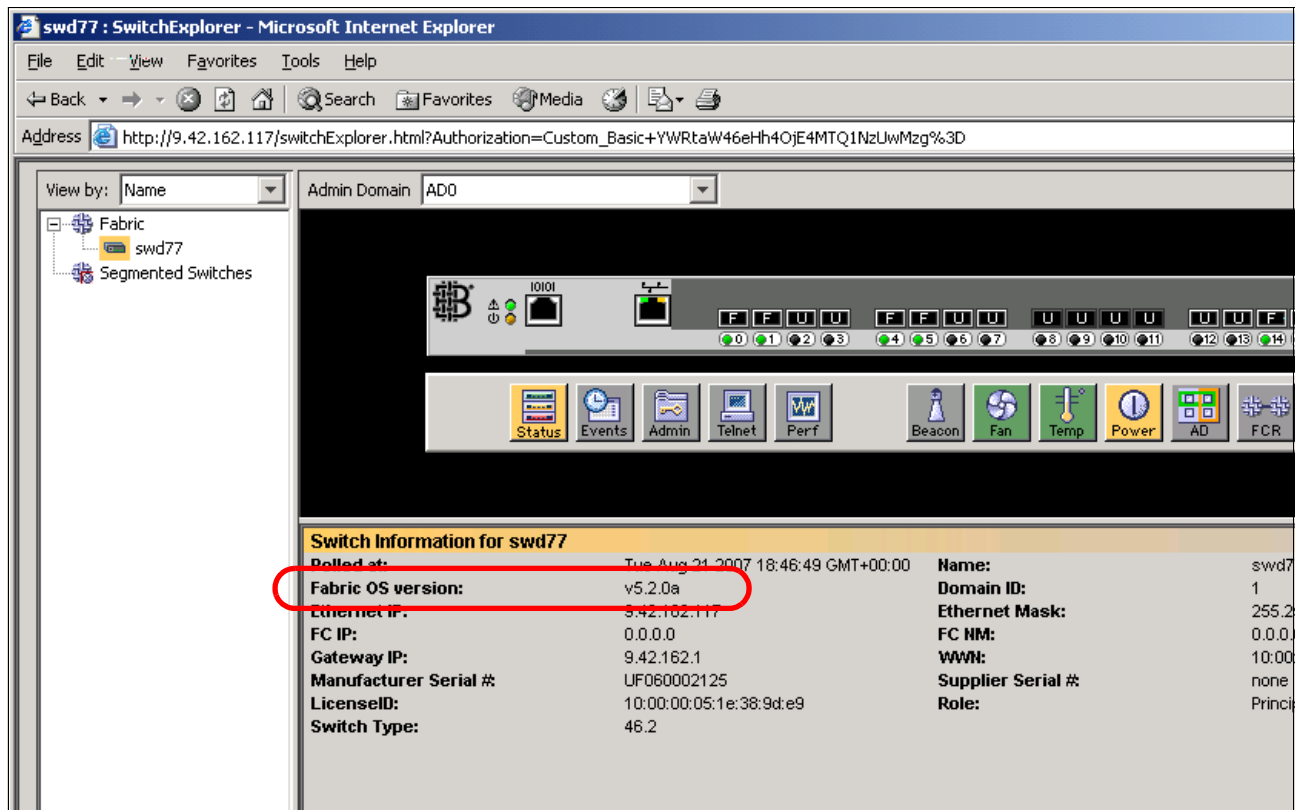


Figure 3-32 Displaying firmware version of the Brocade switch

McDATA

To display the firmware version:

1. On your workstation, open a supported browser window, and then enter the switch management IP address in the address field.
2. Enter a login name and password.
3. The firmware version displays as the **Firmware Level** in the main interface (Figure 3-33).

The screenshot displays the EFCM™ Basic Edition web interface for a McData switch. The top navigation bar includes 'Fabric', 'Product', 'Configure', 'Security', 'Logs', 'Maintenance', 'Upgrade', and 'Help'. The main content area is titled 'Product > Hardware' and features two images: a 'Front View' and a 'Rear View' of the switch. Below the images is a table of attributes:

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

Figure 3-33 Displaying firmware version of the McDATA switch

3.4.2 Enable NPIV

Each port of an external switch which is connected to the QLogic 4 Gb Intelligent Pass-thru Module has to be NPIV enabled.

To verify and to enable the NPIV feature, you can use either a Telnet session (CLI) or a GUI.

Using Telnet (CLI) session

You can use a Telnet session to manage the switch. There are different login names and passwords applied on the different switch types. Refer to the related switch documentation

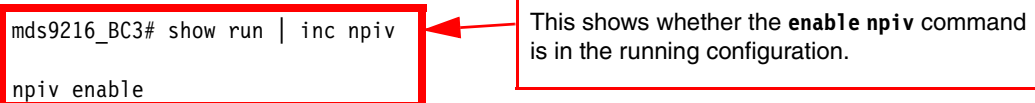
Cisco MDS 9216

It is currently not possible to show the NPIV enable status on a specific port or host. However, you can show it is configured using CLI commands as we describe in this section.

Examples of commands in this section describe each of the NPIV capabilities. Figure 3-34 indicates whether the **enable npiv** command is in the running configuration.

```
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# show run | inc npiv
npiv enable
```



This shows whether the **enable npiv** command is in the running configuration.

Figure 3-34 Displaying NPIV enable of Cisco MDS 9216

Executing the **show int** command indicates the NPIV status of the selected port, where the fiber cable is attached directly from the IPM to the Cisco SAN switch. In our lab, port 2 is the designated port that was used, as indicated in Figure 3-35.

```

mds9216_BC3# show int

fc1/2 is up
  Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
  Port WWN is 20:02:00:0d:ec:01:ac:c0

Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port mode is F, FCID is 0x610006
Port vsan is 100
Speed is 2 Gbps
Transmit B2B Credit is 8
Receive B2B Credit is 16
Receive data field Size is 2112
Beacon is turned off
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 16 bits/sec, 2 bytes/sec, 0 frames/sec
  6 frames input, 288 bytes
  0 discards, 0 errors
  0 CRC, 0 unknown class
  0 too long, 0 too short
  5 frames output, 720 bytes
  0 discards, 0 errors
  0 input OLS, 0 LRR, 1 NOS, 0 loop inits
  2 output OLS, 1 LRR, 0 NOS, 1 loop inits
  16 receive B2B credit remaining
  8 transmit B2B credit remaining
  
```

Figure 3-35 NPIV status on port 2

To complete the NPIV capability on this switch, the **show flogi database** command indicates which hosts are logged in from which port as shown in Figure 3-36.

```

mds9216_BC3# show flogi database

-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/2      100    0x610006     20:00:00:c0:dd:0d:36:3f  10:00:00:c0:dd:0d:36:3f

Total number of flogi = 1.
  
```

Figure 3-36 The show flogi database command

Enter the **config terminal** command to enable configuration mode. Configuration mode has to be enabled to enable NPIV feature.

Enter the **npiv enable** command to enable NPIV capability on all ports of the switch. Enabling NPIV on individual port basis is not possible.

Figure 3-37 shows how to enable NPIV capability in a Cisco MDS 9216.

```
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 3-37 Enable NPIV capability of the Cisco MDS 9216

Brocade

Enter the **portcfgshow** command to display the NPIV capability.

Enter the **portcfgnpivport** command to enable the NPIV capability of an individual port.

Note: The syntax of the **portcfgnpivport** command is as follows:

```
portcfgnpivport [Slot/PortNumber], [Mode]
```

where:

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

Figure 3-38 shows how to enable NPIV in Port 3 of Slot 0 and the changes made after 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

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

swd77:admin>

```

Figure 3-38 Display and enable NPIV capability of the Brocade switch

McDATA

Enter the **config features show** command to display the NPIV feature in the switch (Figure 3-39).

```
Root> config features show
```

Installed Feature Set	Feature	State	Exp
NPIV	NPIV	Enabled	---
Element Manager License	Element Manager License	Installed	
SANtegrity Binding*	Binding Trial*	Disabled	
SANtegrity Authentication*	SANtegrity Auth Trial*	Disabled	
Open Trunking*	Open Trunking Trial*	Disabled	

* - Trial license is available for this feature

Figure 3-39 Displaying NPIV feature in the McDATA switch

Enter the **show NPIV config** command to display the NPIV configuration on each port.

Enter the **config features NPIV** command to enable NPIV capability on all ports of the switch. Enabling NPIV on individual port basis is not possible.

Note: The syntax of the **config features** command is;

```
config features NPIV [Mode]
```

where:

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

Enter the **config NPIV maxPortIDs** command to configure the maximum number of virtual connection allowed to access the particular port.

