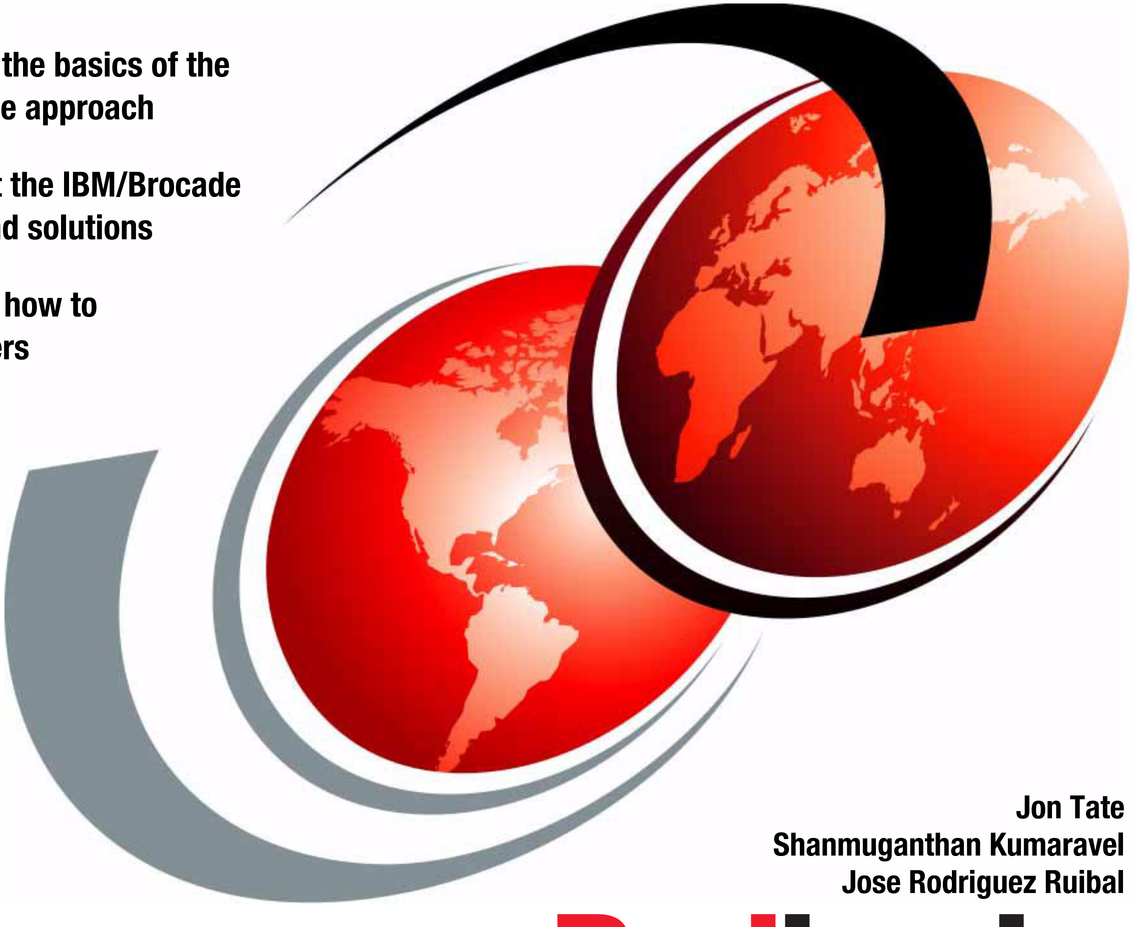
IBM System Storage b-type Multiprotocol Routing

An Introduction and Implementation



Read about the basics of the IBM/Brocade approach

Learn about the IBM/Brocade products and solutions

Understand how to install routers

Jon Tate
Shanmuganthan Kumaravel
Jose Rodriguez Ruibal

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM System Storage b-type Multiprotocol Routing: An Introduction and Implementation

March 2011

SG24-7544-03

Note: Before using this information and the product it supports, read the information in "Notices" on page ix.

Fourth Edition (March 2011)

This edition applies to Data Center Fabric Manager v10.4.1 and Fabric Operating System v6.4

Contents

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

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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

AIX 5L™
AIX®
DS4000®
DS8000®
Enterprise Storage Server®
eServer™
FICON®
IBM®
Redbooks®
Redbooks (logo) ®
System p®
System Storage®
System x®
Tivoli®
TotalStorage®

The following terms are trademarks of other companies:

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

The rapid spread and adoption of production storage area networks (SANs) has fueled the need for multiprotocol routers. The routers provide improved scalability, security, and manageability by enabling devices in separate SAN fabrics to communicate without merging fabrics into a single, large SAN fabric. This capability enables clients to deploy separate SAN solutions at the departmental and data center levels. Then, clients can consolidate these separate solutions into large enterprise SAN solutions as their experience and requirements grow and change.

Alternatively, multiprotocol routers can help to connect existing enterprise SANs for a variety of reasons. For instance, the introduction of Small Computer System Interface over IP (iSCSI) provides for the connection of low-end, low-cost hosts to enterprise SANs. The use of an Internet Protocol (IP) in the Fibre Channel (FC) environment provides for resource consolidation and disaster recovery planning over long distances. And the use of FC-FC routing services provides connectivity between two or more fabrics without having to merge them into a single SAN.

This IBM® Redbooks® publication targets storage network administrators, system designers, architects, and IT professionals who sell, design, or administer SANs. It introduces you to products, concepts, and technology in the IBM System Storage® SAN Routing portfolio, which is based on Brocade products and technology. This book discusses the features of these products and provides examples of how you can deploy and use them.

Our intent is to show how to implement the functions and features of the IBM/Brocade portfolio. To get the best use from this book, you must be familiar with SANs, basic SAN tasks, and the terminology associated with SANs. If you are not, read the following IBM Redbooks publications before you start this one:

- *Introduction to Storage Area Networks*, SG24-5470
- *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116

The team who wrote this book

This book was produced by a working at the International Technical Support Organization, San Jose Center.

Jon Tate is a Project Manager for IBM System Storage SAN Solutions at the International Technical Support Organization, San Jose Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing Level 2 support for IBM storage products. Jon has more than 25 years of experience in storage software and management, services, and support, and is both an IBM Certified IT Specialist and an IBM SAN Certified Specialist. He is also the UK Chairman of the Storage Networking Industry Association.

Shanmuganthan Kumaravel is an IBM Technical Services Specialist for the ITD-SSO MR Storage team of IBM India. He supports SAN, and disk products of both IBM and Hewlett Packard since August 2008. Prior to this he worked for HP product support providing remote support on HP SAN storage products, servers and operating systems including HP UNIX® and Linux®. Shan is a Brocade Certified SAN Designer (BCSD), Brocade Certified Fabric Administrator (BCFA) and an HP Certified System Engineer (HPCSE).

Jose Rodriguez Ruibal is the Technical Sales Leader for the IBM System x® Networking team, based in Montpellier, France, and covering the southwest Europe region. He has more than 12 years of experience in IT, and has worked for IBM for more than eight years. His experience includes serving as Benchmark Manager in the IBM PSSC Benchmark Center in Montpellier, working as an IT Architect for Nokia while living in Finland for three years and IT Architect and Team Leader for the IBM STG OEM and Next Generation Networks teams in EMEA. Prior to joining IBM, he worked for Red Hat and other consulting firms. His areas of expertise include Business Development, Strategic OEM Alliances and long-term IT projects in the Telecom, Media & Defense industries, high-level IT architecture and complex solutions design, Linux and all x86 hardware. Jose has co-authored other Redbooks on Linux solutions, on IBM x86 servers and on Performance Tuning for x86 servers. He holds an MSC and a BSC in Computer Engineering and Computer Systems from Nebrija University, Madrid.

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

Sangam Racherla
Lori Bideaux
International Technical Support Organization, San Jose Center

Doris Konieczny
IBM Storage Systems Group

Jure Arzensek
Gareth Edwards
Steve Fodor
Steve Garraway
Jim Kelly
Nikolaj Kjeldsen

Carsten Larsen
Andy McManus
Dariusz Myszka
Sangam Racherla
Pauli Ramo
Simon Richardson
Glen Routley
Chris Seiwert
Leos Stehlik
Marcus Thordal
Ricardo Trentin
Alexander Watson
The authors of previous versions of this book

A special mention must go to Brocade for their unparalleled support of this residency in terms of equipment and support in many areas throughout. We especially thank the following individuals:

Jim Baldyga
Mansi Botadra
Yong Choi
Silviano Gaona
Jason Russo
Brian Steffler
Marcus Thordal
Steven Tong
Brocade Communications Systems

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

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 books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

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

  ibm.com/redbooks

- Send your comments in an email 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

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition might also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-7544-03
for IBM System Storage b-type Multiprotocol Routing: An Introduction and Implementation
as created or updated on March 11, 2011.

March 2011, Fourth Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- Virtual fabrics
- Data Center Fabric Manager
- Fabric OS 6.4.1

Changed information

All graphics have been updated to show the latest software where changes have been made.

1

SAN routing introduction

Storage area networks (SANs) are networks that are used primarily for connecting hosts to their primary storage devices, whether they are disk or tape. With SANs, no data loss should occur. Applications and operating systems are designed to expect the best performance and reliability of the SAN storage environment. By design, loss of data or slow performance is generally not tolerated.

With the continued growth of the use of SAN fabrics to provide connection to business-critical storage, pressure has been mounting to provide further capabilities within the corporate SAN environment. To help meet these needs, SAN routing capabilities have been introduced to provide users with new methods to meet and manage their daily business needs. The Storage Network Industry Association (SNIA) adopted a group of SAN routing protocols by which the Fibre Channel environment can better serve its users.

Today’s SAN routing can provide you with techniques to meet these requirements:

- Departmental isolation while still allowing for resource sharing
- Technology migration and integration
- Remote replication of disk systems
- Disaster recovery (DR) capabilities
- Remote access to disk and tape systems
- Low-cost and existing connections to SANs

An important point to understand is that not all SAN multiprotocol routers are equal. Some routers support certain protocols and methods; others support different capabilities. To help in your planning and decision making, this book points out which of these devices support which capabilities.

This chapter introduces the terminology, technologies, and the value propositions for SAN routing techniques.

1.1 SAN routing definitions

To get the most out of this book, you should clearly understand the terms and principles of the various Fibre Channel (FC) routing protocols and methodologies prior to designing routed networks.

In this section, we briefly introduce several terms that are used later in this chapter and in the remainder of this book.

1.1.1 Fibre Channel

Fibre Channel is a set of standards for a serial input/output (I/O) bus developed through industry cooperation. A Fibre Channel frame consists of a header, payload, and 32-bit cyclic redundancy check (CRC) bracketed by start of frame (SOF) and end of frame (EOF) delimiters. The header contains the control information necessary to route frames between defined points known as N_Ports, and manage exchanges and sequences.

It is beyond the scope of this book to cover Fibre Channel in any great depth. For more detailed discussions, see the following IBM Redbooks publications:

- *Introduction to Storage Area Networks*, SG24-5470
- *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384

Figure 1-1 shows the layout of a Fibre Channel frame.

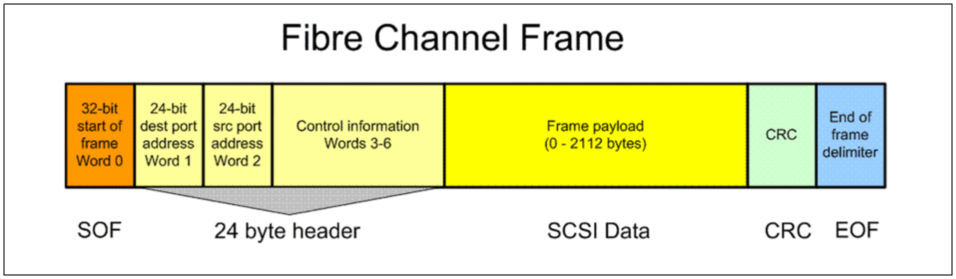

Fibre Channel Frame
32-bit start of frame Word 0
24-bit dest port address Word 1
24-bit src port address Word 2
Control information Words 3-6
Frame payload (0 - 2112 bytes)
CRC
End of frame delimiter
SOF
24 byte header
SCSI Data
CRC
EOF

Figure 1-1 Fibre Channel frame structure

1.1.2 Fibre Channel switching

A Fibre Channel switch filters and forwards packets between Fibre Channel connections within the same fabric, but it cannot transmit packets to a different fabric. When Fibre Channel switches are connected together, by way of inter-switch links (ISL), they merge to become a single fabric with one set of fabric services, which potentially is a single point of failure for the data center design.

Important: Fibre Channel switching cannot pass packets between fabrics.

1.1.3 Fibre Channel routing

A Fibre Channel router (FC-FC) is used to forward data packets between two or more fabrics while maintaining their independence from each other. Routers use headers and forwarding tables to determine the best path for forwarding the packets.

Separate fabrics each have their own addressing schemes. When they are joined by a router, there must be a way to translate the addresses between the two fabrics. This mechanism is called network address translation (NAT) and is inherent in the Cisco, Brocade, and McDATA multiprotocol switch/router products. It is sometimes referred to as FC-NAT to differentiate it from a similar mechanism that exists in the IP routers.

Important: Fibre Channel routers forward packets between fabrics.

1.1.4 Tunneling

Tunneling is a technique that allows one network to send its data through another network's connections. Tunneling works by encapsulating a network protocol in packets carried by the second network. For example, in a Fibre Channel over Internet Protocol (FCIP) solution, Fibre Channel packets can be encapsulated inside IP packets. Tunneling raises issues of packet size, compression, out-of-order packet delivery, and congestion control. Refer to 1.2.1, "Fibre Channel over Internet Protocol (FCIP)" on page 4 for more information

1.1.5 Routers and gateways

When a Fibre Channel router has to provide protocol conversion or tunneling services, it is actually acting as a gateway rather than a router. However, a recent common practice broadens the use of the term *router* to allow for these functions to be included. FCIP is an example of tunneling; Internet Small Computer System Interface (iSCSI) and Internet Fibre Channel Protocol (iFCP) are examples of protocol conversion.

1.1.6 Fibre Channel routing between physical or virtual fabrics

Brocade's routing solutions offer FC-FC routing between separate physical fabrics and virtual fabric which is described in Chapter 8, "Routing in virtual fabrics" on page 129.

1.2 Routed gateway protocols

This section introduces the protocols that can be encountered in today's *routed* environments.

1.2.1 Fibre Channel over Internet Protocol (FCIP)

FCIP is a method for tunneling Fibre Channel packets through an IP network. It is the most commonly used method to interconnect SANs to support the need for high availability, business continuance disaster recovery (BCDR), remote mirroring, and remote backup and archiving facilities. FCIP encapsulates Fibre Channel block data and transports it over a TCP socket, or tunnel. TCP/IP services establish connectivity between remote devices. The Fibre Channel packets are not altered in any way. They are encapsulated in an IP envelope and transmitted.

FCIP allows you to connect to a Gigabit Ethernet connection, and provides the IP transport to enable the transfer of the SAN across LAN, MAN, or WAN networks. This approach is a great advantage of FCIP, in that it can help with overcoming the distance limitations found with native Fibre Channel.

One must be careful when using another networking technique to carry Fibre Channel SAN packets over. A requirement of SANs is have no data loss. Applications and operating systems are designed to expect the high level of performance and reliability of the SAN storage environment. Loss of data or slow performance is generally not tolerated by their design. Therefore, using this type of transport is best applied to functions that do not have tight boundaries applied to them. Examples of good usage for this model are Business Continuance/ Disaster Recovery (BCDR) tools such as Global Mirroring, or Global Copy. In general, for an application to be a good fit it would need to be designed to function in a LAN-based IP environment.

This technique can also be used to enable geographically distributed SAN devices to be linked using existing IP infrastructures, while keeping fabric services intact. Although this capability is possible, you should first consider the previously described factors with regard to your environment.

Figure 1-2 shows a basic FCIP network design.

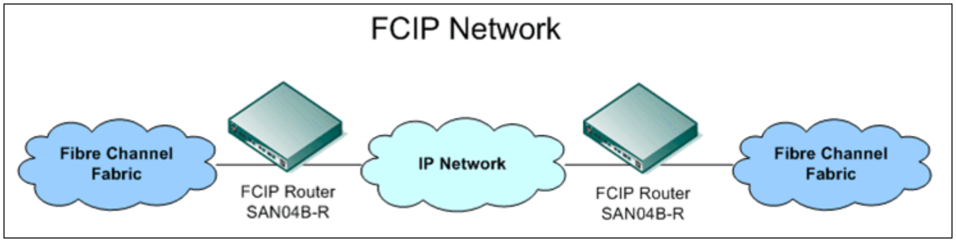


Figure 1-2 FCIP network

The architecture of FCIP is outlined in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3821, “Fibre Channel Over TCP/IP (FCIP),” available at the following web page:

`http://www.ietf.org/rfc/rfc3821.txt`

Figure 1-3 shows the structure of the FCIP tunneling packet. This example assumes that the Fibre Channel packet is small enough to fit inside a single IP packet.