Note: The syntax of the **config NPIV maxPortIDs** command is:

```
config NPIV maxPortIDs [PortNumber] [MaximumVirtualConnections]
```

Figure 3-40 shows how to enable NPIV and how to configure 10 maximum virtual connections (NPIV logins) on Port 0.

```
Root> config features NPIV 1
Root>

Root> config NPIV maxPortIDs 0 10
Root>

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

Figure 3-40 Enable, configure, and display NPIV of the McDATA switch

Using the GUI

You can use a Web browser to manage the Brocade and McDATA switches.

Cisco MDS 9216

There is currently no browser-based option to view the status of NPIV. You need to use the CLI commands as described in “Cisco MDS 9216” on page 57.

Brocade

To verify the NPIV feature of a port:

1. On your workstation, open a supported browser window, and then enter the switch management IP address in the address field.
2. Enter a login name and password.
3. In the main interface, click the port icon to open the Port Administration Service window.
4. In the General tab, you can verify the NPIV capability as shown in the NPIV Enabled value (see Figure 3-41 on page 63).

To enable the NPIV feature in a port:

1. Open the Port Administration Service window.
2. Click **Enable NPIV** in the grey selection bar at the top to enable the NPIV feature of the port. Click **Disable NPIV** to disable it.

Figure 3-41 shows that the NPIV feature of Port 0 is enabled.

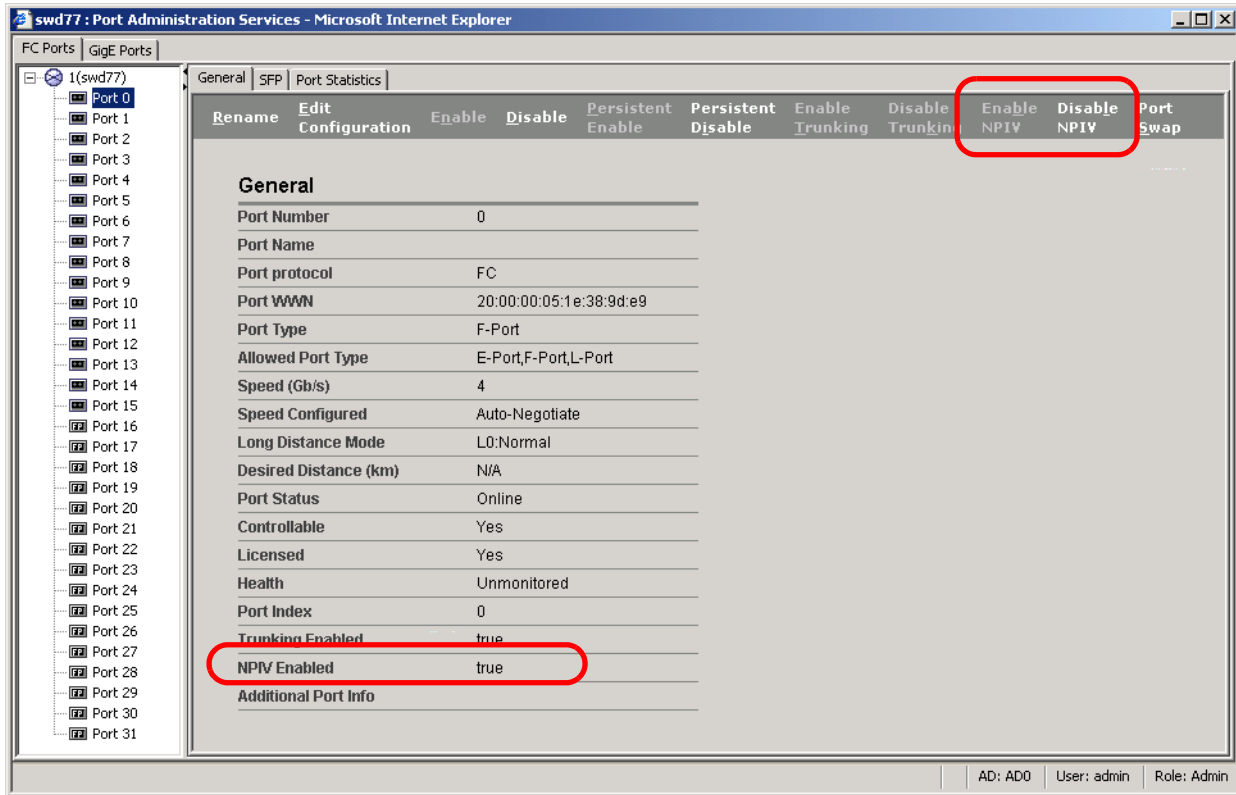


Figure 3-41 Display and configure NPIV capability of the Brocade switch

McDATA

To verify the NPIV feature of the switch:

1. On your workstation, open a supported browser window, and then enter the switch management IP address in the address field.
2. Enter a login name and password.
3. Open the Maintenance Feature Installation windows.
4. The NPIV feature displays under feature installation table.

Figure 3-42 shows that NPIV feature is installed in the switch.

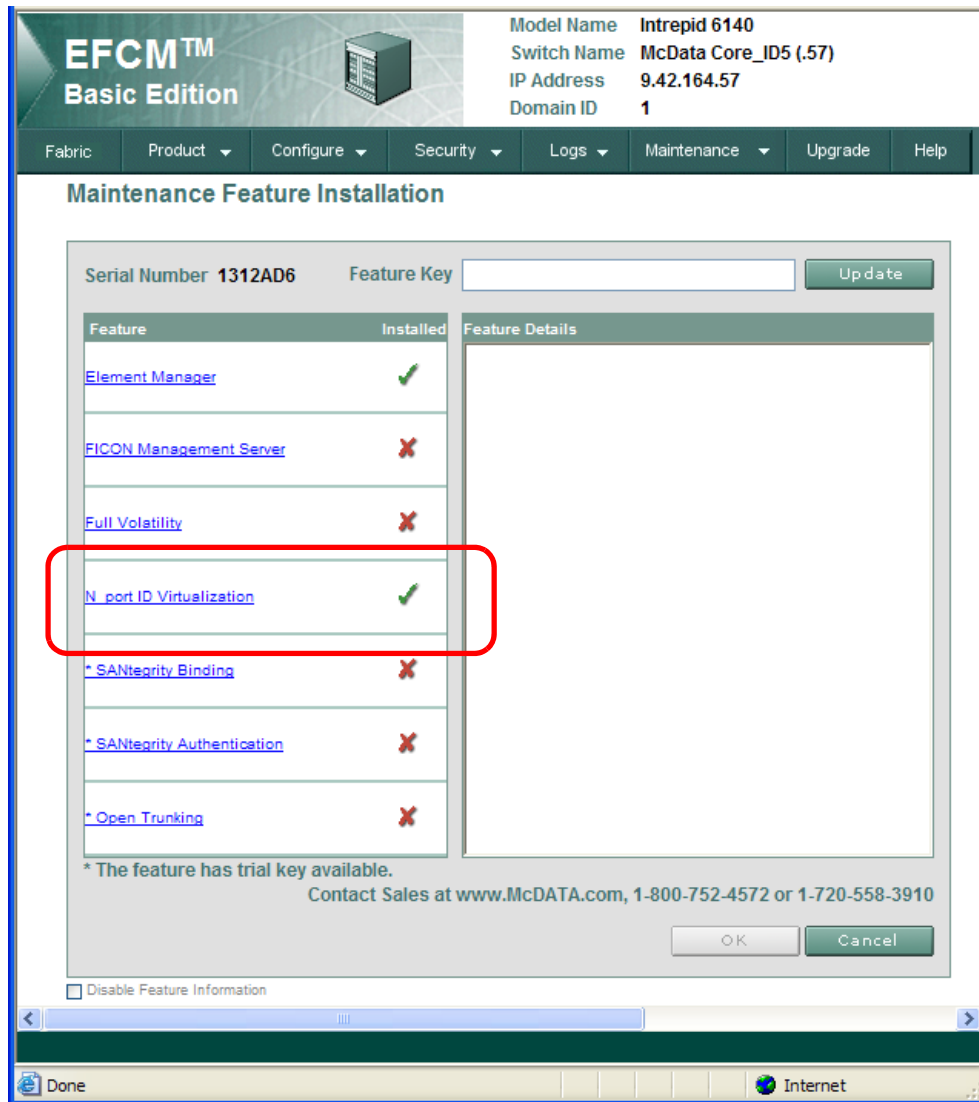


Figure 3-42 Display feature activation of the McDATA switch

Note: A check mark next to a particular feature indicates that the feature is already activated in the switch.

To install the NPIV feature in the switch:

1. Open the Maintenance Feature Installation window.
2. Enter the feature key for NPIV.
3. Continue to update.

Note: McDATA switches require feature key installation. The NPIV feature key can be requested from Brocade free of charge.

To enable NPIV feature in the switch and configure the port NPIV login limit:

1. Go to the main interface.
2. Click **Configure** → **Ports** → **NPIV**.
3. Click **Enable** in the NPIV Status box to enable the NPIV feature in all ports of the switch.
4. Enter the login number limit in the box.
5. Click **OK** to activate the modified configuration.

Figure 3-43 shows how to enable the NPIV feature and configure 10 NPIV login maximum in Port 0 and Port 1.

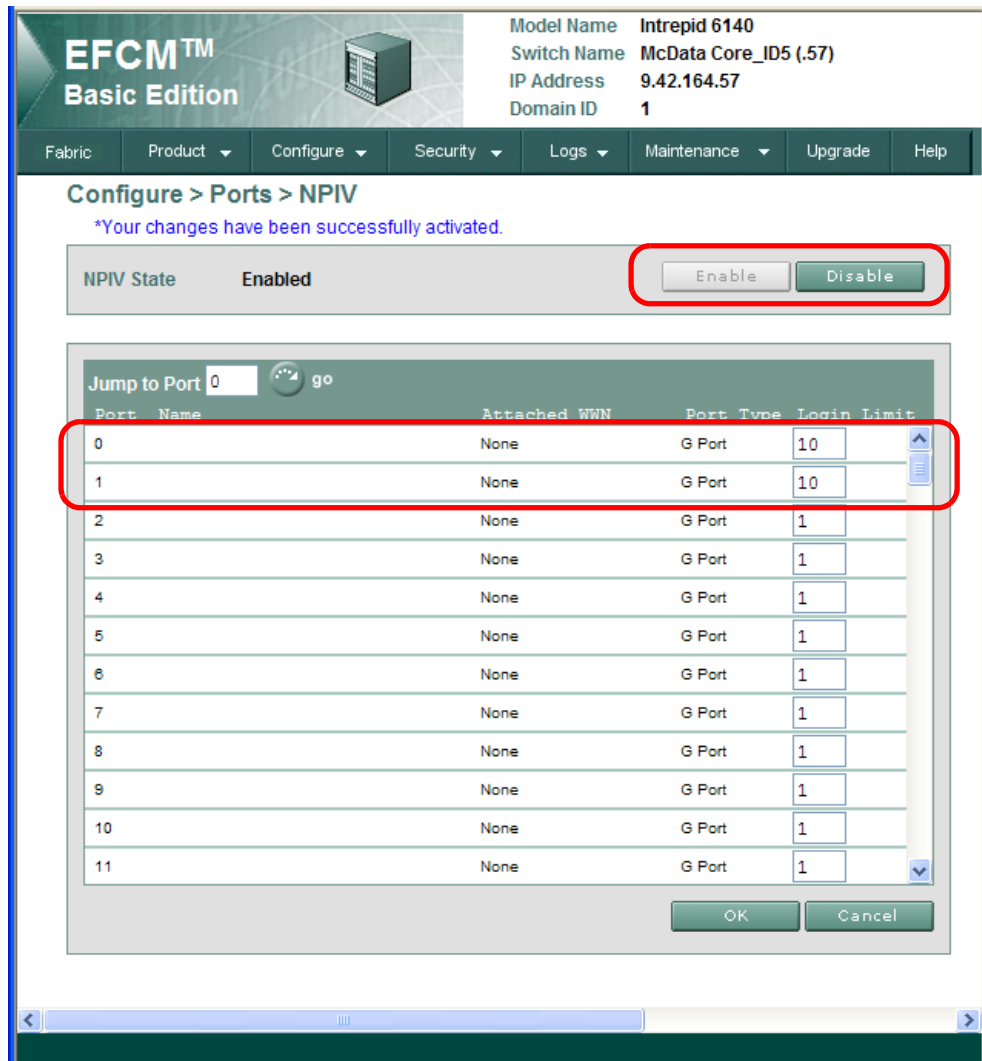


Figure 3-43 Enable NPIV and configure NPIV login limit of the McDATA switch

3.5 Configuring the connection

This section discusses the typical tasks to configure the connection to the external switch and to configure zoning and redundancy. We also discuss clustering.

Because the IPM acts as a transparent device in the SAN, it shows all HBAs transparently to the external switch. Configuring the connection through IPM does not require as many steps as configuring connection through a switch. Basically, you only have connect it to a setup external switch and verify that the connection is configured successfully.

We discuss the following topics in this section:

- ▶ 3.5.1, “Connecting the Intelligent Pass-thru Module to external switch”
- ▶ 3.5.2, “Verify the connection” on page 69
- ▶ 3.5.3, “Configure zoning” on page 72
- ▶ 3.5.4, “Configure redundancy and load balancing” on page 74
- ▶ 3.5.5, “Storage attachment” on page 75

3.5.1 Connecting the Intelligent Pass-thru Module to external switch

For this section, we used the following devices in our lab:

- ▶ BladeCenter H chassis
- ▶ BladeCenter HS21 and LS21 servers
- ▶ Multi-Switch Interconnect Modules (MSIM) in bay 8 and bay 10 of the chassis
- ▶ QLogic 4 Gb Intelligent Pass-thru Modules, one in each MSIM.
- ▶ External Brocade 7500 switch
- ▶ Workstation management console

The idea is to give you a clear description about the simplicity of configuring the connection with IPM implemented in the SAN.

Figure 3-44 shows the connection setup in our lab.

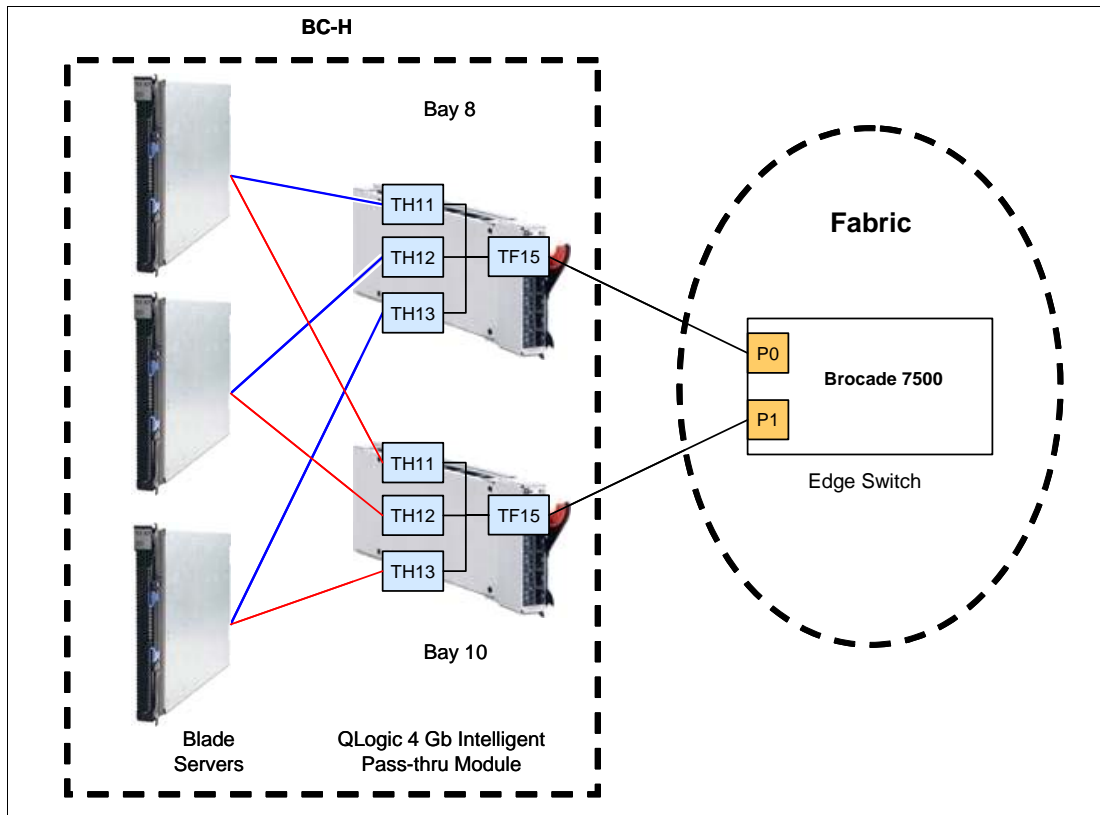


Figure 3-44 Connection setup in the lab

As shown in our lab setup in Figure 3-44, we connected each of the three blade servers to two IPMs. We connected the IPM in bay 8 to port 0 of the Brocade 7500 and connected the IPM in bay 10 to port 1 of the Brocade 7500.

Figure 3-45 shows the green LEDs at Port 0 and Port 1 (circled in red) that indicate good connection to an IPM's port. We can also see that connecting the switch to the transparent IPMs does not add any domain to the fabric. We can observe from the red circle on the left pane as per Figure 3-45.

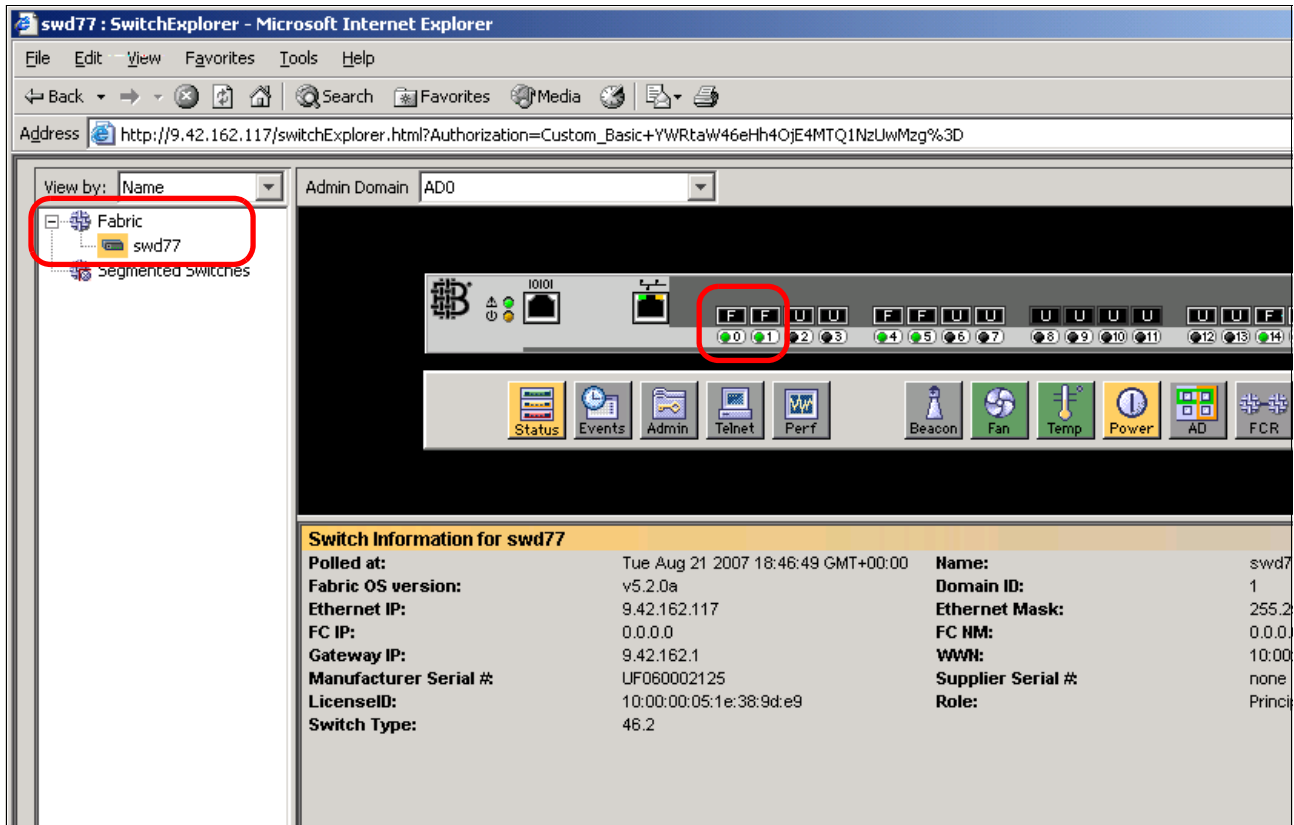


Figure 3-45 Brocade Web Tools main interface

If IPM is in *Full Fabric Mode*, the domain ID indicates its own ID as shown in Figure 3-46. Figure 3-45 and Figure 3-46 address the difference between Transparent Mode and Full Fabric Mode on IPM.