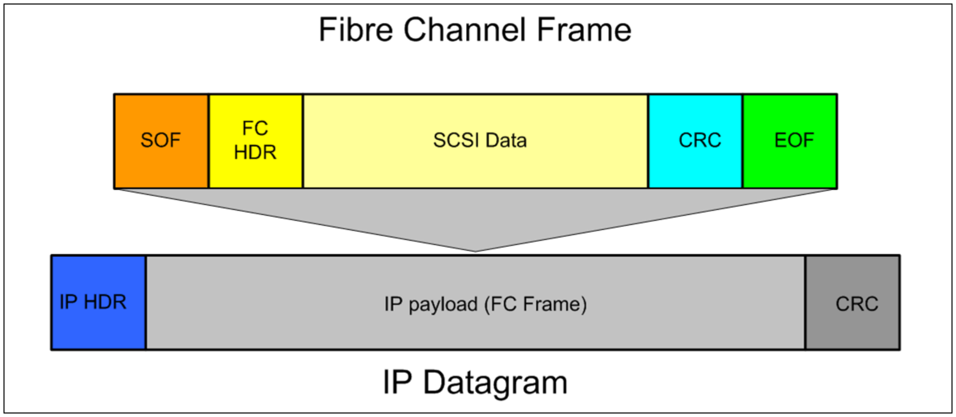


Figure 1-3 FCIP encapsulates the Fibre Channel frame into IP packets

Merging fabrics

Because FCIP tunnels Fibre Channel, creating an FCIP link is similar to creating an inter-switch link (ISL), and the two fabrics at either end are merged into a single fabric. This approach creates issues in situations where you do not want to merge the two fabrics for business reasons, or where the link connection is prone to occasional fluctuations or outages.

Although many corporate IP links appear to be robust, knowing for certain is difficult because traditional IP-based applications tend to be retry-tolerant by design. Fibre Channel fabric services are not so retry-tolerant. Each time the link disappears or reappears, the switches renegotiate and the fabric is reconfigured.

To prevent this effect from being an issue, combine FCIP with FC-FC routing, and thereby maintain the member fabrics independent of each other, each containing its own separate Fibre Channel services.

1.2.2 iSCSI protocol

The Small Computer Systems Interface (SCSI) protocol has a client/server architecture. Clients (called initiators) issue SCSI commands to request services from logical units on a server known as a target. A SCSI transport maps the protocol to a specific interconnect.

The SCSI protocol has been mapped over a number of transports, including Parallel SCSI, Intelligent Peripheral Interface (IPI), IEEE-1394 (firewire), and Fibre Channel. All of these transports are ways to pass SCSI commands. Each transport is I/O specific and has limited distance capabilities.

The iSCSI protocol is a means of transporting SCSI packets over TCP/IP to take advantage of the existing Internet infrastructure.

A session between an iSCSI initiator and an iSCSI target is defined by a session ID that is a combination of an initiator part (ISID) and a target part (Target Portal Group Tag).

The direction of the iSCSI transfer is defined with respect to the initiator. Outbound or outgoing transfers are from an initiator to a target. Inbound or incoming transfers are from a target to an initiator.

Figure 1-4 shows a basic iSCSI design.

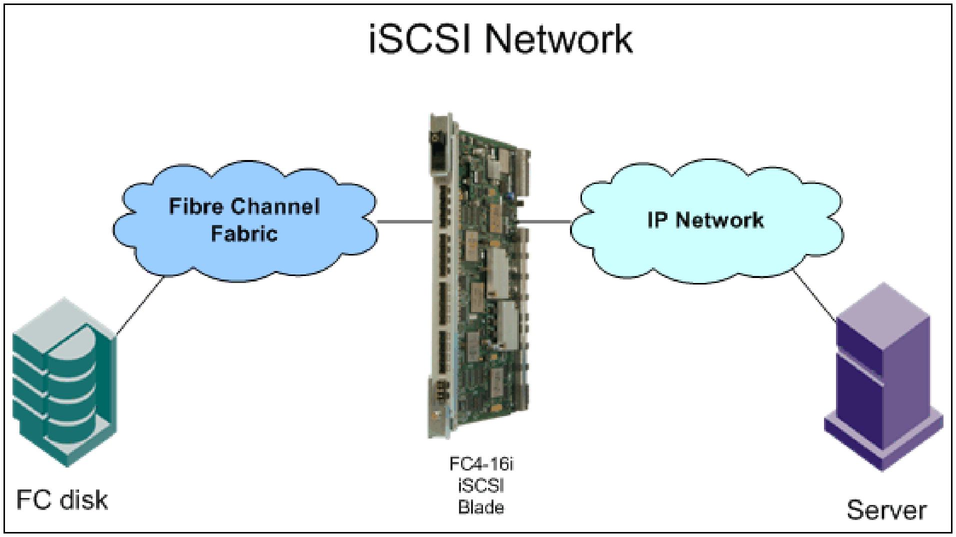


Figure 1-4 iSCSI network

For performance reasons, iSCSI allows what is called a *phase-collapse*, which is when a command and its associated data are shipped together from initiator to target, and responses and data can be shipped together from the target.

An iSCSI name specifies a logical initiator or target. It is not tied to a port or hardware adapter. When multiple network interface cards (NICs) are used, they should generally all present for the target host the same iSCSI initiator name to the targets because they are paths to the same SCSI layer. In most operating systems, the named entity is the operating system image.

The architecture of iSCSI is outlined in IETF RFC 3720, “Internet Small Computer Systems Interface (iSCSI),” available at the following web page:

http://www.ietf.org/rfc/rfc3720.txt

Figure 1-5 shows the format of the iSCSI packet.

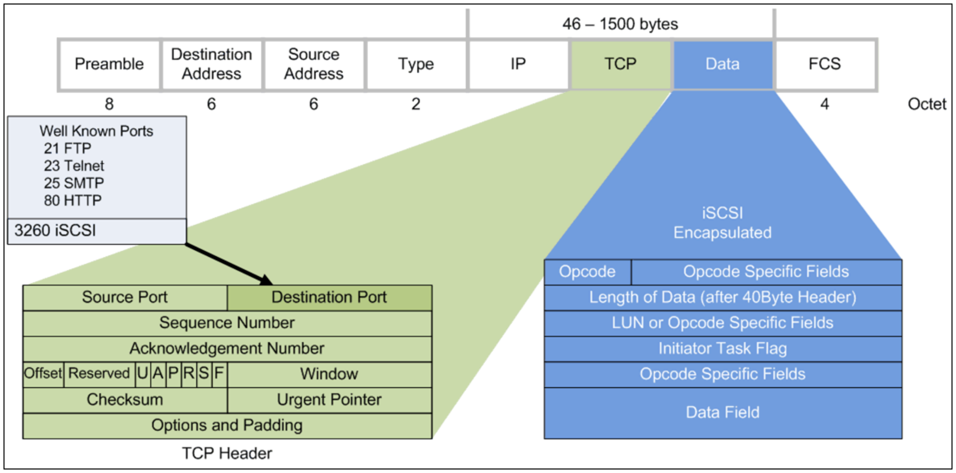


Figure 1-5 iSCSI packet format

Testing on iSCSI latency has shown a best case difference of up to 1 ms of additional latency for each disk I/O as compared to Fibre Channel. This comparison does not include such factors as trying to use iSCSI I/O over a shared, congested, or long-distance IP network, all of which might be tempting for some clients. iSCSI generally uses a shared 1 Gbps network. Section 1.3.3, “Round-trip delay” on page 10 also applies to iSCSI operations.

iSCSI naming and discovery

The three ways for an iSCSI initiator to understand what devices are in the network are as follows:

- In small networks, you can use the **`sendtargets`** command.
- In medium to large networks, you can use the Service Location Protocol (SLP, multicast discovery).
- In the larger networks, using Internet Storage Name Service (iSNS) when possible is considered a best practice.

You can find a range of drafts that cover iSCSI naming, discovery, and booting at the following web page:

http://www.ietf.org/proceedings/02mar/220.htm

1.3 Routing issues

The topics in this section briefly describe issues associated with a routed Fibre Channel environment.

1.3.1 Packet size

The standard size of a Fibre Channel packet (frame) is 2,148 bytes, and the standard IP packet size is 1,500 bytes (with a 1,460 byte payload). Therefore, every Fibre Channel frame is split in two (fragmented), to be transported over a standard IP network. To avoid this fragmentation, you can use jumbo IP packets to accommodate the larger Fibre Channel packets. Keep in mind that jumbo IP packet support must be enabled in every piece of LAN equipment for the entire data path. In addition, a jumbo IP packet is not compatible with any devices in the network that do not have a jumbo IP packet enabled.

Alternatively, you can introduce a variety of schemes to split Fibre Channel packets across two IP packets. Some compression algorithms can allow multiple small Fibre Channel packets or packet segments to share a single IP packet.

Each technology and various vendors can implement this differently. They all strive to avoid sending small, inefficient packets.

1.3.2 TCP congestion control

Sometimes, standard TCP congestion mechanisms might not be suitable for tunneling storage. Standard TCP congestion control is designed to react quickly and severely to network congestion, and recover slowly. This approach is well-suited to traditional IP networks, which are somewhat variable and unreliable. However, for storage applications, this approach is not always appropriate and might cause disruption to latency-sensitive applications.

When three duplicate unanswered packets are sent on a traditional TCP network, the sending rate backs off by 50%. When packets are successfully sent, the sending rate does a slow-start linear ramp-up again. The minimum send rate is normally set as follows:

```
minimum = maximum/20
```

Some vendors tweak the back-off and recovery algorithms. For example, the tweaking causes the sending rate to drop by 12.5% each time congestion is encountered, and then to recover rapidly to the full sending rate by doubling each time until full-rate is regained.

Other vendors take a simpler approach to achieve much the same end. Rather than introduce new algorithms, they suggest the following setting:

```
minimum = maximum x 0.8
```

If you share your IP link between storage and other IP applications, using either of these storage-friendly congestion controls can affect your other applications.

You can find the specification for TCP congestion control on the following web site:

http://www.ietf.org/rfc/rfc2581.txt

1.3.3 Round-trip delay

Round-trip time link latency (also known as RTT) is the time duration for a packet to make a round-trip across the link. The term *propagation delay* is also sometimes used. Round-trip delay generally includes both inherent latency and delays as a result of congestion. This topic can be critical to the success of your long-distance network and must be well understood when discussing or determining what the application will be. If the application requires fast responses to its I/O, the need for multiple packets per I/O can be a problem.

Be sure that you understand all relevant factors, including the following factors:

- Latency is cumulative.
- Switches and routers add a small amount of latency.
- Calculations can get close, but reality is as important.
- Verify the amount of latency by using a utility (for example, **`ping`**).

Fiber optic cable has an inherent latency of approximately 5 µs per kilometer each way (or 10 µs RTT). Typical Fibre Channel devices, such as switches and routers, have inherent latencies of around 5 µs each way. IP routers might vary in the range of 5–100 µs in theory, but when tested with filters applied, the results are more likely to be measured in milliseconds. In many cases, this measurement can quickly jump to exceed the acceptable level of the applications being run.

This approach is the essential problem with tunneling Fibre Channel over IP. Fibre Channel applications are generally designed for networks that have round-trip delays measured in microseconds (µs). IP networks generally deliver round-trip delays measured in milliseconds or tens of milliseconds. Internet connections often have round-trip delays measured in hundreds of milliseconds. This type of delay can be unacceptable to a synchronous remote mirroring application.

Remember, round-trip delay is the total of the network, so all latency parts caused by additional routers and firewalls along the network connection also need to be added to the total delay. The total round-trip delay varies considerably depending on the models of routers or firewalls used, network configurations, and the traffic congestion on the link.

If you are purchasing the routers or firewalls, a best practice is to include the latency of any particular product in the criteria that you use to choose the products. If you are provisioning the link from a service provider, a best practice is to include at least the maximum total round-trip latency of the link in the service level agreement (SLA).

Time of frame in transit

The time of frame in transit is the actual time that it takes for a given frame to be passed across the link. The measurement is purely for the transfer time and not for processing or the acknowledgement to be returned. Each frame transfer will have its own measurement because it depends on both the frame size and link speed to be determined.

The maximum size of the payload in a Fibre Channel frame is 2112 bytes. The Fibre Channel headers add 36 bytes to this, for a total Fibre Channel frame size of 2148 bytes. If possible, when transferring data, use Fibre Channel frames at or near the full size. This approach is especially true when transferring over long distances.

If we assume that we are using jumbo frames in the Ethernet, the complete Fibre Channel frame can be sent within one Ethernet packet. The TCP and IP headers and the Ethernet medium access control (MAC) add a minimum of 54 bytes to the size of the frame, giving a total Ethernet packet size of 2202 bytes, or 17616 bits.

For smaller frames, such as the Fibre Channel acknowledgement frames, the time in transit is much shorter. The minimum possible Fibre Channel frame is one with no payload. With FCIP encapsulation, the minimum size of a packet with only the headers is 90 bytes, or 720 bits.

Table 1-1 shows the transmission rates and theoretical times for transmitting these FCIP packets over certain common wide area network (WAN) link speeds.

Table 1-1 FCIP packet transmission times over different WAN links

Link type	Link speed	Large packet	Small packet
Gigabit Ethernet	1250 Mbps	14 µs	0.6 µs
OC-12	622.08 Mbps	28 µs	1.2 µs
OC-3	155.52 Mbps	113 µs	4.7 µs
T3	44.736 Mbps	394 µs	16.5 µs
E1	2.048 Mbps	8600 µs	359 µs
T1	1.544 Mbps	11 400 µs	477 µs

Remember that the speed of a network is no faster than its slowest segment.

If we cannot enable jumbo frame support, each large Fibre Channel frame must be fragmented into two Ethernet packets. This doubles the amount of TCP, IP, and Ethernet MAC usage for the data transfer.

Normally, each Fibre Channel operation transfers data in only one direction. The frames going in the other direction are close to the minimum size.

1.3.4 Write acceleration

Write acceleration, or *fast write* as it is commonly called, is designed to help mitigate the problem of the high latency of long-distance networks. Write acceleration eliminates the time spent waiting for a target to tell the sender that it is ready to receive data. The idea is to begin sending the data before the target has sent the ready signal, knowing that the ready signal will almost certainly arrive as planned. Data integrity is not jeopardized because the write is not assumed to have been successful until the final acknowledgement has been received.

Note: IBM System Storage DS8000®, IBM System Storage DS6800, and IBM Enterprise Storage Server® already use similar technology for remote mirror and therefore do not benefit from write acceleration in the SAN.

All other IBM storage products should gain from enabling write acceleration in the SAN.

Figure 1-6 shows a standard write request.

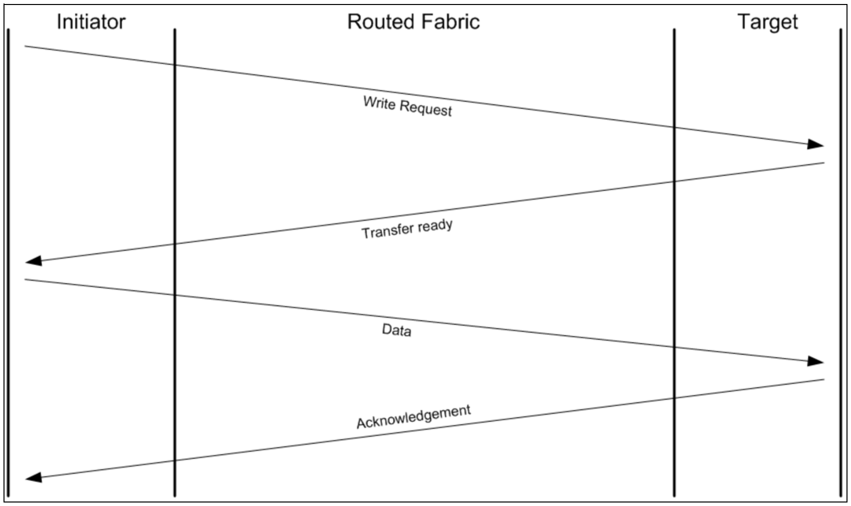


Figure 1-6 A standard write request

Figure 1-7 shows an accelerated write request.

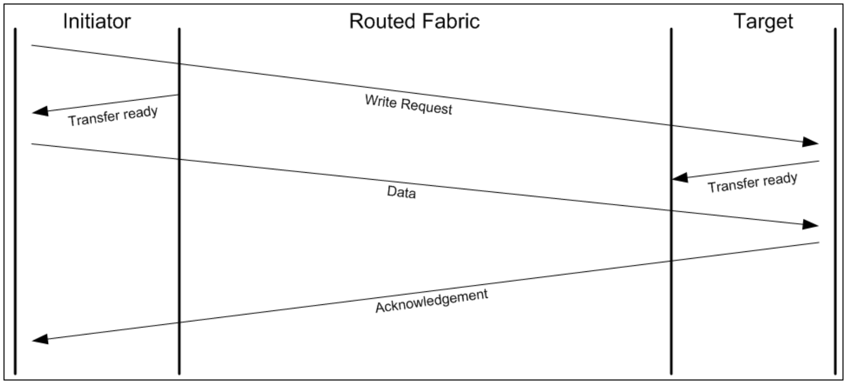


Figure 1-7 Write acceleration or fast write request

1.3.5 Tape acceleration

Tape acceleration (TA) or Tape Pipelining takes write acceleration one step further by spoofing the transfer ready and the write acknowledgement. This gives the tape transfer a better chance of streaming rather than running stop and start. The risk here is that writes have been acknowledged but might not have completed successfully.

Without tape acceleration, a sophisticated backup and restore application, such as IBM Tivoli® Storage Manager, can recover and restart from a broken link. However, with TA, Tivoli Storage Manager believes that any write for which it has received an acknowledgement must have completed successfully. The restarting point is therefore set after that last acknowledgement. With TA, that acknowledgement was spoofed so it might not reflect the real status of that write.

Tape acceleration provides faster tape writing at the cost of recoverability. Although the write-acknowledgments are spoofed, the writing of the final tape mark is never spoofed. This process provides some degree of integrity control when using TA.

Figure 1-8 shows how you can use tape acceleration to improve data streaming.