```
IPM4GbT: admin> show fabric
```

Domain	WWN	Enet IP Addr	FC IP Addr	SymbolicName
*1 (0x01)	10:00:00:05:1e:34:47:03	9.42.171.202	0.0.0.0	SWD77
2 (0x02)	10:00:00:c0:dd:0d:35:bc	9.42.171.78	0.0.0.0	IPM4GbT

* indicates principal switch

ID 1 is the Brocade external SAN switch
ID 2 is the Intelligent Pass-thru Module

Figure 3-46 IPM Full Fabric Mode

3.5.2 Verify the connection

A simple way to verify the connection in a SAN is to see the HBA from a switch within the SAN. After an HBA is properly connected to a switch, its WWN will appear in the switch. This section gives some examples of how to see the HBA WWNs of the three blade servers from a Brocade switch attached to the Intelligent Pass-thru Modules.

To see all HBAs attached to a Brocade switch through Web Tool (GUI):

1. On your workstation, open a supported browser window, and then enter the switch management IP address in the address field.
2. Enter a login name and password.
3. In the main interface, under the left pane, click the Name Server icon to open the Name Server window.
4. Verify the appearance of the WWNs of the HBAs attached to the corresponding blade servers.

Figure 3-47 shows the how the HBA WWNs appear in the Name Server table. The HBAs connected through transparent IPMs are indicated by the **NPIV** state of the **Initiator**.

Tip: Because each of our HBA cards has 2 ports connected to two modules, we see three WWNs attached to Port 0 and three WWNs attached to Port 1.

The screenshot shows a web browser window titled "swd77 : Name Server Table. - Microsoft Internet Explorer". The main content is a "Name Server" table. At the top, there are controls for "Auto Refresh" (unchecked), "Auto-Refresh Interval" (15 seconds), and "Number of Devices" (12). Below the controls is a table with the following columns: Domain, Port #, Port ID, Port Type, Device Port WWN, Device Node WWN, Device Name, NPIV(...), and Host vs. Target. The table contains 12 rows of data. Red boxes highlight the "Port #", "Port ID", "Device Port WWN", "Device Node WWN", "Device Name", and "NPIV(...)" columns for several rows. Red arrows point from the labels "Port 0 devices" and "Port 1 devices" to the "Port #" column, indicating that rows with Port # 0 are connected to Port 0 and rows with Port # 1 are connected to Port 1.

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	NPIV(...)	Host vs. Target
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	NPIV	Initiator
1	15	010000	N	20:25:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FAST 0916	Physical	Initiator+Target
1	5	010500	N	20:14:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FAST 0916	Physical	Initiator+Target
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	NPIV	Initiator
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 (...)	NPIV	Initiator
1	4	010400	N	20:24:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FAST 0916	Physical	Initiator+Target
1	14	010e00	N	20:15:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FAST 0916	Physical	Initiator+Target
1	1	010100	N	20:00:00:c0:dd:0d:35:8f	10:00:00:c0:dd:0d:35:8f		Physical	Unknown(Initia...
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 (...)	NPIV	Initiator
1	0	010000	N	20:00:00:c0:dd:0d:35:8f	10:00:00:c0:dd:0d:35:8f		Physical	Unknown(Initia...
1	1	010101	N	21:00:00:1b:32:18:1a:0b	20:00:00:1b:32:18:1a:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	NPIV	Initiator
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	NPIV	Initiator

Figure 3-47 Verify the connection through WebTools Name Server table

We can also use Telnet session (CLI) to display the HBAs which connected to the switch.

Enter the `switchshow` command to verify that the NPIV links are logged in to the ports.

Figure 3-48 shows that Port 0 and Port 1 have NPIV connection logged in.

```
swd77 login: admin
Password:
Please change passwords for switch default accounts now.
Use Control-C to exit or press 'Enter' key to proceed.

Password was not changed. Will prompt again at next login
until password is changed.

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  No_Light
3  3  id  N4  No_Light
```

Figure 3-48 Verify NPIV links logged in the ports

Enter the **portshow** command to display the devices connected to a particular port.

Figure 3-49 shows that 3 HBAs are logged (through NPIV connection) in Port 0.

```
swd77:admin> portshow 0
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: 0
portId: 010000
portIfId: 4302080b
portWwn: 20:00:00:05:1e:38:9d:e9
portWwn of device(s) connected:
    21:01:00:1b:32:38:1a:0b
    21:01:00:1b:32:37:40:de
    21:01:00:1b:32:38:15:0b
    20:00:00:c0:dd:0d:35:a3
Distance: normal
portSpeed: N4Gbps
```

Figure 3-49 Display devices logged in a port

Enter the `nsshow` command to display all device WWNs detected by the switch.

Figure 3-50 shows that 3 HBAs are logged (through NPIV connection) in Port 0.

```
swd77:admin> nsshow
{
  Type Pid   COS   PortName                               NodeName                               TTL(sec)
  N   010000; 2,3;20:00:00:c0:dd:0d:35:a3;10:00:00:c0:dd:0d:35:a3; na
      Fabric Port Name: 20:00:00:05:1e:38:9d:e9
      Permanent Port Name: 20:00:00:c0:dd:0d:35:a3
      Port Index: 0
      Share Area: No
      Device Shared in Other AD: No
  N   010001; 2,3;21:01:00:1b:32:38:1a:0b;20:01:00:1b:32:38:1a:0b; na
      FC4s: FCP
      NodeSymb: [35] "QMI3472 FW:v4.00.23 DVR:v8.01.07-k1"
      Fabric Port Name: 20:00:00:05:1e:38:9d:e9
      Permanent Port Name: 21:01:00:1b:32:38:1a:0b
      Port Index: 0
      Share Area: No
      Device Shared in Other AD: No
  N   010002; 2,3;21:01:00:1b:32:37:40:de;20:01:00:1b:32:37:40:de; na
      FC4s: FCP
      NodeSymb: [40] "QMI3472 FW:v4.00.23 DVR:v9.1.2.19 (w32)"
      Fabric Port Name: 20:00:00:05:1e:38:9d:e9
      Permanent Port Name: 21:01:00:1b:32:37:40:de
      Port Index: 0
      Share Area: No
      Device Shared in Other AD: No
  N   010003; 2,3;21:01:00:1b:32:38:15:0b;20:01:00:1b:32:38:15:0b; na
      FC4s: FCP
      NodeSymb: [35] "QMI3472 FW:v4.00.23 DVR:v8.01.07-k1"
      Fabric Port Name: 20:00:00:05:1e:38:9d:e9
      Permanent Port Name: 21:01:00:1b:32:38:15:0b
      Port Index: 0
      Share Area: No
      Device Shared in Other AD: No
  ...
}
```

Figure 3-50 Display all devices logged in a switch

3.5.3 Configure zoning

After all connections are verified successfully from the fabric, you can configure zoning for the related devices. This section gives some examples of how to configure zoning for the HBA WWNs of three blade servers from a Brocade switch attached to the two Intelligent Pass-thru Modules.

Because the Intelligent Pass-thru Module acts as a transparent device in the SAN, it shows all HBAs transparently to the external switch. Configuring the zoning with an IPM requires no different basic steps compared to configuring it with an FCSM or an OPM. As soon as you can see all devices, you need to zone in the switch name server, you can configure the zone.

To configure the zoning:

1. List all the devices that you want to include in the zone.
2. Verify that all devices that you want to include in the zone appear in the fabric switch name server.
3. Open the Zone Admin window by selecting the **Zoning** icon located in the left pane of WebTools main interface.
4. Go to the Zone tab to manage or create the zone.
5. Go to the Zone Config tab to manage or create the zone configuration.

Figure 3-51 shows that a port of each HBA of the three blade servers are connected to Port 0 of the Brocade switch.

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	NPIV(...)	Host vs. Target
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	NPIV	Initiator
1	15	010F00	N	20:25:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	5	010500	N	20:14:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