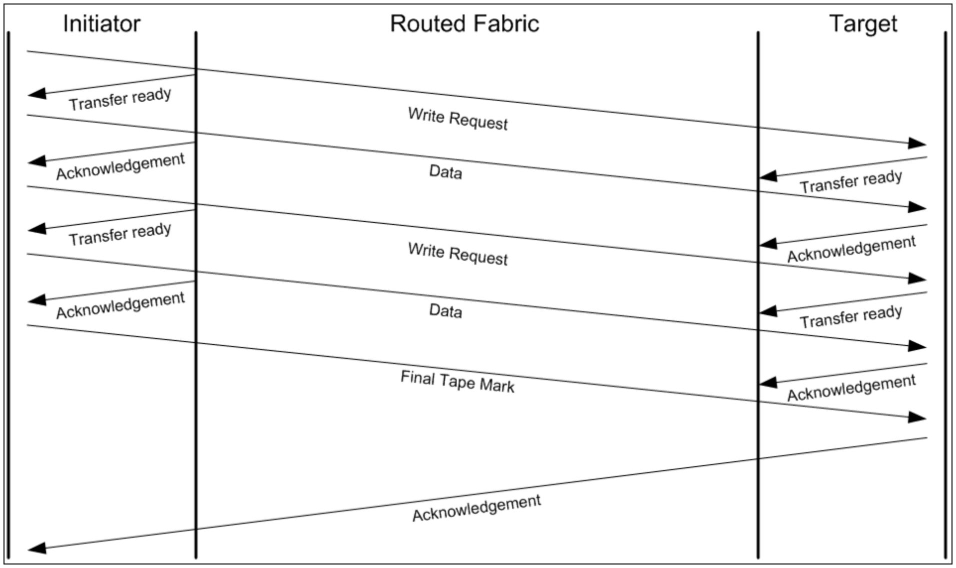


Figure 1-8 Tape acceleration example

1.4 Multiprotocol scenarios

The solutions described in this section show how you can use multiprotocol routers.

1.4.1 Dividing fabrics into sub-fabrics

Suppose that you have eight switches in your data center, and they are grouped into two fabrics of four switches each. Two of the switches are used to connect the development/test environment, two are used to connect a joint-venture subsidiary company, and four are used to connect the main production environment.

The development and test environment does not follow the same change-control disciplines as the production environment. Also, systems and switches can be upgraded, downgraded, or rebooted on occasion.

In this scenario, the joint-venture subsidiary company is for sale. The mandate is to provide as much separation and security as possible between the three functional groups. In summary, we have a requirement to provide a degree of isolation and a degree of sharing. In the past, this would have been accommodated through zoning. Some fabric vendors might still recommend that approach as the simplest and most cost-effective. However, as the complexity of the environment grows, zoning can become more complex. Any mistake in setup or changes can disrupt the entire fabric. In larger fabrics with many switches and separate business units, for example, in a shared services hosting environment, separation and routing are of great value for creating a larger number of simple fabrics, rather than a few, more complex fabrics.

If using virtual fabrics also, you can apply additional separation within a physical fabric.

1.4.2 Requirement to share devices across fabrics

Consider the backup/restore environment for our scenario that is to be shared among the three new fabric environments.

Adding FC-FC routing to the network allows each of the three environments to run separate fabric services and still provides the capability to share the tape backup environment.

Note: FC-FC routing can provide departmental isolation and accommodate resource sharing.

Note: The above two requirements can be also met by having the Integrated Routing License which allows the FC-FC routing feature to be integrated into the SAN switch which is explained more detailed in **Chapter 9, “FC-FC routing implementation” on page 149**.

1.4.3 Connecting a remote mirrored site over IP

Suppose you want to replicate your disk system to a remote site, perhaps 50 km away synchronously, or 500 km away asynchronously. Using FCIP tunneling, you can transmit your data to the remote disk system over a standard IP network. The router includes Fibre Channel ports to connect back-end devices or switches and IP ports to connect to a standard IP wide area network router. Standard IP networks are generally much lower in cost to provide and maintain than traditional high-quality dedicated dense wavelength division multiplexing (DWDM) networks. They also have the advantage of being understood by existing internal operational staff.

Similarly, you might want to provide storage volumes from your disk system to a remote site. You can do this by using FCIP tunnelling. As mentioned earlier, this might not work for all applications because the performance and reliability is not as fast or dependable as that of the Fibre Channel SAN.

Note: FCIP can provide a low-cost way to connect remote sites using familiar IP network disciplines.

1.4.4 Connecting hosts using iSCSI

Many hosts and their applications do not require high-bandwidth low-latency access to storage. High performance-oriented applications in this type of environment are not ideal. But for hosts with low usage or tolerant applications, iSCSI can be a more cost-effective connection method. iSCSI can be thought of as an IP SAN. There is no requirement to provide Fibre Channel switch ports for every server, or to purchase Fibre Channel host bus adapters (HBAs), nor to lay fiber-optic cable between storage and servers. iSCSI hosts have a special initiator driver that is loaded to support the device mapping.

The iSCSI blade or routers have both Fibre Channel ports and IP ports to connect servers located either locally over the LAN, or remotely over a standard IP wide area network connection.

Note: The iSCSI router is effectively the iSCSI target. Each iSCSI initiator, such as the server, is mapped to a worldwide name (WWN) generated by the router. Regarding the Fibre Channel disk system, it sees each initiator as a separate Fibre Channel attached server. Fibre Channel logical unit numbers (LUNS) are mapped to iSCSI Qualified Names (IQNs) generated by the router. As far as the iSCSI initiator is concerned, it sees iSCSI targets.

The iSCSI connection delivers block I/O access to the server, so it is application independent. That is, an application cannot really differentiate between direct SCSI, iSCSI, or Fibre Channel, because all three are delivering SCSI block I/Os.

Different router vendors quote different limits on the number of iSCSI connections that are supported on a single IP port.

iSCSI places a significant packetizing and depacketizing workload on the server CPU. This can be mitigated by using TCP/IP offload engine (TOE) Ethernet cards. However, because these cards can be expensive, they tend to undermine the low-cost advantage of iSCSI.

Note: You can use iSCSI to provide low-cost connections to the SAN for servers that are not performance-critical.

2

Multiprotocol routing terminology and concepts

This chapter presents terms and concepts related to the IBM System Storage b-type storage area network (SAN) multiprotocol routing solution. It also defines terms related to the iSCSI blade for the IBM director-type family of SAN-switches. The Internet small computer system interface (iSCSI) is an industry standard specified by the Internet Engineering Task Force (IETF).

We described basic iSCSI concepts in Chapter 1, “SAN routing introduction” on page 1. For further information regarding iSCSI, consult the following documents:

- *TCP/IP Tutorial and Technical Overview*, GG24-3376
- *Using iSCSI Solutions' Planning and Implementation*, SG24-6291

> **Note:** Concepts and terms in this chapter relate to Fabric OS v6.4.1.

2.1 SAN multiprotocol routing terminology

Multiprotocol routing introduced capabilities to create hierarchical Fibre Channel (FC) networks spanning multiple separate FC fabrics.

SAN multiprotocol routers provide selective data connectivity through hardware-enforced access control but prevent fabric services from propagating between fabrics. As a result, FC fabrics remain separate entities even though a data path exists between them. This approach is similar to the Internetworking world, where separate IP subnets are interconnected using IP routers and firewalls.

Table 2-1 provides a review of the specific terminology that is used throughout the remainder of this book.

Table 2-1 SAN multiprotocol routing terminology

Term	Explanation
FC router	A device that can route traffic between otherwise disjointed FC fabrics through its FC-FC routing service. In this book, it is similar to SAN multiprotocol router.
E_Port	A port on an FC switch or router that connects to another switch or router, forming an ISL. If the devices previously formed separate fabrics, these fabrics can merge, putting all fabric services into one distributed image.
VE_Port	An FCIP capable port on an FC router (FCR) can be configured as a *Virtual E_Port*. This is physically an IP/Ethernet interface, but it *looks* like an FC E_Port to the fabric. An FCIP tunnel between VE_Ports *looks* like an ISL to the fabric.
EX_Port	FCRs use EX_Ports instead of E_Ports on interfaces enabled for FC-FC routing. To connect an FCR to an FC switch, you connect its EX_Port to the switch’s E_Port through an appropriate cable. FCRs use E_Ports or VE_Ports to form backbone fabrics.
VEX_Port	In addition to supporting VE_Ports, FCIP capable ports can be configured as *Virtual EX_Port*s. This is physically an IP/Ethernet interface, but it *looks* like an FC EX_Port to the fabric. VEX_Ports connects to VE_Ports to form inter-fabric links (IFLs).
ISL	The connection between two E_Ports is an *inter-switch link*.
IFL	The connection between an E_Port and an EX_Port is an *inter-fabric link*.

Term	Explanation
Tunnel	The FCIP connection between FCRs is a tunnel. A tunnel can contain one logical ISL or IFL.
Edge fabric	This is Fibre Channel fabric connected to a router through an EX_Port (IFL). This is, for the most part, where the hosts and storage are attached.
Backbone fabric	FCRs provide a backbone (BB) fabric to interconnect routers for more scalable and flexible FC-FC routed SANs. Each router can have many edge fabric connections, but only one BB fabric. FCRs connect to the BB fabric through E_Ports, and all N_ and NL_ port connections on an FCR are part of the BB fabric. With Fabric OS based FCRs, hosts and storage devices can be connected to the BB fabric. All non-FCR ports in a director are part of the BB fabric.
MetaSAN	The collection of edge fabrics and backbone fabrics that are interconnected is called a *metaSAN*. A metaSAN can be compared to the combined IP networks forming an Internet.
Fabric ID	Each edge fabric has a fabric ID (FID) that is unique within the metaSAN. The same FID must be configured on all EX_Ports connected to that edge fabric. The backbone fabric must also have a unique FID configured.
Front domain (phantom domain)	Each router connected to an edge fabric through EX_Ports projects a front (phantom) domain (FD) to that edge fabric. Behind each FD is a path to the *translate domains*. Backbone fabrics do not have front domains.
Translate domain (phantom domain)	A translate (phantom) domain (xlate) represents the remote fabric in which an imported device exists. Only a single translate domain is projected for each remote fabric, regardless of the number of imported devices being imported from each remote fabric.
LSAN	Logical SANs are zones that span fabrics while traversing at least one EX_Port or VEX_Port. For a device to be imported/exported between fabrics, an LSAN zone must exist in both the importing and the exporting fabric. LSANs are how connectivity is configured across routers.
FC-NAT	Fibre Channel Network Address Translation is how devices are presented to the fabrics into which they have been imported. It can be compared to IP NAT.
FCRP	Fibre Channel Router Protocol is used between FCRs to coordinate their activities. FCRP can operate on backbone attached E_Ports and edge domain attached EX_Ports.

Figure 2-1 shows a metaSAN with three edge fabrics connected to a single backbone fabric.

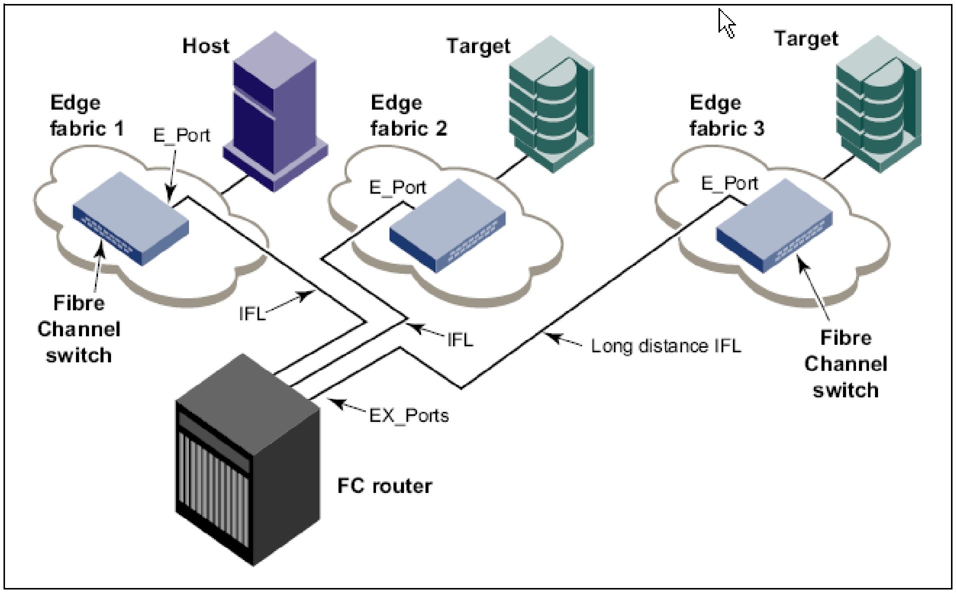


Figure 2-1 MetaSAN with three edge fabrics connected to a backbone fabric

The switches in an edge fabric treat an IFL as a normal ISL. Through the IFL, the switches gain access to a set of phantom domains that are never principal domains in the edge fabric. Two types of phantom domains are created in the edge fabric:

- A front domain (FD) is created in the edge fabric to represent each router that connects to the edge fabric through EX_Ports. Prior to Fabric OS v5.2, a separate front domain would be created for each EX_Port link.
- Every remote edge fabric that has at least one node exported to the local edge fabric is represented by a single translate domain (xlate). Even if a remote fabric has multiple FC switches or is exporting multiple nodes, just one translate domain is projected into the local edge fabric to represent the entire remote fabric.

The phantom domains can have the following connections:

- The virtual links connecting front domains to translate domains are called *phantom links*.
- The exported nodes of a remote fabric represented by port addresses connected to the translate domain are called proxy devices.

The translate domains are used to perform FC-NAT between the different edge fabrics. The translate domain IDs persist across router reboots and can be assigned manually.

The front domains are used to provide multiple paths to the translate domains through the different IFLs that are available and allow normal Fabric Shortest Path First (FSPF) routing across the paths.

When counting the hop count in the complete metaSAN, you must count the ISLs and IFLs as hops. You do not need to count the phantom links, because they are not physical links and do not add any delay to the data path.

The port IDs (PIDs) of the proxy devices follow the specific format 0xAABBBB, where:

- AA is the translate domain for the remote fabric where the physical device is attached.
- BBBB is the virtual slot number in the range 0xf001–0xffff.

The virtual slot numbers can be assigned automatically, or you can assign them manually.

Because the proxy device PID usually differs from the PID in the source fabric, the PID cannot be used as a unique identifier throughout the metaSAN. The device worldwide name (WWN), however, stays the same, and therefore a WWN is a unique identifier in a metaSAN. Because of this, LSAN members must be represented by port WWNs or aliases for these.

> **Note:** Some operating systems, such as IBM AIX® 5L™ or HP-UX, by default assume that the PID of any device stays constant. If you have any servers that are subject to this behavior, define both the translate domain IDs and the virtual slot numbers manually to ensure that they remain constant.

Figure 2-2 shows the logical view of an edge fabric with four IFL connections to another edge fabric. The entire remote edge fabric is represented as a translate domain.

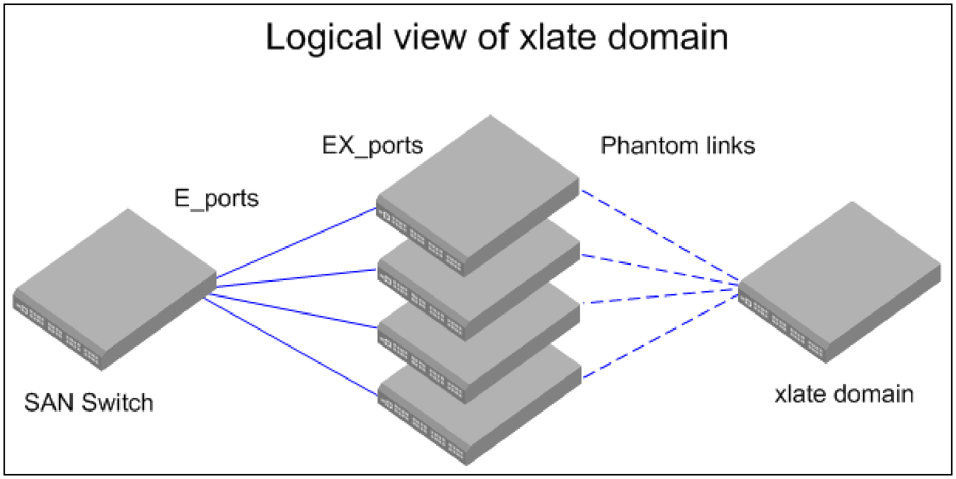


Figure 2-2 Edge fabric logical view of remote fabric

To support FCIP tunneling across IP networks, we introduce the virtual E_Port (VE_Port) and virtual EX_Port (VEX_Port). These virtual ports are physically connected to the Gigabit Ethernet (GbE) ports and represent FCIP tunnel end points.

VE_Ports function exactly as E_Ports, and an ISL connection is created between two VE_Ports.

VEX_Ports function exactly like EX_Ports, and an IFL connection is created between a VEX_Port and a VE_Port.

Figure 2-3 shows ISL and IFL connections created using FCIP tunnels between two SAN routers.