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	NPIV	Initiator
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 (...)	NPIV	Initiator
1	4	010400	N	20:24:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	14	010e00	N	20:15:00:a0:b8:26:1c:30	20:04:00:a0:b8:26:1c:30	IBM 1814 FASTT 0916	Physical	Initiator+Target
1	1	010100	N	20:00:00:c0:dd:0d:35:8f	10:00:00:c0:dd:0d:35:8f		Physical	Unknown(Initia...
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 (...)	NPIV	Initiator
1	0	010000	N	20:00:00:c0:dd:0d:35:a3	10:00:00:c0:dd:0d:35:a3		Physical	Unknown(Initia...
1	1	010101	N	21:00:00:1b:32:18:1a:0b	20:00:00:1b:32:18:1a:0b	QMI3472 FW:v4.00.23 DVR:v8.01.07-k1	NPIV	Initiator
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	NPIV	Initiator

Figure 3-51 HBA WWNs displayed in the Name Server

As illustrated in Figure 3-52, in the Zone Admin window, we can see those HBA WWNs.

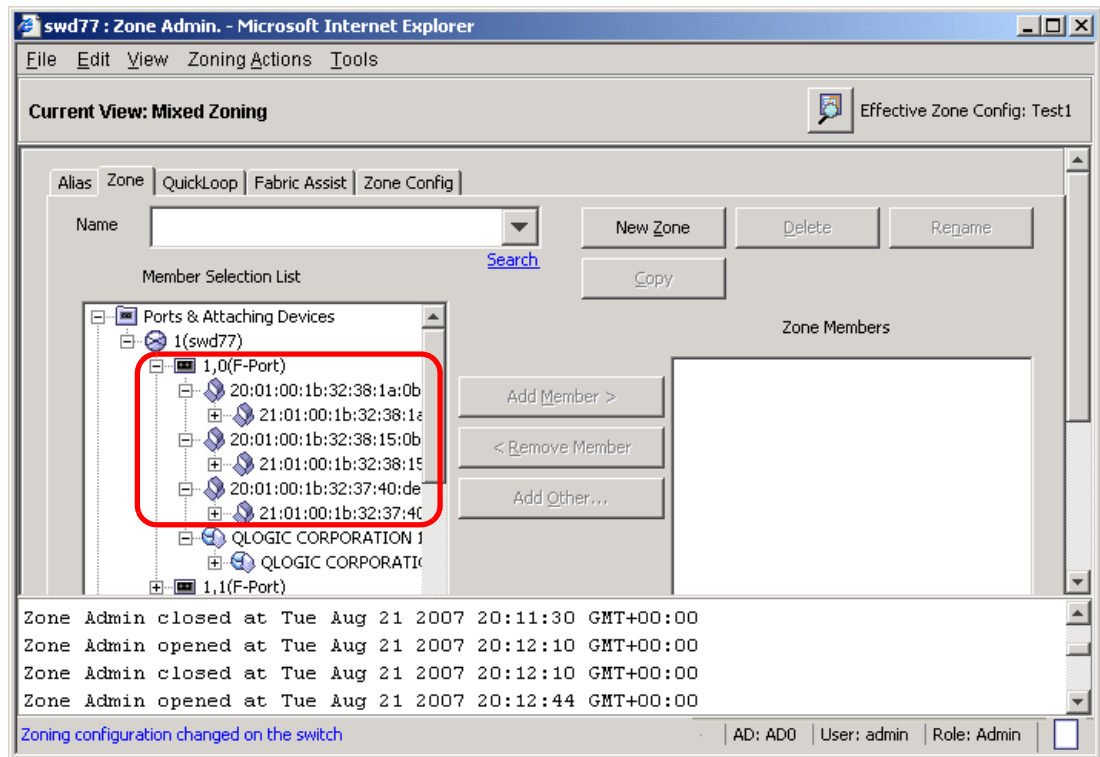


Figure 3-52 HBA WWNs displayed in the Zone Admin window

Now, you can manage zoning by Adding or Removing the Zone Member and manage the zone configuration as well.

3.5.4 Configure redundancy and load balancing

This section discusses how to configure redundancy and load balancing from the Intelligent Pass-thru Module point of view.

Unlike the original Optical Pass-thru Module, the Intelligent Pass-thru Module provides a redundancy and load balancing feature on its ports. Using IPM, we can assign a TH_Port to multiple TF_Ports. For redundancy purposes, a backup port mapping can also be specified. A TH_Port can be mapped to multiple primary and secondary ports. A port designated as primary will be the first path chosen. If there are multiple primary ports, the TH_Ports are distributed (using algorithm) across the TF_Ports. Backup ports only become active when all primary ports fail.

To configure redundancy connection from an HBA through an IPM:

1. Ensure that minimum two TF_Ports are connected to the fabric switch.
2. Map a TH_Port to a minimum of one primary port and one backup port

To configure load balancing connection from an HBA through an IPM:

1. Ensure that minimum two TF_Ports are connected to the fabric switch.
2. Map a TH_Port to a minimum of two primary ports.

Figure 3-53 shows how to configure the redundancy and load balancing for Port 1 in the same time. For the load balancing purpose, the traffic from Port 1 is distributed across Port 0, Port 15 and Port 16. As the backup ports, Port 17 and Port 18 will become active after Port 0, Port 15 and Port 16 fail.

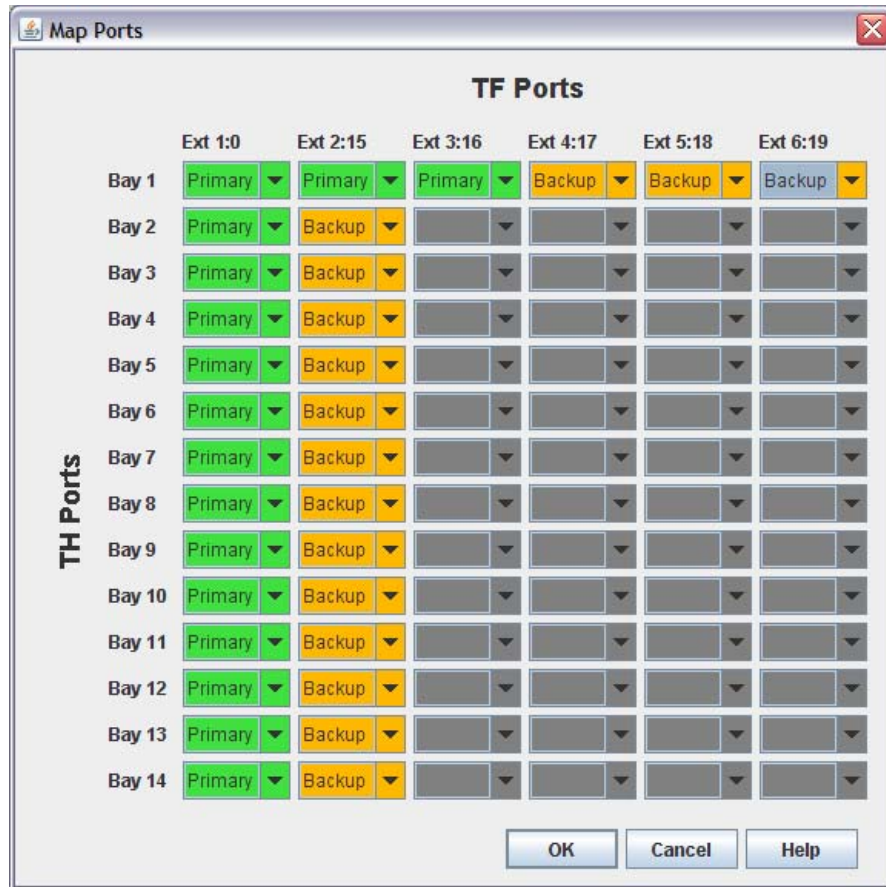


Figure 3-53 Configure redundancy and load balancing using Port Mapping

3.5.5 Storage attachment

In this section we describe the use of the Intelligent Pass-thru Module in a clustering environment. In this section, we show the results of failover and fallback at the servers, storage and external SAN switch.

In our lab, our environment consisted of:

- ▶ A BladeCenter E chassis
- ▶ Three BladeCenter HS21 servers
- ▶ Two Intelligent Pass-thru Modules
- ▶ One IBM System Storage™ DS4300
- ▶ One IBM 2005-H16 External SAN Switch
- ▶ Windows Server® 2003 Standard Edition and Enterprise Edition

In our test, we set up Microsoft Cluster Server (MSCS) with our storage attached through the Fibre Channel SAN Switch Module.

We were able to implement an MSCS cluster successfully using the Intelligent Pass-thru Module and the redundant paths that we configured meant that the data continued to be available even after a path failure.

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

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

To set up the configuration:

1. Define the zoning of each blade server that you intend to have in the MSCS environment. Figure 3-54 shows the initial zoning stage.

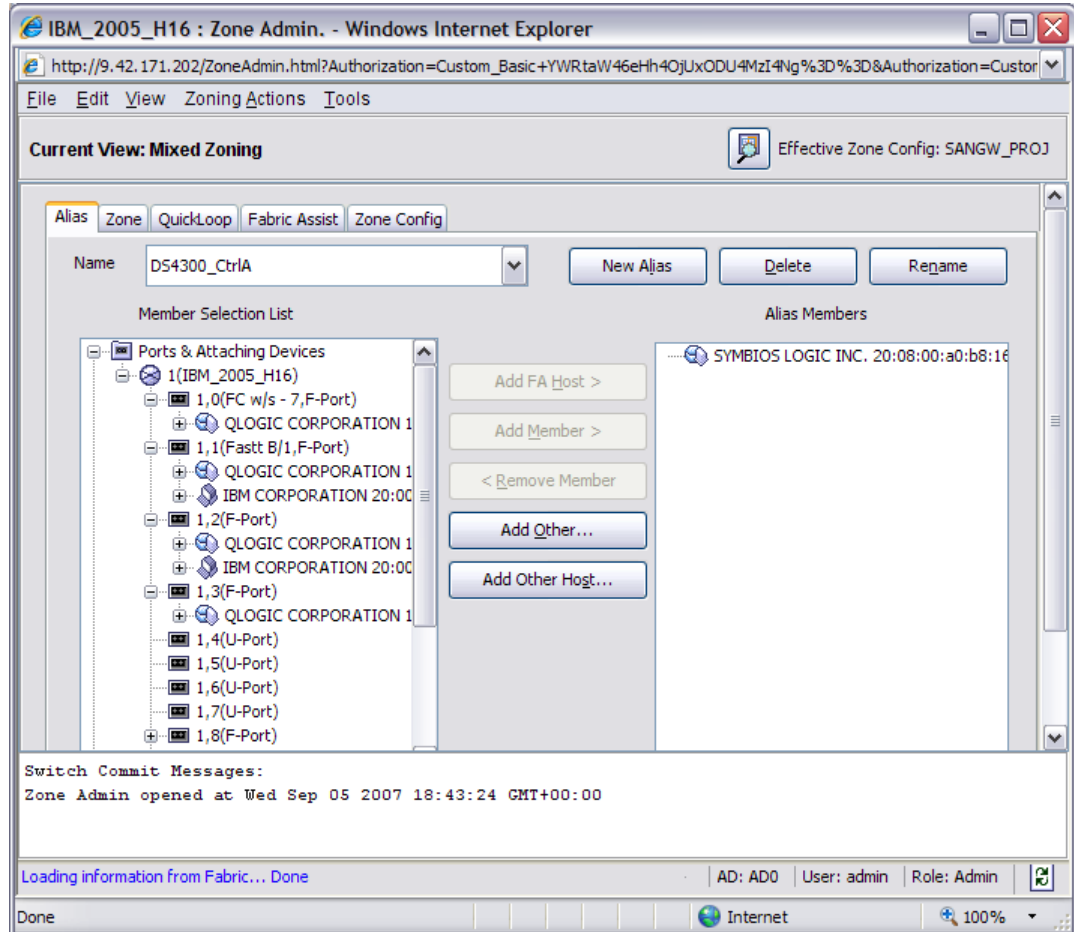


Figure 3-54 Initial stage setup on defining the alias name

2. After you have created the alias name based on the WWN, define the zoning of each alias as shown in Figure 3-55.

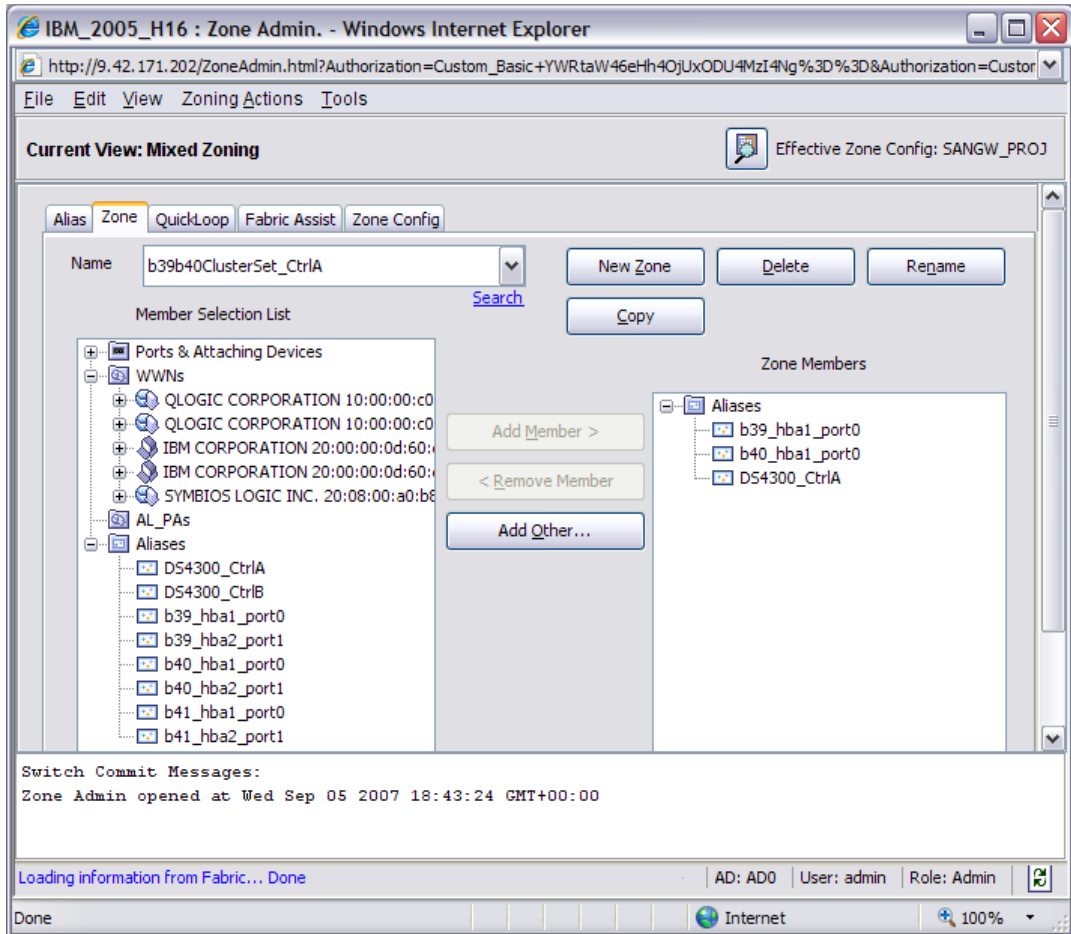


Figure 3-55 Define a zone

3. Save the configuration that you have made in the SAN switch to activate the configuration as shown in Figure 3-56.

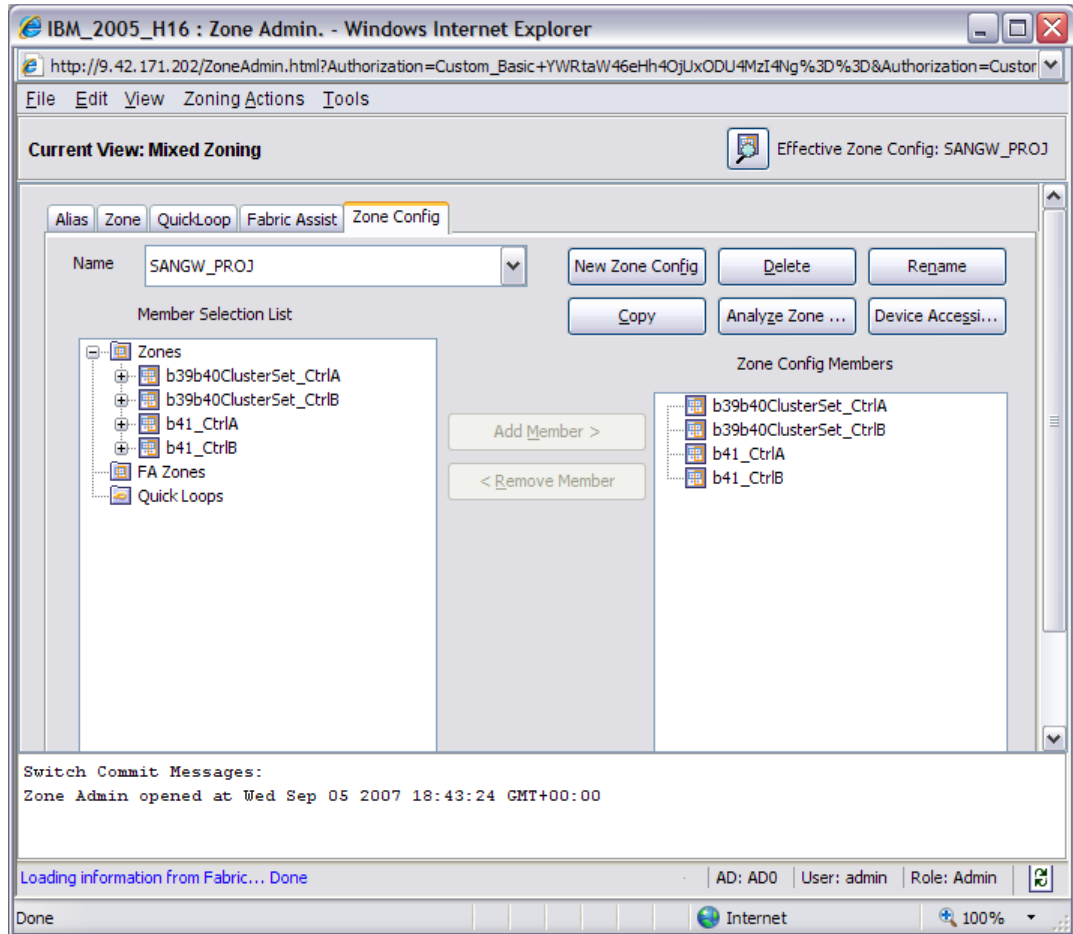


Figure 3-56 Complete the zoning configuration

4. After you complete the HBA assigning and zoning, 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), as shown in Figure 3-57.

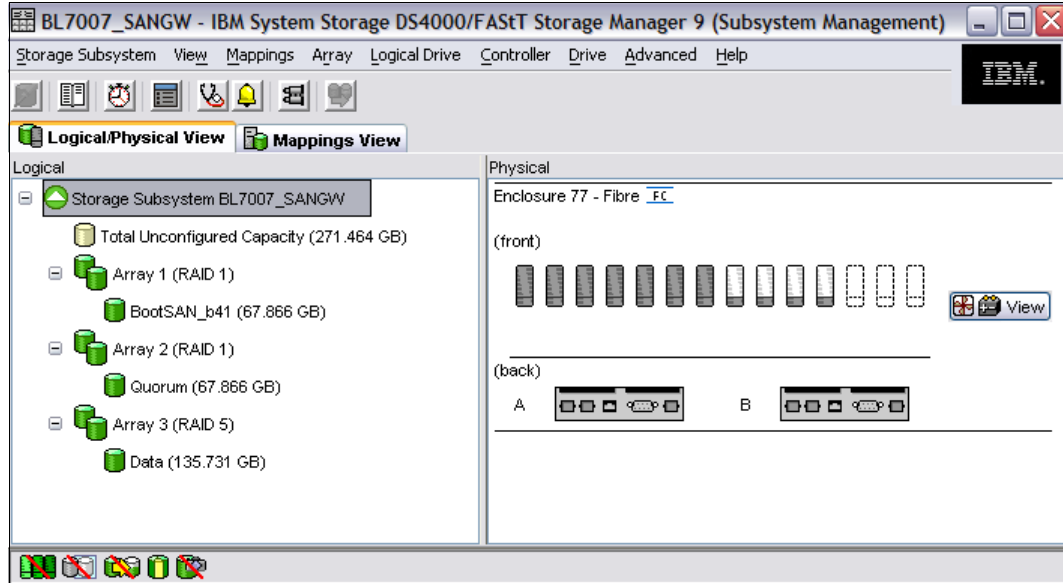


Figure 3-57 Storage partition assigning

- During the synchronizing of the array, proceed with the disk mapping for your server to identify the new partitions on the operating systems (Figure 3-58).

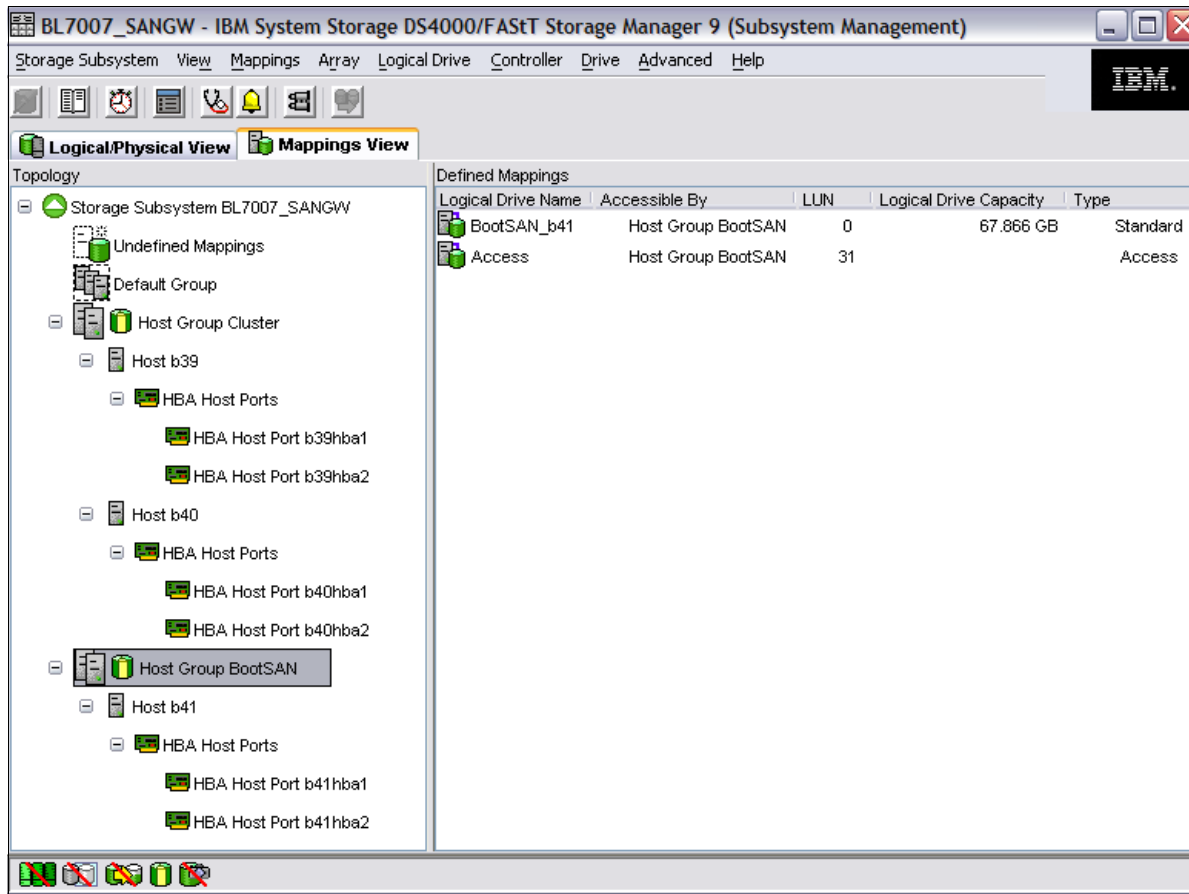


Figure 3-58 Storage mapping

Now you have completed the storage assigning for the blade server and can proceed with setting up MSCS. (We do not cover this topic in this document.)

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

When you have completed the initial setup of blade server, SAN storage, SAN switch, and operating systems, you can proceed with the test cases that we initiated in our test lab. Because IPM works as similar as the Fibre Channel Switch Module, setting up the MSCS is straight forward. We provide some of our test cases for your review.

To test the port redundancy, we disabled port 0 whereby the settings of port 0 are *PrimaryTFport* and port 15 are *BackupTFport*. You can disable port through GUI or CLI. We used the GUI so that we could have a clearer picture of the failover initiate automatically, without any interruption at the cluster server sets, as shown in Figure 3-59 for the IPM and Figure 3-60 in the MSCS.

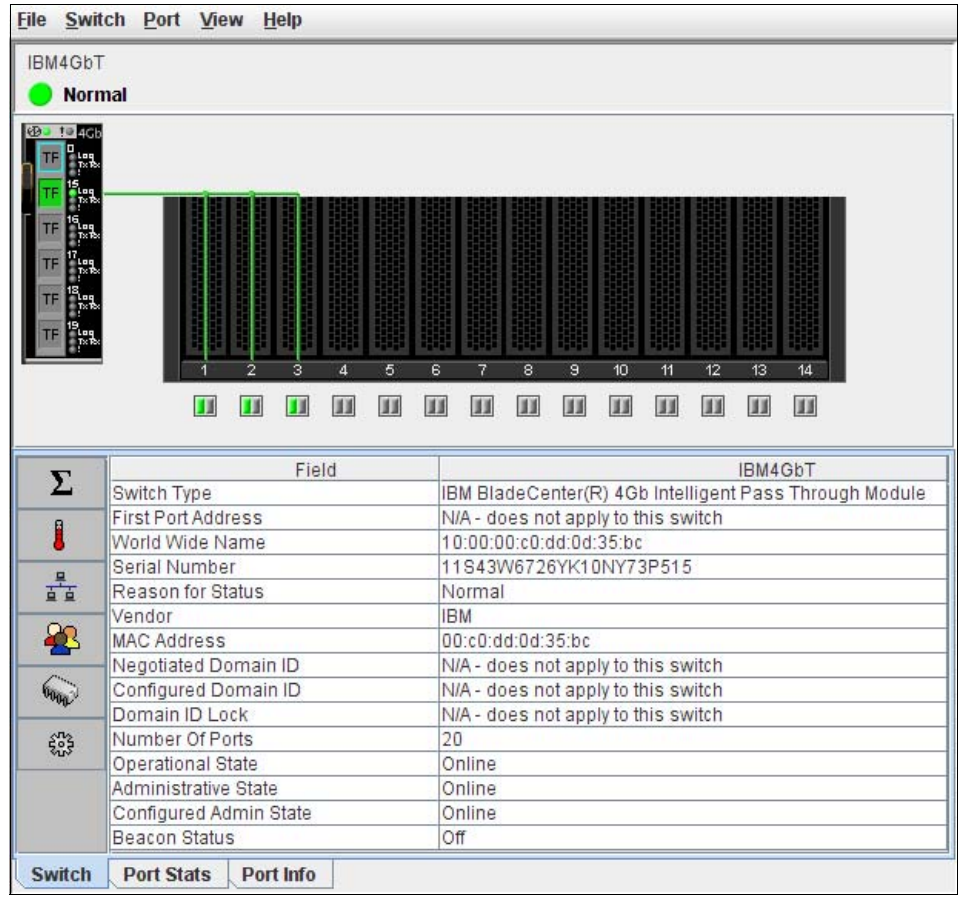


Figure 3-59 Indicate actual result port failover between port 0 and port 15

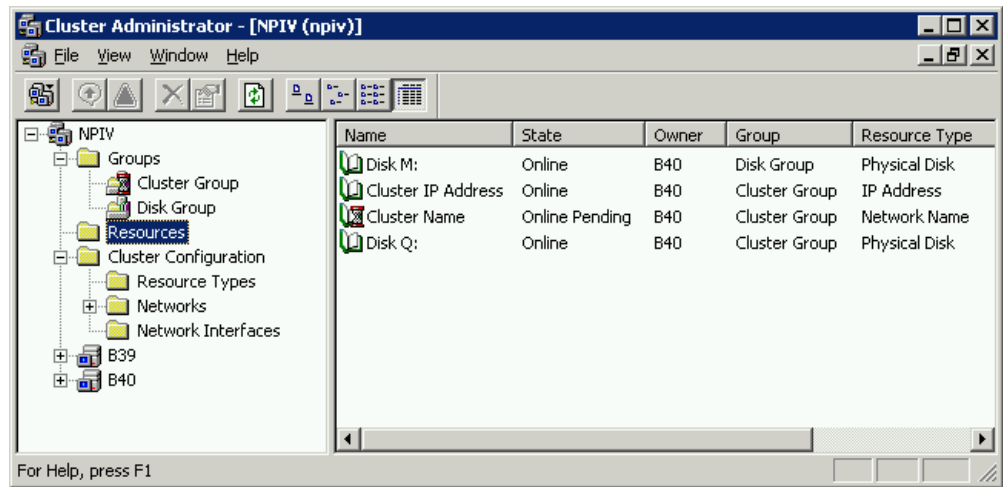


Figure 3-60 MSCS failover