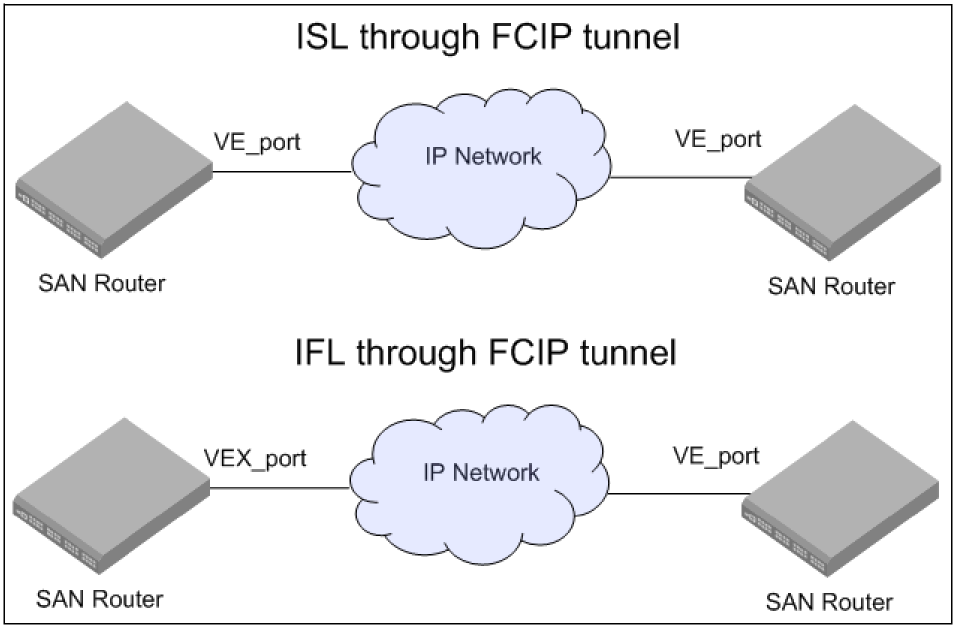


Figure 2-3   ISL and IFL connections through FCIP tunnels

2.1.1 Zone configurations

A zone configuration is a group of one or more zones. A zone can be included in more than one zone configuration. When a zone configuration is in effect, all zones that are members of that configuration are in effect.

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during the business hours and another enabled overnight. However, only one zone configuration can be enabled at a time.

The types of zone configurations are as follows:

- Defined configuration

  This type is the complete set of all zone objects defined in the fabric.

- Effective configuration

  This type is a single zone configuration that is currently in effect. The effective configuration is built when you enable a specified zone configuration.

- Saved configuration

  This type is a copy of the defined configuration plus the name of the effective configuration, which is saved in flash memory. (You can also provide a backup of the zoning configuration and restore the zoning configuration.) Differences might exist between the saved configuration and the defined configuration if you have modified any of the zone definitions and have not saved the configuration.

- Disabled configuration

  The effective configuration is removed from flash memory.

2.1.2 Fabric OS 6.4.0 changes

With the 6.4.0 firmware of Fabric OS, there are some changes in the Traffic Isolation (TI) Zones. These changes are listed here:

- Device ports can now be in multiple Traffic Isolation Zones at the same time.
- Devices in a failover disabled TI zone are able to communicate with local devices that are not part of the same TI zone.

  Prior to Fabric OS 6.4.0, devices would need to be in a failover enabled TI zone to communicate with local devices.

- Domain Controller connectivity between the switches never affect the TI zones

> **Note:** These new features are supported in the Condor2 and GoldenEye2 ASICs. They are not supported on the 8Gbps blades for DCX.

In the following sections we expand on the changes made.

Overlapping TI Zones with failover disabled

Even with failover disabled it is now possible to have devices in more than one zone. By enabling this feature, a link failure will not affect the alternative path.

The best way to illustrate this new change is by example and we will use Figure 2-4. In it we have a Channel Device that is a member of both the green and red zones with failover disabled. We also have two Control Units (CU), A and B, that are members of the two zones.

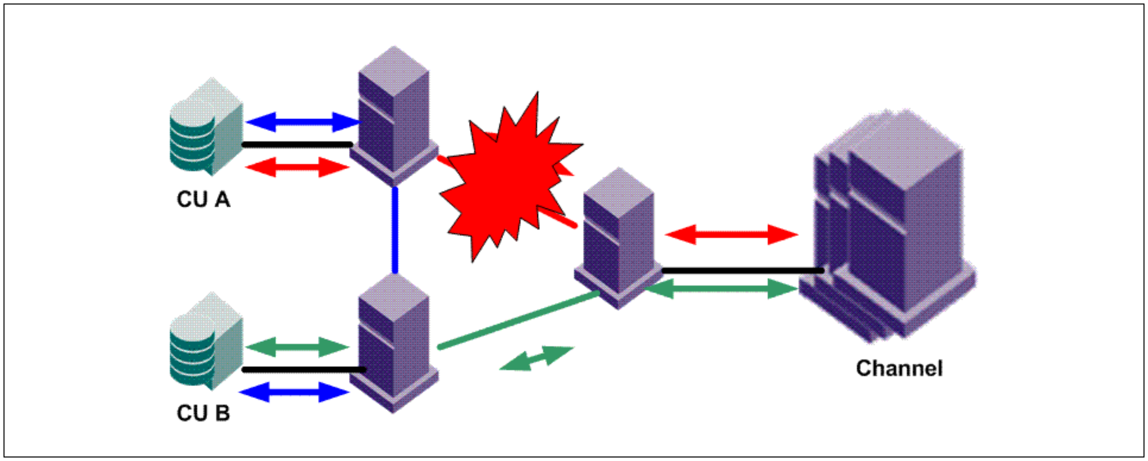


Figure 2-4 Link failure on TI Zone with failover disabled

This example illustrates how devices can now be members of multiple TI zones. The Channel is a member of both the green and the red TI zones, which have failover disabled. CU A is member of the red and blue zones and CU B is member of the green and blue zones.

In the event of an ISL failure, which in our example would be the ISL between the Channel and CU A, that takes the link offline, communication with CU B is maintained. However, the traffic between the Channel and CU A is halted because failover is disabled.

Local device communication

The devices that are members of a TI zone can now communicate with local devices that are not member of the failover disabled TI zone. In versions prior to 6.4, this communication would be blocked.

In Figure 2-5, we see that now it is possible that a host can communicate with a local device event. In this example, the host needs access to the tape library using a dedicated failover disabled TI zone (in blue), and also to the local storage. The green zone in the figure represents this new capability to access local devices, even when the host is connected to a failover disabled zone.

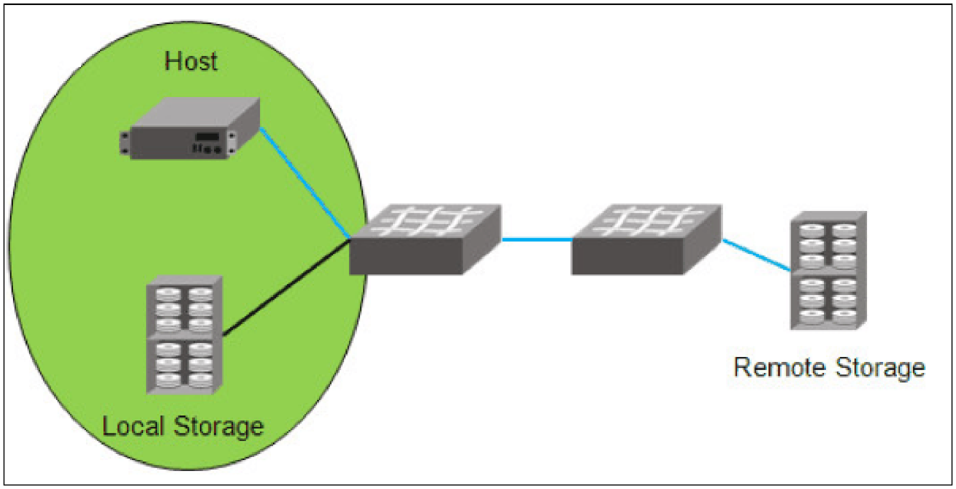


Figure 2-5 Example of local device communication

Domain controller only routes

As an example let's say we have three domain controller links between three switches. They are installed in such a way that switch 2 is between switch 1 and 3. The links between switch 1 and 2 are failover enabled, and the one between switch 2 and 3 is not.

Consider a link failure between one of the two links in the communication of switch 1 and switch 2. Prior to version 6.4, in case of a link failure between more than two switches, if the main ISL between the two switches was down, the first switch would not be able to connect to the third switch by the second switch in a case of a failover disabled zone configuration between switch 1 and switch 3. Now, even in a case of link failure between the first two controllers, the communication will reach the third controller.

Note: Domain Controller refers to switch-to-switch communication coming from the embbeded port PID 0xFFFFxx (where xx is the domain ID). This traffic is for switch-to-switch management and updated within a fabric. The traffic information will be updated on all the elements of the fabric that are connected to the management port.

2.2 Overview of the FC-FC routing solution

To demonstrate the SAN multiprotocol routing terms, we create a small metaSAN consisting of two single-switch edge fabrics and a single FCR backbone fabric. Each edge fabric has two IFL connections to the router for redundancy. The IFL connections are not trunked, and EX_Ports project different front domains into the edge fabrics (front domain consolidation is not used).

The fabric parameters are set as follows:

- Fabric 1
  - Core PID format: 1
  - Domain ID used: 1
  - Fabric ID: 1
- Fabric 2
  - Core PID format: 0
  - Domain ID used: 1
  - Fabric ID: 2

Because we use a different core PID format in the fabrics, we cannot merge them into a single fabric. We also use the same domain ID on both fabrics. Changing either of these parameters would be disruptive to the fabric, and requirements might exist that mandate the specific setup. We must enable the server that is connected to fabric 1 to access a storage device that is connected to fabric 2. We implement this by creating an LSAN called LSAN_A_Zone.

Figure 2-6 shows the layout of our environment.

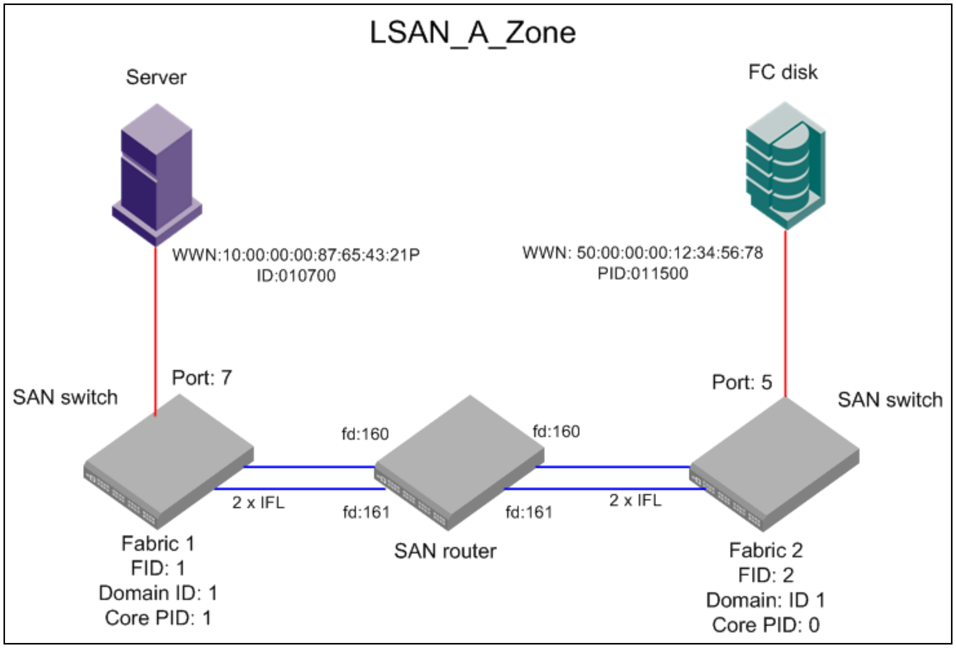


Figure 2-6 FC-FC routing example layout

The FC router (FCR) automatically assigns a separate front domain for each IFL in each edge fabric, starting from a default preferred domain ID 160. The front domain IDs must be unique only within a single edge fabric, and the same front domain ID can be assigned in several different edge fabrics.

We create the LSAN by creating a zone named LSAN_A_Zone in both fabric 1 and fabric 2. The zone has two members: the port WWNs 10:00:00:00:87:65:43:21 and 50:00:00:00:12:34:56:78 (server and storage device).

The FCR automatically intercepts any zone with a name starting with “LSAN_”, and scans for LSAN members (port WWNs) present in more than one LSAN zone. If found, LSAN members are imported/exported in edge fabrics using FC-NAT.

In our case, we assume that fabric 2 is given translate domain ID 5 in fabric 1, and fabric 1 is given translate domain ID 6 in fabric 2. Any fabric 2 members exported to fabric 1 are represented in fabric 1 by proxy devices with PIDs starting from 05f001. Any fabric 1 members exported to fabric 2 are represented in fabric 2 by proxy devices with PIDs starting from 06f001.

Figure 2-7 shows the logical view seen by the server in fabric 1.

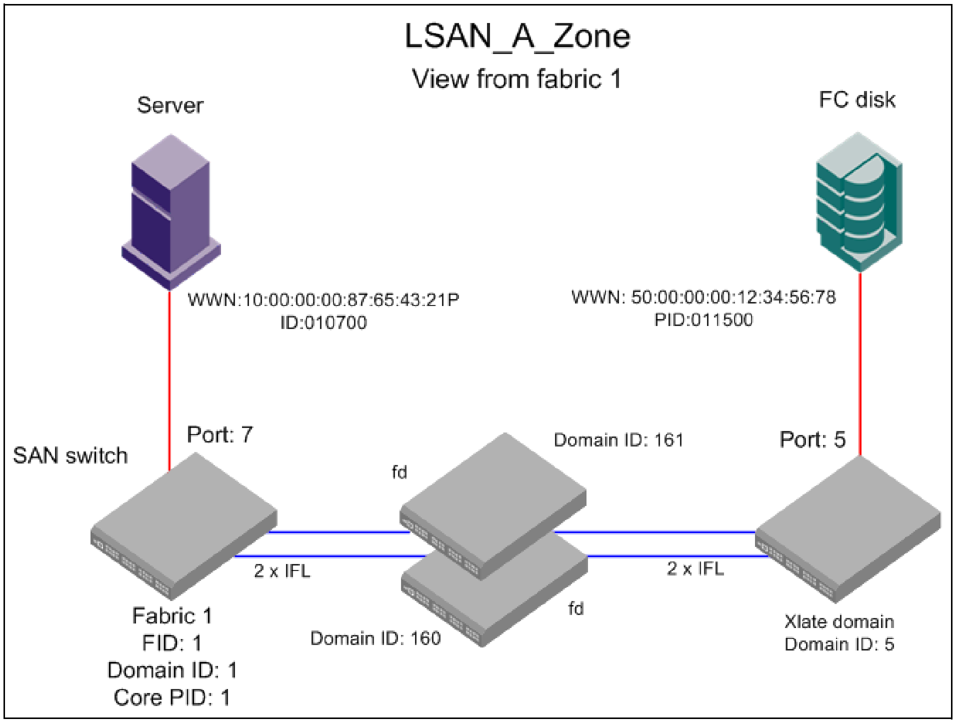


Figure 2-7 Logical view from fabric 1

Figure 2-8 shows the logical view seen by the storage device in fabric 2.

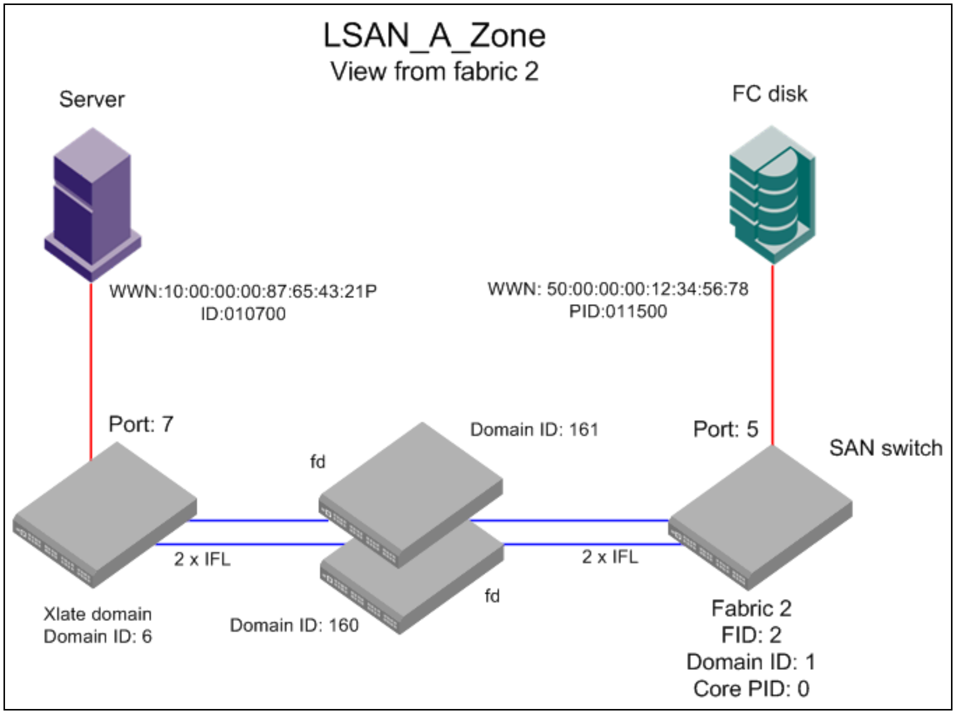


Figure 2-8 Logical view from fabric 2

The WWNs of the LSAN members are not changed by the FC-NAT. This way you can still use the real WWN of the server for logical unit number (LUN) masking in the storage device.

2.3 iSCSI terms

Table 2-2 lists terms that are used to describe the iSCSI gateway service found on the iSCSI blade for the SAN256B director.