In this example, you can either disable the port on the IPM or you can turn off the IPM. Either way, the result remains the same—users are still able to access the data or continue working without interruption. Figure 3-61 shows the results, indicating power off for the IPM in Bay 3.

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
<input type="checkbox"/>	2	Ethernet SM	00:05:5D:71:82:04	192.168.70.128	On	POST results available: FF: Module completed POST
<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

Figure 3-61 Indicate actual result of turning off the IPM in Bay 3

Abbreviations and acronyms

AMM	Advanced Management Module	SFP	small form-factor pluggable
BC	BladeCenter	SSH	Secure Shell
BIOS	basic input output system	TE	Transparent Embedded
CLI	command line interface	TFTP	Trivial File Transfer Protocol
FAN	Fabric Address Notification	VM	virtual machine
FB	failback	WWN	World Wide Name
FC	Fibre Channel	WWPN	World Wide Port Name
FCSM	Fibre Channel Switch Module		
FICON	Fibre Connection		
FO	failover		
FTP	file transfer protocol		
GB	gigabyte		
GUI	graphical user interface		
HBA	host bus adapter		
HT	Hyper-Threading		
I/O	input/output		
IBM	International Business Machines Corporation		
ID	identifier		
IP	Internet Protocol		
IPM	Intelligent Pass-thru Module		
ISL	Inter-Switch Link		
IT	information technology		
ITSO	International Technical Support Organization		
LED	light emitting diode		
LUN	logical unit number		
MDS	Multilayer Director Switch		
MSCS	Microsoft Cluster Server		
MSIM	Multi-Switch Interconnect Module		
NDCLA	Non-Disruptive Code Load Activation		
NPIV	N_Port ID Virtualization		
OPM	Optical Pass-thru Module		
OS	operating system		
PID	process ID		
PN	part number		
RAID	redundant array of independent disks		
RSCN	Registered State Change Notification		
SAN	storage area network		

Related publications

We consider the publications that we list in this section particularly suitable for a more detailed discussion of the topics that we cover 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 Redbooks, at the IBM Redbooks Web site:

ibm.com/redbooks

Related publications from 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>
- ▶ Brocade switch firmware:
<http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/supportresources?brandind=5000031&familyind=5329725&taskind=2>
- ▶ Cisco switch firmware:
<http://www.cisco.com/public/sw-center/>
- ▶ QLogicSANbox 9000 switch firmware:
http://support.qlogic.com/support/product_resources.asp?id=1006&type=switch
- ▶ SANbox 5600/2 switch firmware:
http://support.qlogic.com/support/product_resources.asp?id=929&type=switch
- ▶ SANbox 5200/2 switch firmware:
http://support.qlogic.com/support/product_resources.asp?id=540&type=switch
- ▶ McDATA switch firmware:
<http://www.mcdata.com/filecenter/template?page=index>
- ▶ Tftpd32 TFTP client
<http://tftpd32.jounin.net/>
- ▶ 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