Table 2-2 iSCSI terminology

Term	Explanation
Discovery domain	A group of iSCSI virtual targets and iSCSI initiators. Discovery domains (DDs) are used for access control and authentication. Only the iSCSI initiators in the same DD as the iSCSI virtual targets can connect to the FC targets. When there are no DDs, all iSCSI initiators can access all iSCSI virtual targets (no access control). A discovery domain is analogous to a zone object in FC SANs.
Discovery domain set	A group of DDs that can be enabled or disabled. The active discovery domains set (DDSet) enforces the fabric-wide iSCSI virtual target access. Only the DDs in the active DDSet are enforced. Multiple DDSets can be created, but only one DDSet can be active at a time. A discovery domain set is analogous to a zoning configuration in FC SANs.
FC portal	An FC port that connects the iSCSI virtual initiators to the FC SAN. These ports reside as internal ports on the iSCSI blade and connect to the M48 switching backplane.
iSCSI virtual initiator	Proxies between iSCSI initiator to iSCSI virtual targets connections and the physical FC target on the SAN. Each iSCSI-enabled port has one iSCSI virtual initiator (iSCSI VI). An iSCSI VI is similar to an F_Port in a FC fabric. The iSCSI VI registers with the Simple Name Server (SNS) using a symbolic port WWN and node WWN.

IQN	iSCSI Qualified Name. An iSCSI address that uniquely identifies an iSCSI device in the network. It is the equivalent of an FC WWN and is in human readable form. The IQN format is:
	`iqn.yyyy-mm.<reversed domain name>:<user part>`
	The iSCSI blade uses the default IQN format:
	`iqn.1924-02.com.ibm:2109-m48port:<WWN of FC target>`

iSCSI initiator	In client/server terminology, a client that connects to a service (iSCSI virtual target) offered by the server (iSCSI gateway). It is identified by an IQN that uniquely identifies it in the network. The iSCSI initiator proxies communications between applications and data located on a remote SCSI device.

Term	Explanation
iSCSI portal	An iSCSI-enabled port on an iSCSI blade that is assigned an IP address and connected to the IP network. This port receives the iSCSI initiator connection to the iSCSI virtual target. The port is bound to an iSCSI virtual target that connects to the FC target in the FC SAN.
iSCSI portal group	A set of iSCSI-enabled ports. The portal group allows the iSCSI VI to access iSCSI virtual targets using any available port. An iSCSI session can have several connections to an iSCSI virtual target on any port in the group. The portal group name is the slot number of the blade. All online iSCSI-enabled GbE ports participate in the portal group.
iSCSI virtual target	An iSCSI representation of LUNs from one or more FC targets. The physical FC LUN is mapped to the iSCSI virtual targets (iSCSI VT). It is identified by an IQN. The iSCSI gateway proxies the iSCSI initiator's connection using iSCSI VTs.
iSCSI connection	A single link between an iSCSI initiator and an iSCSI VT over a TCP/IP network that carries control messages, SCSI commands, parameters, and data.
iSCSI session	The basic communication pipe from an iSCSI initiator to an iSCSI VT. A session is a group of TCP/IP connections that link an iSCSI initiator with an iSCSI VT. Connections can be added or removed from a session. Sessions are identified by a session ID (iSCSI SSID).
iSCSI LUN mapping	The mapping of the iSCSI VT and the FC target.

3

b-type family multiprotocol routing products

This chapter introduces the storage area network (SAN) multiprotocol routing products or the extension products found in the IBM System Storage family of SAN products. We examine the hardware and software characteristics of the products, and list possible product applications. Current capabilities and limitations of the products are listed together with interoperability information.

We also describe several products that have reached or are about to reach end-of-life, because they are still likely to be encountered in the SAN environment.

It is beyond the scope of this book to cover all the common aspects and features of the IBM System Storage family of SAN products. Only concepts and features relevant to SAN multiprotocol routing are covered in depth. For more detailed information about general aspects of the IBM System Storage family, refer to IBM Redbooks publication *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

3.1 IBM System Storage Multiprotocol routers

The IBM System Storage multiprotocol routers are designed to enable specific protocol routing capabilities and consolidation of SAN islands for infrastructure simplification, without the need to merge the SAN islands into one large SAN. This capability can be used through the interconnection of existing Fibre Channel (FC) fabrics, or it can allow SAN designers to realize new solutions based on a hierarchal networks approach.

The IBM System Storage family features the following products for use with SAN multiprotocol routing:

- IBM System Storage SAN06B-R (2498-R06)
- IBM TotalStorage SAN18B-R (2005-R18)
- IBM TotalStorage SAN04B-R (2005-R04)
- The IBM TotalStorage SAN768B (2499-384) and The IBM TotalStorage SAN384B (2499-192) directors with multi protocol routing / extension blades
  - IBM FC 3890- FCIP extension blade,
  - IBM FC 3850 -FCIP extension blade
- The IBM TotalStorage SAN256B (2109-M48) director with the multi protocol routing / extension blades
  - FC3450 FCIP extension blade
  - FC3460 iSCSI blade

These products are all part of the second-generation IBM System Storage SAN multiprotocol routing products, which are based on the Fabric OS operating system. The first-generation product, based on XPath OS, SAN16B-R (2109-A16) SAN multiprotocol router, has been withdrawn from marketing.

> **Note:** The features and capabilities listed in this chapter assume Fabric OS v6.4.1

3.1.1 IBM System Storage SAN06B-R (2498-R06)

IBM System Storage SAN06B-R (2498-R06) is a rack-based product with 8 Gbps FC routing, switching capabilities along with Fibre Channel Over IP (FCIP) hardware feature. This has 16 8 Gbps FC ports and 6 GbE ethernet ports. Figure 3-1shows the IBM System Storage SAN06B-R (2498-R06).

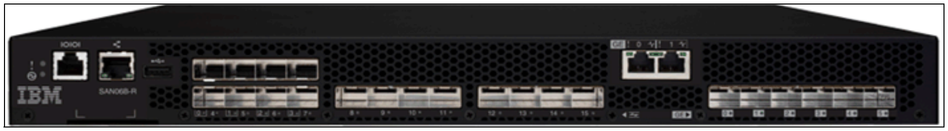


Figure 3-1 IBM System Storage SAN06B-R

This model is available in two different configurations, as a Base Fabric Switch configuration which comes with four active 8 Gbps FC ports and two active 1 GbE ports. It can be upgraded with an additional 12 8 Gbps FC ports and four 1GbE ports. Figure 3-2 shows the base ports and the upgrade license enabled ports.

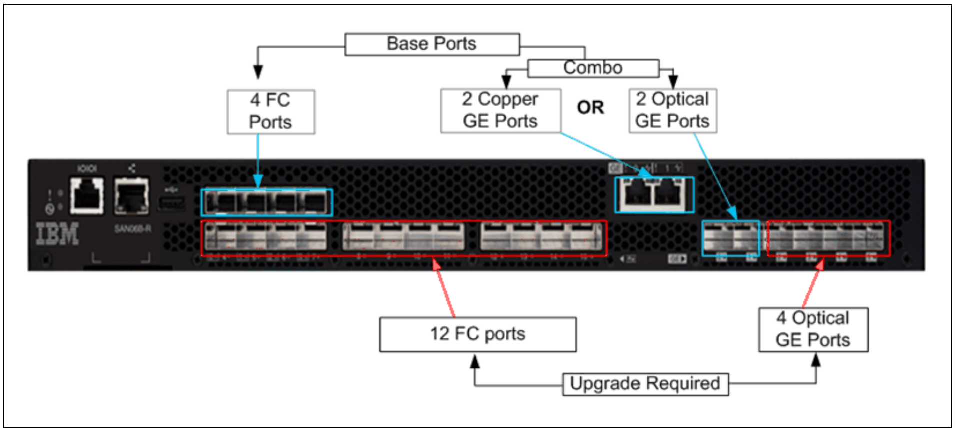


Figure 3-2 San 06B-R (2498-R06) Ports

IBM System Storage SAN06B-R licensed features

Some of the capabilities of the SAN06B-R (2498-R06) switch require feature licenses. These include the following capabilities:

- The SAN06B-R (2498-R06) upgrade license to enable full hardware capabilities, full FCIP tunnel capabilities, support of advanced capabilities such as open systems tape pipelining (OSTP), FICON® CUP support, and separately licensed advanced FICON acceleration capabilities.
- The Advanced Extension License to enable FCIP trunking and Adaptive Rate Limiting (ARL).
- The Advanced FICON acceleration license to enable accelerated tape read/write and accelerated data mirroring over distance in FICON environments.
- The IR is required for FCR. The IR license is required to configure VEX_ports.

The features supported on the base and fully license upgraded SAN06B-R (2498-R06) are listed in Table 3-1. For further more detailed information about HW and features, refer the *Installation, Service and User Guide*, GC27-2270-01, available from IBM support web page:

http://www.ibm.com/support

Table 3-1 Supported Features on Base and Upgraded SAN06B-R

Feature	**Base SAN06B-R**	**License upgraded SAN06B-R**
Number of Fibre Channel ports	4	16
Number of GbE ports	2	6
Fibre Channel routing between remote fabrics for fault isolation (Licensed)	Yes	Yes
FCIP Tunnel	Yes	Yes
Number of FCIP tunnels	2	8
FCIP Trunking (Licensed)	Yes	Yes
Adaptive Rate Limiting (Licensed)	Yes	Yes
FC frame compression	Yes	Yes
Storage optimized TCP	Yes	Yes
Fast Write over FCIP tunnel	Yes	Yes
Open Systems Tape Pipelining over FCIP tunnel	No	Yes
FICON XRC emulation and Tape Pipelining over FCIP (Licensed)	No	Yes
FICON CUP (Licensed)	No	Yes

Management tools

SAN06B-R can be managed with the standard tools similar to the other b-type SAN switches using Webtools, CLI, SNMP, DCFM or with a dedicated management server

FCIP Trunking

FCIP trunks are built by creating a set of FCIP circuits. FCIP circuits create multiple source and destination addresses for routing traffic over a WAN, providing load leveling and failover capabilities over FCIP tunnels. The collection of one or more circuits between two switches is referred to as the tunnel. Figure 3-3 shows the view of tunnel and circuits in the SAN06B-R.

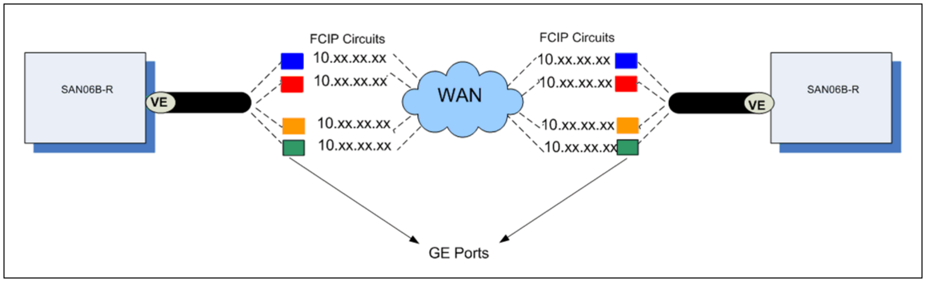


Figure 3-3 FCIP Circuits and tunnel in SAN06B-R

3.1.2 SAN18B-R and the SAN04B-R

IBM System Storage SAN18B-R (2005-R18) and SAN04B-R (2005-R04) are rack-based products with 4Gb FC routing, switching and the FCIP hardware features. These two switches are based on the same hardware platform with the 4 Gbps Condor application-specific integrated circuit (ASIC). The SAN04B-R is the base model with two FC ports and two GbE ports. This base SAN04B-R is upgradeable by applying an additionally purchased license key to become a fully functional SAN18B-R with sixteen FC ports together with two Gigabit Ethernet (GbE) ports.

High performance is assured by the non-oversubscribed 4 Gbps FC ports and the hardware-assisted traffic processing across the GbE ports. Hardware-based compression, large window sizes, and selective acknowledgement of IP packets optimize performance of IP traffic as well, although the SAN04B-R is rate limited to 50 Mbps on each GbE port.

Both the SAN18B-R and SAN04B-R come in a 1U form factor for standard 19-inch rack mount. Figure 3-4 shows the SAN18B-R. The SAN04B-R looks the same except for the product labeling.

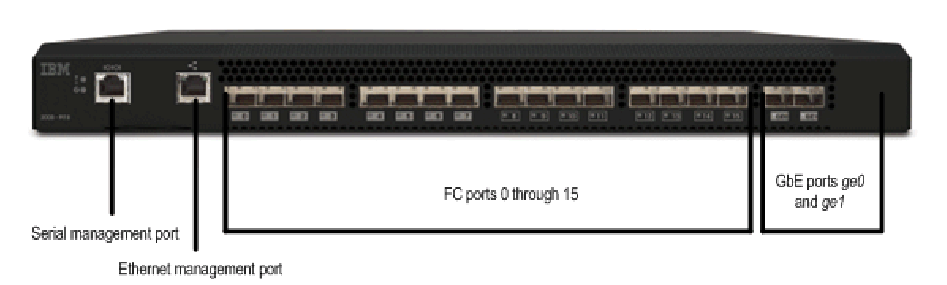


Figure 3-4 SAN18B-R (2005-R18)

With the ability to route between FC SANs, these routers can provide metropolitan and global SAN extension for business continuity solutions. This is accomplished by using the existing Metro Area Network (MAN) or Wide Area Network (WAN) IP infrastructure. The SAN18B-R can configure up to eight virtual Fibre Channel over IP (FCIP) tunnels per GbE/IP port; the SAN04B-R is limited to one tunnel per port, to provide scalability and efficient use of MAN and WAN resources.

Both routers can be managed by using the same integrated management tools as the rest of the IBM System Storage b-type family. This approach allows simple installation, configuration, and everyday administration.

Hardware components

The SAN18B-R and SAN04B-R offer high-speed FC and IP ports for excellent performance. In addition, hot swap redundant power supplies and fans provide high availability. We discuss these hardware components in the following sections.

Fibre Channel ports

The routers have 16 FC ports, numbered 0–15. Only ports 0 and 1 are enabled for use on the SAN04B-R. The FC ports support FC-FC routing services with auto-negotiated speeds up to 4 Gbps. In addition to the FC routing capabilities, the ports also support traditional FC connection services, such as F-port, FL-port, and E-port. You can use a variety of Small Form Pluggable (SFP) modules with the FC ports, including both short and long wavelength modules. An LED below each FC port indicates the operational status of the port.

On the SAN18B-R and SAN04B-R the configuration and port management utilities, found in Web Tools, show 32 ports, numbered 0–31. Ports 0–15 are the

16 physical FC ports. Ports 16–23 represent the virtual ports assigned to FCIP tunnels defined on the Gigabit Ethernet port 0 (GE0) and ports 24–31 represent the virtual ports assigned to FCIP tunnels defined on the Gigabit Ethernet port 1 (GE1).

> **Note:** The SAN04B-R is licensed for FC ports 0 and 1 only.

Gigabit Ethernet ports

Two GbE ports support the FCIP and FC-FC routing services at link speeds of 1 Gbps. The ports are labelled **GE0** and **GE1**. On the SAN18B-R, you can configure up to eight FCIP tunnels on each GbE port. Therefore, there are eight virtual ports allocated to each physical GbE port. The virtual ports can be configured as either VE_Ports (fabrics merge through the FCIP tunnel) or as VEX_Ports (fabrics do not merge). Virtual ports 16–23 represent the eight FCIP tunnels across physical port GE0, and virtual ports 24–31 correspond to the eight tunnels across GE1. As with the FC ports, the GbE ports use SFP modules to interface with the LAN/WAN.

> **Note:** The SAN04B-R is rate limited to 50 Mbps and only supports a single FCIP tunnel per GbE port.

Standard and optional features

The SAN18B-R and SAN04B-R include with the following standard features:

- Web Tools
- Advanced zoning
- FC-FC routing service (EX_Ports)
- Fabric Watch
- FC Extended Fabrics support

> **Note:** Web Tools and Advanced Zoning are part of the base Fabric OS (FOS) after FOS v6.1.0. In FOS v6.1.0 and later, these licenses might be recognized as “Unknown1” and “Unknown2.” Do not be alarmed or remove these licenses if you have to downgrade to a previous FOS version.

The following features are optional and require an additional license:

- High-performance Extension License includes IPSec, Fast Write and Tape Pipelining over FCIP and FC, and hardware-based data compression included on the SAN04B-R
- FCIP activation
- Advanced Performance Monitoring
- ISL trunking

Note: The Advanced Security license, also known as Secure Fabric OS (SFOS), is still available as an optional feature for Fabric OS v5.3.0 on the SAN18B-R. However, because SFOS is replaced by the ACL feature, this license should only be required for interoperability with existing SFOS-based environments.

Web Tools

Web Tools is a comprehensive set of management tools that use a web browser interface. To launch the Web Tools, point a supported browser to the management IP address. Through Web Tools, you can upgrade, configure, and manage the SAN18B-R and SAN04B-R routers.

FC-FC routing service

The Fibre Channel to Fibre Channel (FC-FC) routing service enables devices in separate FC SAN fabrics to communicate across routers without actually merging the fabrics. The entire routed SAN network consisting of several SAN fabrics is known as a metaSAN.

The FC-FC routing service is also able to connect to IBM TotalStorage® m-type family FC SANs natively and either interconnect with other m-type FC SANs or interconnect with b-type based FC SANs. Using this feature m-type fabrics can enjoy the same metaSAN features as b-type fabrics.

Advanced Zoning

Advanced Zoning provides hardware-enforced access control over fabric resources to prevent unauthorized access. Zone membership can be specified at port, AL-PA, and WWN level. It also simplifies heterogeneous storage management.

Fabric Watch

Fabric Watch tracks a variety of SAN fabric elements, events, and counters. Monitoring fabric-wide events, ports, transceivers, and environmental parameters permits early fault detection and isolation as well as performance measurement. Fabric Watch lets administrators define how often to measure each switch and fabric element and specify notification thresholds. Event notification is possible through either simple mail transfer protocol (SMTP), simple network management protocol (SNMP), or UNIX syslog daemon.

FC Extended Fabrics support

The Extended Fabrics feature provides native FC connectivity over longer distances up to 500 kilometers. Extended Fabrics is ideal for deploying single, distributed fabrics over dark fiber or dense wavelength division multiplexing (DWDM)-based network connections. These extended distance connections use standard switch ports that provide E_Port or EX_Port interconnectivity over extended long wave transceivers (SFPs), Fibre Channel repeaters, and DWDM devices. When Extended Fabrics is installed, E_Ports can be configured with a large pool of buffer credits. The enhanced switch buffers help ensure that data transfer can occur at near full bandwidth to efficiently use the long-distance connection.

High-performance Extension (FCIP)

FCIP provides extension of FC SANs over longer distances across IP networks. Basically, the FC traffic is encapsulated within IP packets, which are transferred across the IP network. Native FC connectivity is much more expensive over long distance than IP connectivity, and this is usually the primary reason for FC over IP implementation. With FCIP, you can extend your SANs across thousands of kilometers at a sensible cost.

The FCIP activation license also permits the use of the Fast Write function for either FCIP or FC connections. Fast Write mitigates the distance-imposed latency effects for Small Computer System Interface (SCSI) write operations when the initiator and target are geographically dispersed. Fast Write enables the entire data segment of a SCSI write operation to be transported across a long distance without the inefficiencies of transfer-ready commands to travel back and forth across the link. By not having to wait for potentially numerous round-trip protocol handshake messages, the SAN multiprotocol router can expedite transfer of the SCSI write operation, significantly improving throughput.

Note: The Fast Write feature cannot be active for both FC and FCIP connections at the same time.

Advanced Performance Monitoring

The Advanced Performance Monitoring feature identifies end-to-end bandwidth use and provides useful information for capacity planning. In addition to capacity planning, it can also be used for troubleshooting.

ISL trunking

The ISL trunking feature enables FC frames to be efficiently load balanced across multiple physical ISL connections, while preserving in-order delivery. Up to eight 4 Gbps links can be combined to set up a single logical ISL connection with up to 32 Gbps throughput per trunk. As with other 4 Gbps IBM products, trunking is implemented masterless, meaning that a failure on any of the links in the trunk does not cause disruptions to traffic or the fabric.

Similar trunking capabilities are also available on inter-fabric links (IFLs) going from EX_Ports on a router to the same edge fabric. As with ISL trunking, up to eight 4 Gbps IFLs can be combined into a single logical IFL for a maximum throughput of 32 Gbps per trunk. IFL trunks are not masterless, and if the master link fails the trunk will be taken off for a short period of time for reconfiguration.

Together with fabric shortest path first (FSPF) enhancements such as Traffic Isolation (TI) zones and dynamic load sharing (DLS), ISL and IFL trunking provide the best possible use of all paths in the metaSAN.

3.2 IBM SAN Director blade options

IBM System Storage SAN768B (2499-384), SAN384B (2499-192), and IBM TotalStorage SAN256B (2109-M48) directors are designed to meet the highest performance and availability demands, in a modular, high density single chassis design. With no single point of failure on active components, these directors provide larger data centers with high throughput and high availability.

These directors integrate a passive switch backplane with expansion slots open for various types of blade modules. The two center slots contain the two redundant control processor (CP) blades, the SAN768B and SAN384B has an additional two slots for redundant core switching blades, leaving eight or four slots open respectively for a user-configurable selection of blades.

Figure 3-5 shows the SAN768B and SAN256B directors with various blades installed.

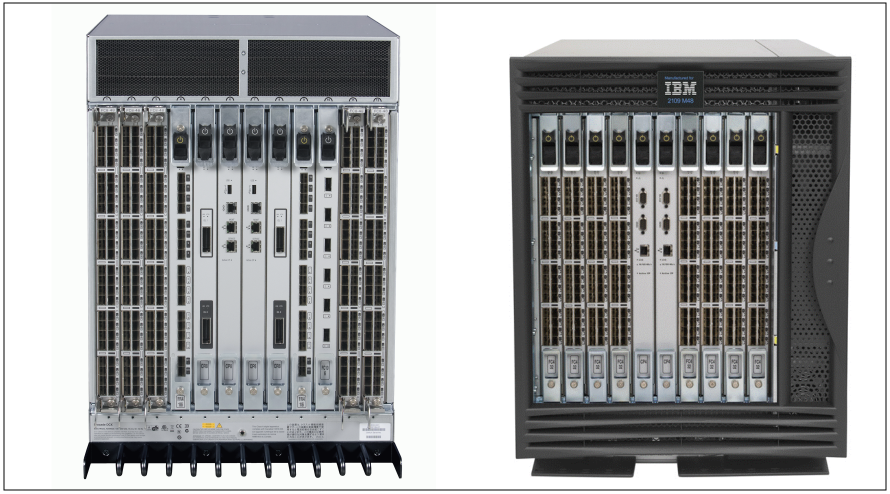


Figure 3-5 SAN768B (2499-384) and SAN256B (2109-M48) directors

Figure 3-6 shows SAN384B director with optional 48-port FC blades installed.

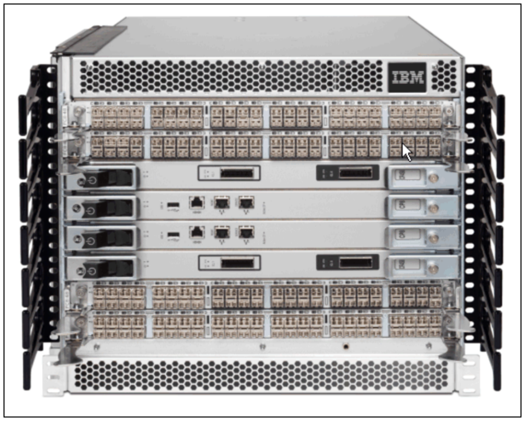


Figure 3-6 SAN384B (2499-192)

All of these directors can be populated with optional multiprotocol blades as described in Table 3-2.

Table 3-2 Multiprotocol blade options

	SAN256B feature code	**SAN384B feature code**	**SAN768B feature code**
8 Gbps Routing Blade	N/A	FC 3890	FC 3890
4 Gbps Routing Blade	FC 3450	FC 3850	FC 3850
iSCSI blade	FC 3460	N/A	N/A

3.2.1 FC Routing Blades

The FC Routing Blade can be installed to provide FC-FC routing and FCIP distance extension capabilities. When installed, the blade turns the director into a fully integrated switching and multiprotocol routing platform, which can be used to realize even the most demanding metaSAN configurations. The iSCSI blade and FC Routing Blade are intelligent blades. In the SAN256B, a maximum combination of four intelligent blades can be installed per chassis. Up to two FC Routing Blades can be installed per chassis, depending on the number of other intelligent blades installed. In the SAN768B and SAN384B, a maximum of four FC Routing Blades can be installed in the same chassis.

Note: Based on evaluation of the environment where the director is placed, an option to install up to two more FC Routing Blades in a SAN256B, also dependent on the number of other intelligent blades installed (giving a total of four), exists through the Request for Price Quotation (RPQ) process. Contact your IBM representative in such cases.

3.2.2 8 Gbps FC Routing Blade - FC 3890

The FC 3890 is the 8 Gbps routing blade that is supported in the SAN768B and the SAN384B. It has 12 FC ports for Fibre Channel routing, 10 1GbE ports for FCIP routing and also an optionally licensed 2 10 GbE ports supporting FCIP.

Figure 3-7 shows the port layout of the blade.

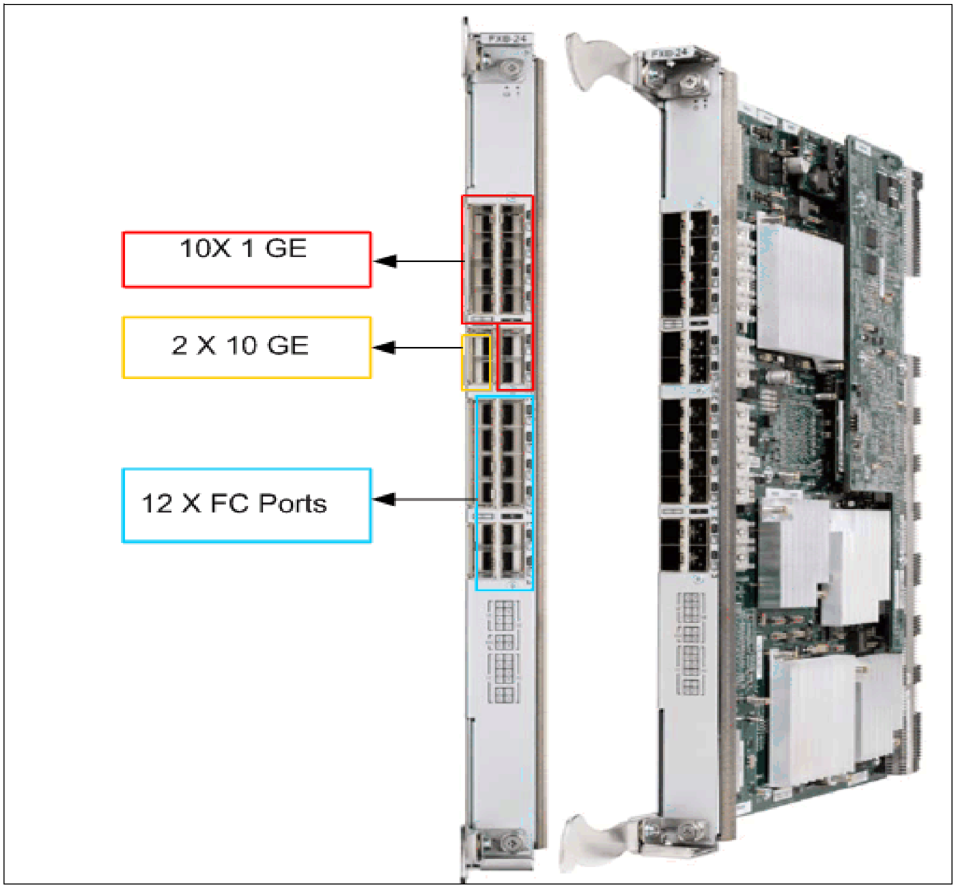


Figure 3-7 8 Gbps Routing Blade FC-3890

8 Gbps Routing blade FC-3890 licensed features

These are optional features of the FC-3890:

- 10 GbE support.
- Advanced FICON acceleration.
- The IR license is required for FCR. The IR license is required to configure VEX_ports.
- The Advanced Extension License is required for FCIP trunking and Adaptive Rate Limiting (ARL).

Modes of operation for GbE ports on the FC-3890

The 8 Gbps routing blade has three modes of operation for the GbE ports:

- 1G only mode: 10X1 GbE ports only can be used.
- 10G only mode: 2 X 10 GbE only can be used.
- Dual mode:10X1 GbE ports and 1 x 10 GbE ports can be used.

The mode of operation of the blade could be identified using the **switchshow** command where it indicates the mode besides the GbE or XGE ports, as shown in Example 3-1.

Example 3-1   switchshow

```
IBM_SAN384B_27:admin> switchshow -slot 1
switchName:     IBM_SAN384B_27
switchType:     77.3
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   16
switchId:       fffc10
switchWwn:      10:00:00:05:1e:94:3a:00
zoning:         ON (IBM_RB)
switchBeacon:   OFF
FC Router:      ON
FC Router BB Fabric ID: 100
Address Mode:   0

Slot   Blade Type     ID   Model Name      Status
-----------------------------------------------------
  1     AP BLADE     75     FX8-24           ENABLED

Index Slot Port Address Media Speed State     Proto
===================================================
..........output truncated for clarity
..............
30    1   30   101e00   --    --   Offline     VE  Disabled
(Persistent)
 31    1   31   101f00   --    --   Offline     VE  Disabled
(Persistent)
       1  ge0           --    1G   No_Module FCIP
       1  ge1           --    1G   No_Module FCIP
       1  ge2           --    1G   No_Module FCIP
       1  ge3           --    1G   No_Module FCIP
       1  ge4           --    1G   No_Module FCIP
       1  ge5           --    1G   No_Module FCIP
       1  ge6           --    1G   No_Module FCIP
       1  ge7           --    1G   No_Module FCIP
       1  ge8           --    1G   No_Module FCIP
       1  ge9           --    1G   No_Module FCIP
       1 xge0           --    10G   No_Module FCIP  Disabled (1G Mode)
       1 xge1           --    10G   No_Module FCIP  Disabled (1G Mode)
```

Note: The Modes “10G only” and “dual mode” can be used only if the 10 Gigabit Ethernet License is available, so the default mode is “1G Mode” for the FC-3890 8 Gbps routing blade. The mode could be changed using the command **`bladecfggemode --set <mode type> -slot <slot number>`**

Scalability of 8 Gbps Routing Blade FC-3890 with VE ports FCIP

The 8 Gbps Routing Blade FC-3890 can support 20 VE_ports therefore 20 FCIP tunnels. The 8 Gbps FCIP routing devices, namely the IBM 06B-R and FC-3890, do not require the VE port to be associated to particular GbE port. In the blade FC-3890 VE ports 12 to 21 can use GbE ports GE0 to GbE 9 os the XGE1.VE ports 22 through 31 can only use XGE1. Total bandwidth availability is 20 Gbps.

Scalability of FCIP Trunking on FC-3890

An FCIP tunnel using GbE ports can have up to four FCIP circuits spread across any four GbE ports. An FCIP tunnel using 10GbE port can have up to 10 FCIP circuits on one 10GbE port. A single circuit can have a maximum of 1Gbps capacity. The scalability of the FCIP tunnel is summarized in Table 3-3.

Table 3-3 Scalability of FCIP tunnel

	Max number of tunnels per 1 GbE port	**Max number of tunnels per 10 GbE port**	**Max number of tunnels per system**
Base SAN06B-R	1	N/A	2
Upgraded SAN06B-R	4	N/A	8
FC-3890 - 8 Gbps Routing Blade			
1GbE only mode	4	N/A	10
Dual mode	4	10	20
10GbE only mode	N/A	10	20

3.2.3 4 Gbps FC Routing Blade

This SAN Routing Blade can be installed with all three IBM b-type directors as indicated in Table 3-2 on page 45. The features of this FC Routing Blade are similar to those of the SAN18B-R. The blade has 16 FC ports and two Gigabit Ethernet ports for IP communication. The FC ports support auto-negotiated speeds up to 4 Gbps. The two Gigabit Ethernet (GbE) can each support up to eight FCIP tunnels.Figure 3-8 shows the 4 Gbps FC Routing Blade.

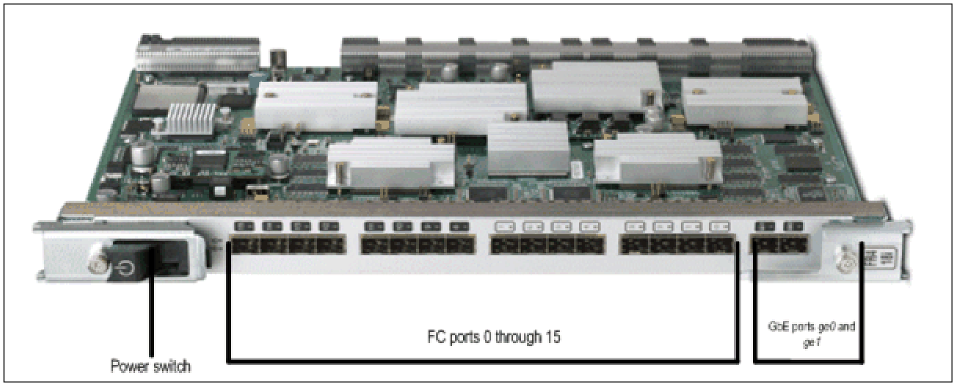


Figure 3-8 4 Gbps FC Routing Blade

Management of this FC Routing Blade integrates into the director’s management interfaces with both CLI and Web Tools GUI. As with the SAN18B-R, management through Data Center Fabric Manager (DCFM) is also possible.

By default, the FC Routing Blade powers up in a disabled state until the FC-FC routing service and the ports are configured and enabled. The router configuration is not stored on the blade itself, but by slot location in the CP. If you move the blade to another slot, the configuration does not follow. It is preserved in the previous slot location. If you install a replacement FC Routing Blade in that slot, it will use the existing slot configuration.

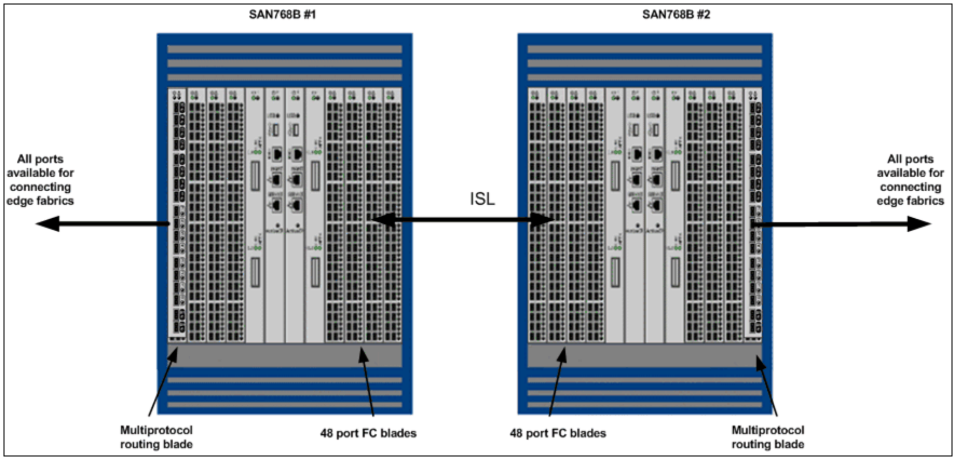
When installed, the FC Routing Blade becomes an integrated part of the director, and, as with all other blades, it is directly connected to the backplane. In comparison to the SAN18B-R or SAN04B-R, this connectivity imposes a difference in terms of scalability. The router blade does not have a ports-on-demand feature.

Because all other ports in the director chassis are directly reachable through the backplane and switching core (they are within the same domain ID), all regular FC ports become part of the FC Routing Blades backbone fabric from a metaSAN perspective. This means that all ports residing on FC port blades are part of the backbone fabric, as the ports on FC Routing Blades that are not configured as EX_Ports or VEX_Ports. Think of this as the FC Routing Blade being extended with more FC ports.

All FC ports on the FC Routing Blade can be used to form IFLs, and the ports on the FC port blades can then be used for interconnecting the switches in the backbone fabric. Besides optimizing the router port usage, this approach allows for the creation of dedicated high-performance backbones with inter-switch bandwidth in the 100+ Gbps range.

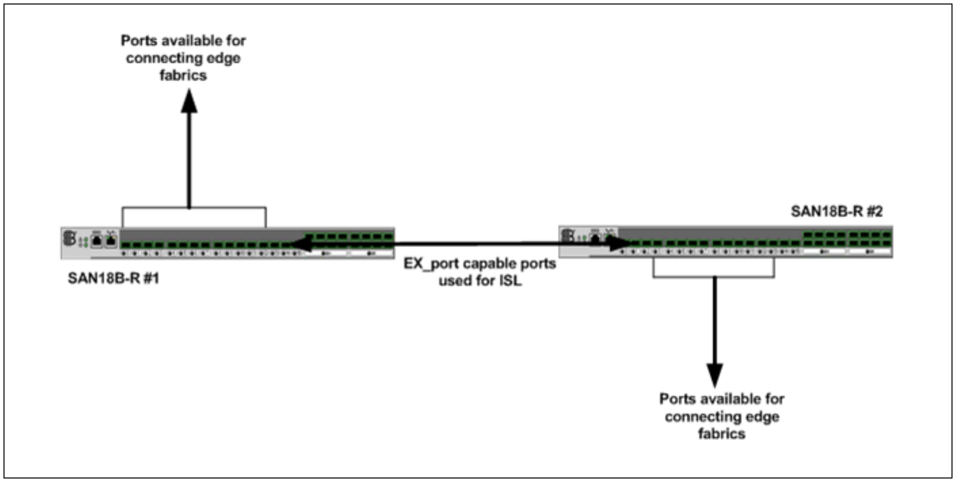
Note: Edge fabric to backbone fabric FC-FC routing is supported in a metaSAN, which means that devices directly connected to switches in backbone fabrics can be accessible to edge fabrics in the metaSAN. On all the IBM SAN Director types of switches, this means that all FC ports can be accessed from edge fabrics connected through IFLs.

Figure 3-9 and Figure 3-10 show how routing ports can be efficiently used with the FC Routing Blade in configurations with backbone fabrics.



SAN768B #1
SAN768B #2
All ports available for connecting edge fabrics
ISL
All ports available for connecting edge fabrics
Multiprotocol routing blade
48 port FC blades
48 port FC blades
Multiprotocol routing blade

Figure 3-9   SAN768Bs connected without using multiprotocol routing capable ports



Ports available for connecting edge fabrics
SAN18B-R #2
SAN18B-R #1
EX_port capable ports used for ISL
Ports available for connecting edge fabrics

Figure 3-10   SAN18B-Rs connected using multiprotocol routing capable ports

Another scalability advantage of using the FC Routing Blade is when more than one blade is inserted into a director chassis. All the blades belong to the same routing entity in the metaSAN, which means that the director as a multiprotocol router has more ports than found on a single multiprotocol routing blade.

Each one of these ports can be directly used as EX_Ports or VEX_Ports without using switch ports to create a backbone fabric between routing entities. All the multiprotocol routing ports in the chassis are managed from the same management interface as the rest of the ports.

Figure 3-11 shows the functional diagram of the 4 Gbps FC Routing Blade. Apart from the backplane connections to the CPs, the SAN18B-R features a similar layout.

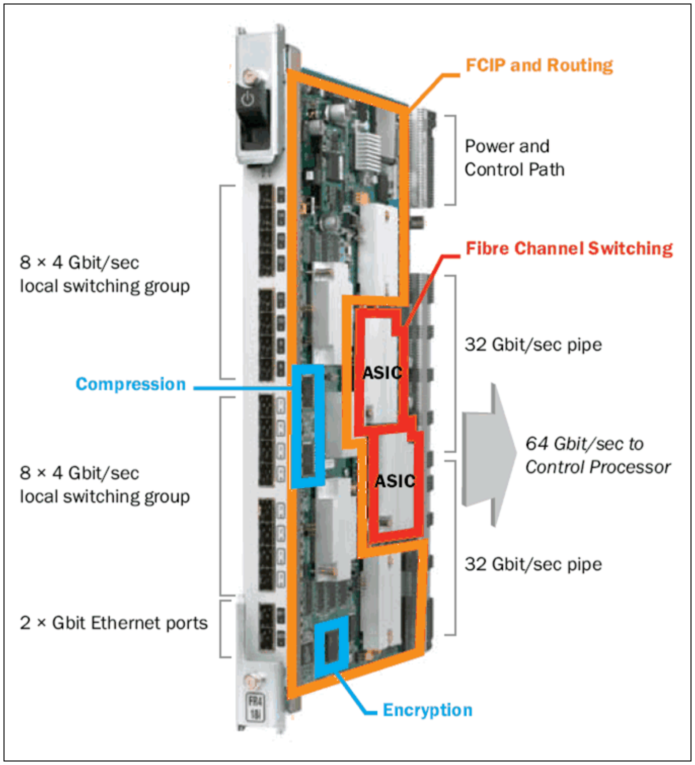


Figure 3-11 Functional diagram of the 4 Gbps FC Routing Blade

Standard and optional features

Available licensed features on the 4 Gbps FC Routing Blade follow the SAN18B-R, except that Enhanced ISL Trunking and Advanced Performance Monitoring licenses are standard (they come with the base director) and that FC Extended Fabrics support is optional.

Pre-Requisites for Routing implementation of SAN 256B

The SAN256B requires additional prerequisites for proper implementation of the FC Routing Blade into a Chassis, as follows (Other than the first bullet, these items are not of concern for the SAN768B and SAN384B directors.):

- For adequate cooling, a best practice is to install one blade in the left-side slot group and the second in the right-side slot group.
- The FC Routing Blade requires that two additional power supplies are installed in the SAN256B director (giving a total of four power supplies).
- The FC Routing Blade requires Fabric OS v5.1.0b or later. You need to make sure that the SAN256B Director is on the appropriate Fabric OS level *before* you install any FC Routing Blade. When the FC Routing Blade is powered on, it will go through the Power On Self Test (POST) procedure and then autolevel with the firmware version in the active CP. If the firmware version is below V5.1.0b, the FC Routing Blade will not work.
- The SAN256B must be running in chassisConfig mode 5. If the SAN256B Director is not in the correct mode, use the **`chassisConfig 5`** command to change it. Be aware that this command is disruptive and requires a reboot.

3.2.4 Integrated Routing in the SAN768B and SAN384B

Integrated routing as described in introduction chapter enables FC switch device to provide FC-FC routing.Table 3-4 lists the FCR-capable 8 Gbps FC port blades.

Table 3-4 8 Gbps FC port blade options

Port blade	SAN768B and SAN384 feature code
16-port blade	FC 3816
32-port blade	FC 3832
48-port blade	FC 3848
64-port blade	FC 3864

The SAN768B with Fabric OS 6.1 and later, and the SAN384B with Fabric OS 6.2.0c and later, can have an Integrated Routing license installed to allow EX_Port configuration on any standard 8 Gbps FC port in the chassis. This approach allows FC-FC routing (FCR) to be configured without requiring an FC Routing Blade in the chassis. A maximum of 128 ports in a SAN768B can be configured as an EX_Port when using Integrated Routing.

Table 3-5 lists the optional licenses for Integrated Routing.

Table 3-5 Optional licenses for Integrated Routing

Model	Integrated Routing license feature code
SAN768B	FC 7889
SAN384B	FC 7890
SAN80B-4	FC 7807
SAN40B-4	FC 7407

Note: The Integrated Routing licences are also available for the SAN80B-4 and SAN40B-4 switches.

Integrated Routing allows any 8 Gbps FC port in a SAN768B and SAN384B to be configured as an EX_port supporting FCR.

FCR support on the 8 Gbps ports is a native capability; hence these ports are referred to as native EX_Ports. This functionality eliminates the need to add a routing blade or use of the SAN18B-R for FCR purposes, and also provides double the bandwidth for each FC router connection when connected to another 8 Gbps-capable port.

FCR capability on native EX_Ports requires the Integrated Routing feature license. Previously, FCR capability was tied to the existence of supported hardware and did not require a separate license.

The Integrated Routing license only affects native EX_Ports. The SAN18B-R EX_Ports and Routing functionality on FCIP ports (VEX_Ports) behave the same as before, regardless of the presence of the Integrated Routing license.

Using both the native EX_Ports and EX_Ports on a routing blade is not supported within a chassis. Only VEX_Ports might be used in the same chassis along with Integrated Routing enabled native EX_Ports (this only applies to the SAN768B and SAN384B because the SAN256B does not support Integrated Routing, even with 8 Gbps blades.)

Notes: If a SAN768B has a FC Routing Blade installed, EX_Ports can be used on either standard FC ports or FC Routing Blade FC ports, but not both.

The SAN256B director does not support Integrated Routing.

3.2.5 iSCSI blade

The iSCSI blade is only an option for installation in the SAN256B directors. It is not supported in the Brocade DCX. The blade provides iSCSI gateway services to lower-end servers or workstations, thereby allowing them to access an FC-based storage infrastructure inexpensively.

Although FC connectivity has remained an optional feature on most servers, all servers today are equipped with Ethernet connections, most of them being GbE-capable. The advent of these standard Ethernet connections was originally intended for accessing IP-based services residing on either a local area network (LAN) or on the Internet. With the increased focus on centralizing storage resources, the demand to have all servers connected to the storage infrastructure has grown. This includes a large number of simple servers where adding FC connectivity is not a feasible option (such as front-end web servers).

iSCSI enables the use of existing IP and Ethernet infrastructures for storage networking. iSCSI is a native IP interconnect that encapsulates SCSI data and commands to transport them on TCP/IP networks.

> **Note:** In the protocol stack, iSCSI resides on top of the Transmission Control Protocol (TCP). iSCSI is an industry standard defined by the Internet Engineering Task Force (IETF). The most current version can be found as a Request For Comments (RFC) document on the RFC Editor web site:
>
> `http://www.rfc-editor.org`

Unlike Fibre Channel, IP networks were not designed with the rigid performance and reliability requirements of storage networking in mind. While applications and operating systems generally tolerate packet loss and varying performance on the LAN, they are built on the assumption that their storage will be fast and reliable. This conceptual difference between FC and IP networks is what has made Fibre Channel the favorite transport for storage data.

This also means that Fibre Channel will not be replaced by iSCSI because core IT systems will continue to demand the performance and reliability offered only by Fibre Channel. Instead, iSCSI complements Fibre Channel and allows servers with less stringent requirements to benefit from having centralized storage available. In fact, for many situations the optimal solution is to have Fibre Channel and iSCSI coexist, with the core IT systems and the storage infrastructure being Fibre Channel-based. Non-FC servers then access this storage infrastructure using an iSCSI-to-FC gateway service that interconnects the IP network with the FC storage services.

Figure 3-12 shows how an iSCSI gateway is placed in the network.

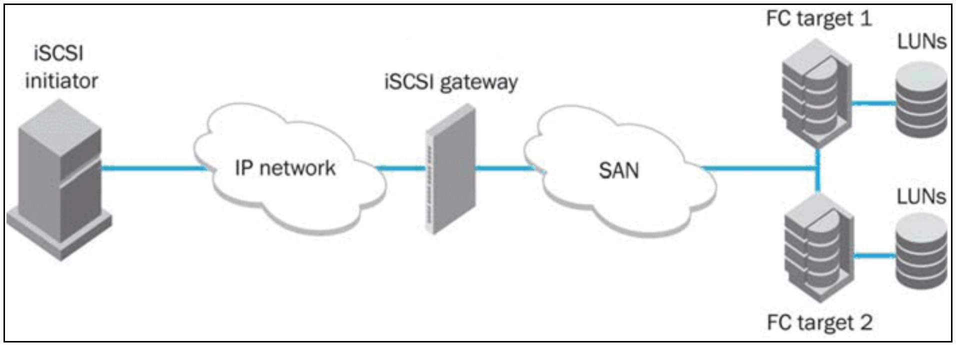


Figure 3-12 iSCSI -to-FC network

The iSCSI blade adds this iSCSI-to-FC gateway functionality only to the SAN256B director, translating iSCSI traffic to Fibre Channel traffic and vice versa.

Figure 3-13 shows the iSCSI blade.

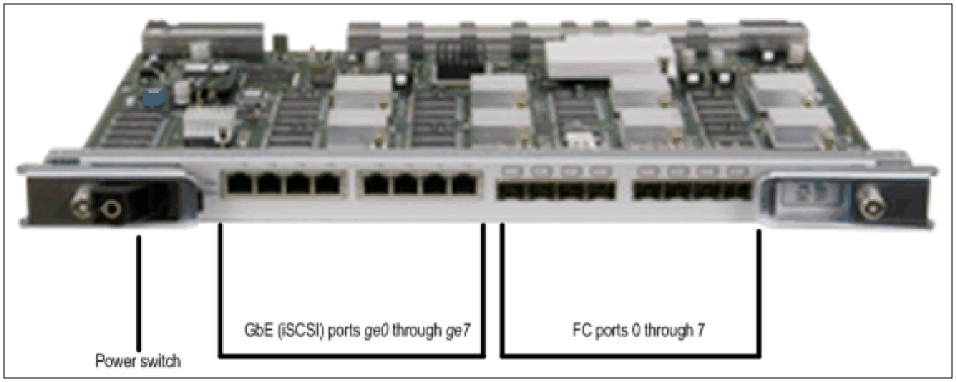


Figure 3-13 iSCSI blade

Using the iSCSI blade, an iSCSI initiator (server) can access a Fibre Channel target (storage device). The iSCSI initiators can either be directly connected to the GbE ports on the iSCSI blade or connected through Ethernet switches. The Fibre Channel targets can be connected directly to the Fibre Channel ports found on the iSCSI blade itself, the normal Fibre Channel ports, or to other switches in the fabric.

The iSCSI blade and FC Routing Blade are intelligent blades. A maximum combination of four intelligent blades can be installed per chassis. Up to four iSCSI blades can be installed per chassis, depending on the number of other intelligent blades installed.

The SAN256B requires additional prerequisites for proper implementation of the iSCSI blade into a chassis:

- A maximum of four iSCSI blades can be installed per chassis.
- The iSCSI blade requires that two additional power supplies are installed in the SAN256B director (giving a total of four power supplies).
- The iSCSI blade requires Fabric OS v5.3.0 or later installed on the SAN256B.
- As for the FC Routing Blade, the SAN256B must be running in chassisConfig mode 5. If the SAN256B Director is not in the correct mode, use the **`chassisConfig 5`** command to change it. This command is disruptive and requires a reboot.

Hardware components

The iSCSI blade offers both high-speed FC and iSCSI ports for enhanced flexibility. In addition, hot swap redundant power supply and cooling is provided by the SAN256B chassis for high availability.

Fibre Channel ports

The iSCSI blade has 8 x 4 Gbps FC ports, numbered 0 through 7. The FC ports support standard FC connections services (E, F, FL ports) at auto-negotiated speeds up to 4 Gbps. You can use a variety of SFP modules with the FC ports, including both short and long wavelength modules. An LED under each FC port indicates the operational status of the port.

Figure 3-14 shows a functional diagram for the iSCSI blade.

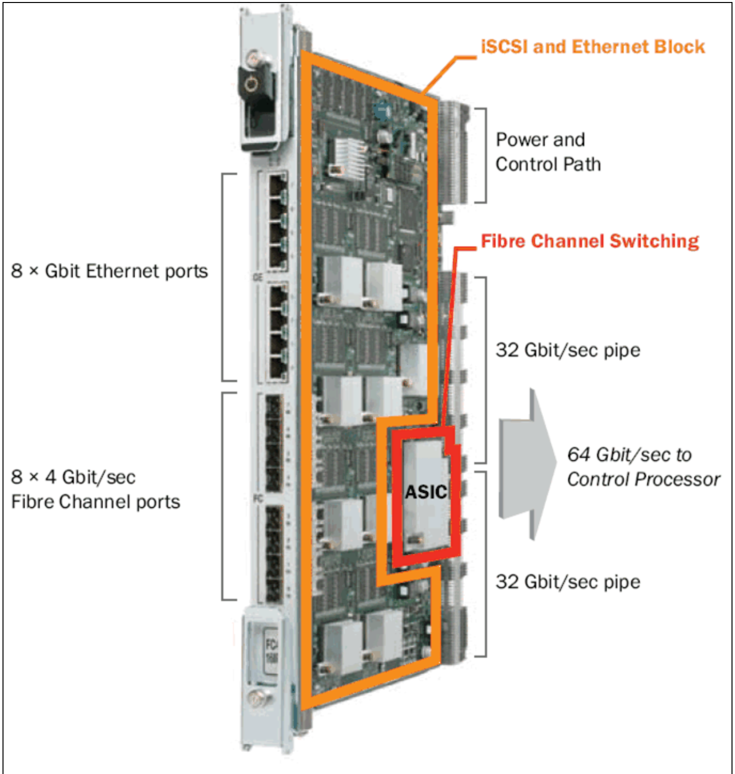


Figure 3-14 iSCSI blade functional diagram

Gigabit Ethernet ports

Eight Gigabit Ethernet ports support the iSCSI service at link speeds of 1 Gbps. The ports are labelled GE0 through GE7 and use standard RJ-45 copper connectors and twisted pair cables (1000BASE-T).

Each GbE can support up to 64 iSCSI initiators, giving a maximum of 512 initiators per blade. With the maximum four iSCSI blades installed, 2048 initiators are supported. A number of iSCSI initiator implementations are supported, including ones for Microsoft® Windows®, Linux, and IBM AIX operating systems.

The iSCSI blade supports connection redirects to load balance across GbE ports and assist in path failover.

> **Note:** The Gigabit Ethernet ports on the iSCSI blade do not support FCIP. Also, the FC ports cannot be configured as FC routing (EX_port) ports.

iSCSI features

The iSCSI blade provides the following gateway services to the iSCSI initiators:

- Access to the fabric using FC devices (iSCSI virtual initiator)
- Support for target registration to an iSCSI Name Server (iSNS) for discovery
- Management of iSCSI initiator access control using discovery domains (DDs) and discovery domain sets (DD sets)
- Session management, such as session tracking and performance monitoring
- Session authentication using Challenge Handshake Authentication Protocol (CHAP)

Licensing and management

The iSCSI blade is managed using the director's management interfaces with both CLI and GUI management possible using Data Center Fabric Manager (DCFM). No separate license is needed for using the iSCSI service. The service runs after it is enabled through the management interface.

3.3 Capabilities and limitations

This section examines the specific limitations of the different configurations and functions of IBM System Storage b-type multiprotocol products. The limitations are based on the capabilities of the current hardware and operating system version, and are subject to change. Always check the current values in the interoperability matrix for your SAN router product. You can find the matrix on the IBM support web site:

http://www.ibm.com/servers/storage/support/san/

This section also lists configurations that, although can be configured, are not supported at the time of writing.

3.3.1 FC-FC routing and FCIP distance extension

When connecting edge fabrics and backbone fabrics, remember the basic connectivity rules:

- Backbone fabrics use only EX_Ports and VEX_Ports to connect to only E_Ports and VE_Ports, respectively, on edge fabrics.
- For two edge fabrics to share devices, they must be connected to the same backbone fabric, meaning no daisy chaining of edge and backbone fabrics.

Figure 3-15 and Figure 3-16 show configurations that are not allowed.

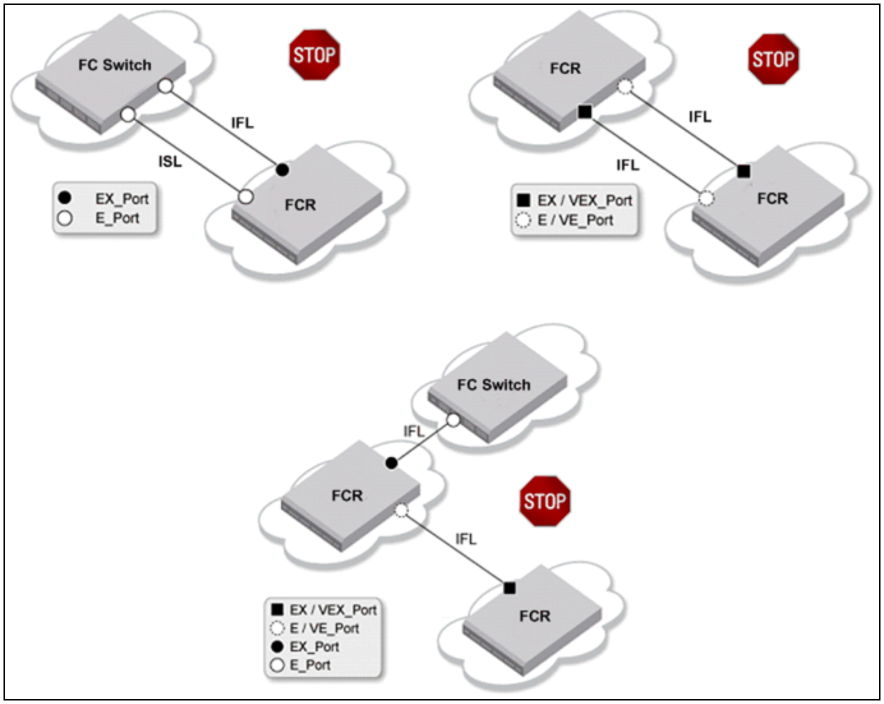


Figure 3-15 Unsupported port configurations

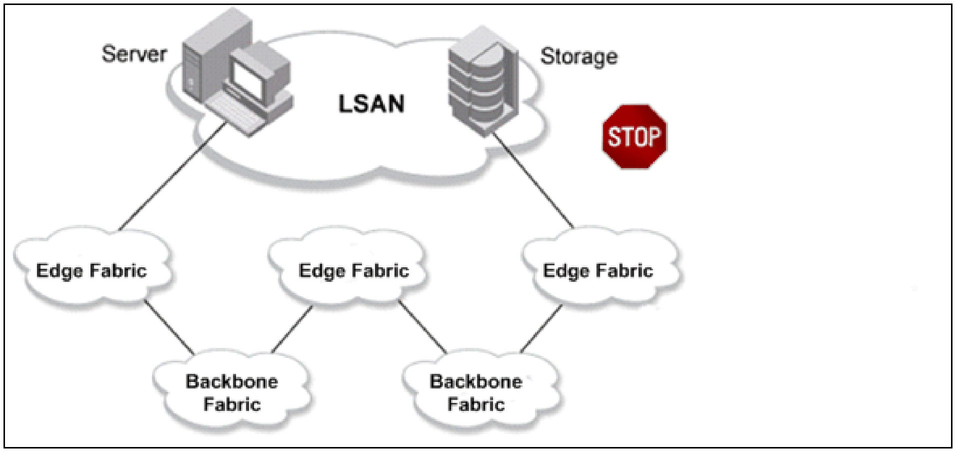


Figure 3-16 No daisy chaining

Figure 3-17 shows an example of a metaSAN where servers access storage at a different site. The servers connect to the backbone through IFL connections, therefore fabrics are not merged. The disk array also connects to the backbone through IFL connections, but in this case the storage is connected through an IP network. Figure 3-17 shows the types of ports involved in a metaSAN.

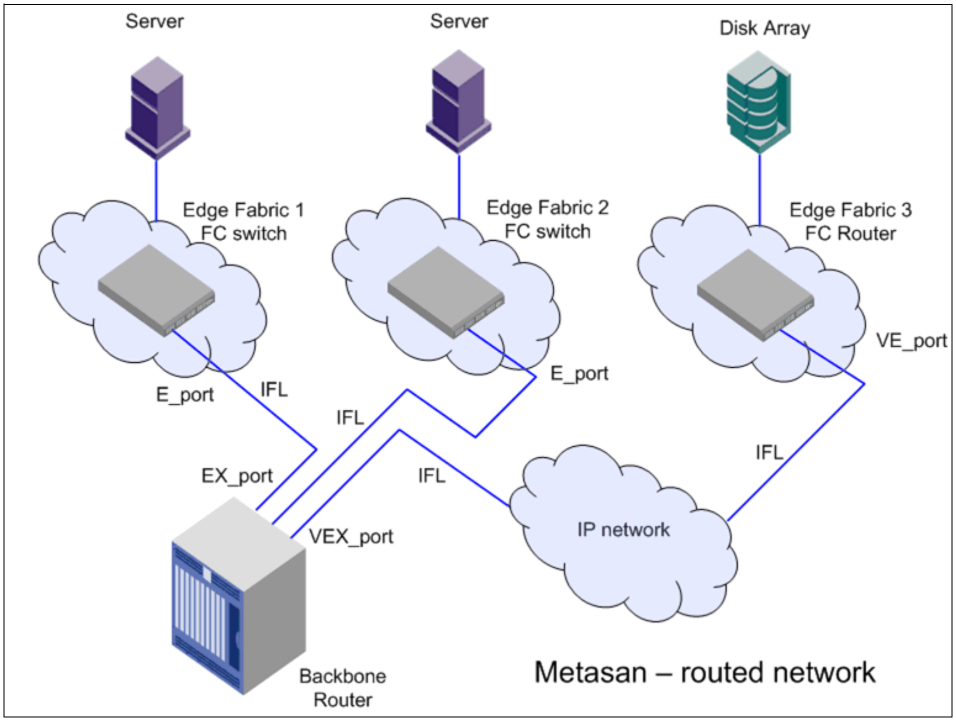


Figure 3-17 MetaSAN: Routed storage network

Interoperability

An interoperability matrix is the best source for compatibility and interoperability information for a particular SAN switch or multiprotocol router. Always obtain updated information for all products included in the solution that you plan to implement prior to implementation.

For the most up-to-date information, see the IBM support web site:

`http://www.ibm.com/servers/storage/support/san/`

If you cannot find the required information, ask your IBM representative to help you obtain the information.

Note: At the IBM support web site, each product has a published *interoperability matrix* that indicates the IBM tested-firmware levels at the time the document was published. Although you might find that on the download link later versions are available for download, these levels are fully tested and supported by IBM also.

3.3.2 iSCSI

Note: The iSCSI blade is not supported in the SAN768B and SAN384B.

Before implementing the iSCSI blade for the SAN256B director, take note of the following capabilities and limitations:

- All eight GbE ports on an iSCSI blade can be configured as iSCSI portals.
- All online GbE ports participate in an iSCSI portal group whose name is the slot number of the blade.
- There are 64 iSCSI initiators per iSCSI blade (2048 with four blades installed).
- The iSCSI blade performs iSCSI-FC gateway services at GbE wire speed.
- Regular Ethernet switches are to be used with the iSCSI blade. They must support Gigabit Ethernet connections to the iSCSI blade.
- The list of supported iSCSI initiators changes often, as ongoing testing completes. For the most current information, go to the IBM support web site:
  `http://www.ibm.com/servers/storage/support/san/`

  At the time of writing, supported initiators are available on the following platforms:

  - Microsoft Windows
  - IBM AIX
  - Red Hat Enterprise Linux
  - SUSE Linux
  - Sun Solaris
  - HP-UX
  - VMware
  - VMware ESX
- The iSCSI blade supports jumbo frames on the GbE ports.
- The iSCSI blade cannot tag Ethernet frames for Virtual LAN (VLAN) use.
- The iSCSI blade does not support IPSec.

- The iSCSI gateway supports only iSCSI Qualified Names (IQNs) and not EUI/NAA names provided by the IEEE registration authority.
- The iSCSI virtual initiator (the iSCSI blade) and the Fibre Channel targets must be part of the same Fibre Channel fabric in the metaSAN. iSCSI virtual initiators cannot be imported/exported across IFLs to other fabrics in the metaSAN.

Note: The minimum supported Fabric OS version on an SAN256B with iSCSI blade installed is v5.3.0.

3.4 Product applications

In this section, we present suggested applications for the IBM System Storage b-type family multiprotocol products. Applications listed should not be considered an exhaustive list, and that other applications exist. The section is meant to showcase possibilities for using the products. Although only one application is shown for each scenario, combinations are possible if device capabilities allow.

3.4.1 SAN04B-R and SAN18B-R

The SAN04B-R (2005-R04) and SAN18B-R (2005-R18) allow for a number of applications, including both FC-FC routing and distance extension using FCIP.

FC fabrics connected through FC-FC routing

FC-FC routers allow interconnection of existing or newly designed and implemented FC fabrics. Acting as a top-level device, it allows fabrics to communicate without merging them. Using the SAN18B-R to perform this fabric interconnection enhances scalability significantly and eliminates having to modify existing fabrics to enable them to communicate.

This approach is particularly useful for older fabrics, which might have constraints because a specific Fabric OS level is required. Through a SAN04B-R or SAN18B-R, these fabrics are able to communicate with other fabrics. Besides being useful for interconnecting older fabrics, these SAN routers can also be highly useful when upgrading an existing SAN infrastructure, allowing SAN designers to start over and use another design type for the expansion (for instance, a core/edge fabric design). This step is possible while maintaining full connectivity to the existing SAN infrastructure through the SAN04B-R or SAN18B-R.

Figure 3-18 shows an example with FC fabrics connected through the SAN04B-R.

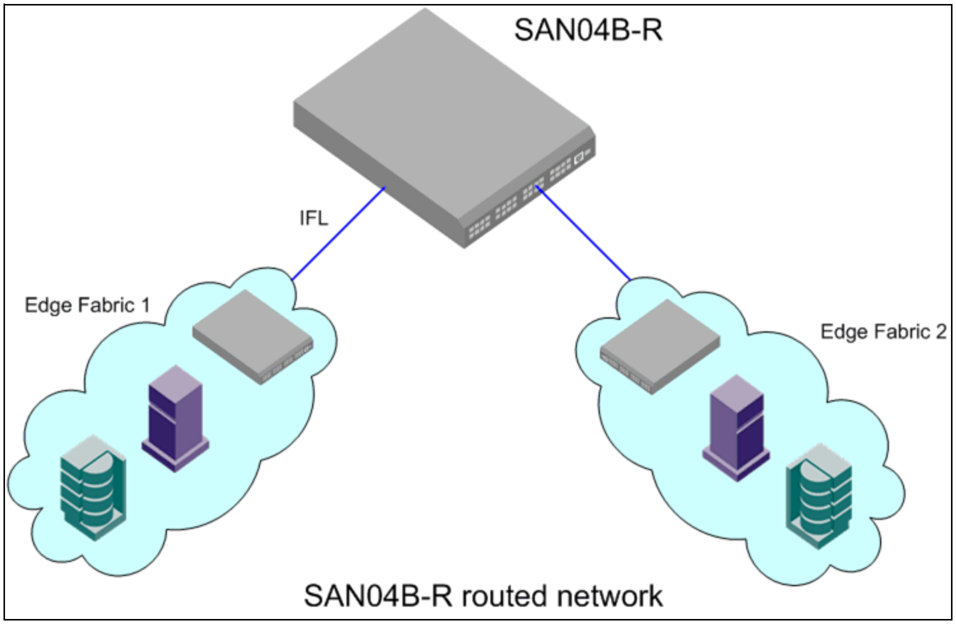


Figure 3-18 FC fabrics interconnected through SAN04B-R

Note: The same process can be accomplished without a dedicated SAN router using any of the newer SAN40B, SAN80B switches or using the 8 Gbps FC port blades in a SAN768B or SAN384B, as these FC ports can be configured as EX_Ports when an Integrated Routing license is present. An 8 Gbps blade in a SAN256B cannot be configured for Integrated Routing.

FC fabrics connected using FCIP distance extension

With Gigabit Ethernet ports and FCIP capabilities, the SAN04B-R and SAN18B-R can be used to interconnect existing FC fabrics using existing IP infrastructure. This approach is especially useful in scenarios with data replication between data centers, where the increased signal delay and lower link reliability common to IP networks is acceptable.

As with FC-FC routing, the number of fabrics that can be connected to a SAN18B-R is limited by the FC port count (16). Using FCIP, this limitation requires more consideration because only two GbE ports are available to pass all sixteen FCIP tunnels to another SAN18B-R GbE port at the other end (unlike

FC-FC, where the IFL link has full non-blocked bandwidth). Further consideration must be given when using the SAN04B-R, as only a single FCIP tunnel can be created per GbE port, and each is limited to 50 Mbps of bandwidth.

Important: The SAN04B-R is licensed for FC ports 0 and 1, a single IP tunnel per GbE port limited to 50 Mbps on that tunnel.

Figure 3-19 shows two fabrics merged into a single fabric using FCIP tunnels.

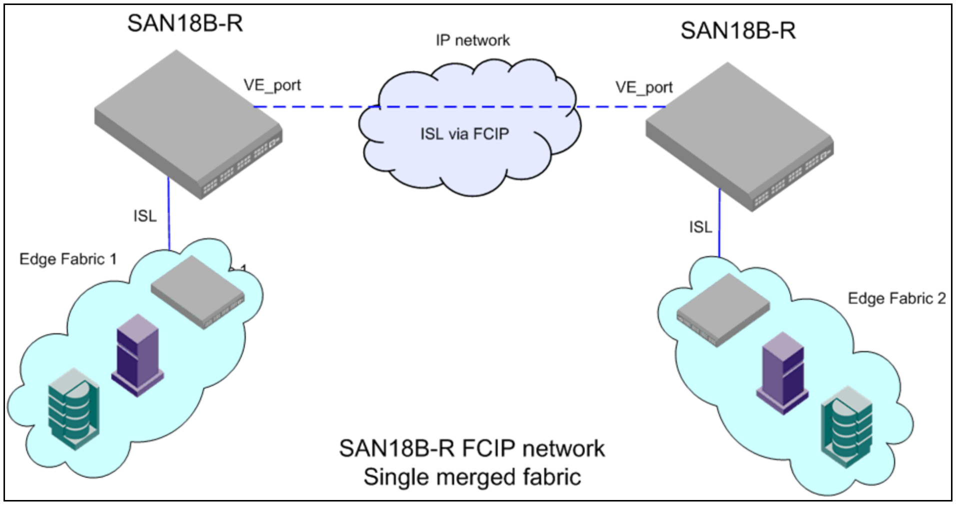


Figure 3-19 Fabric interconnected using FCIP

SAN18B-Rs connected using FCIP distance extension

In situations where no existing FC fabrics are found and the required port count is low, two SAN18B-Rs can be used both for connecting devices and for performing the FCIP distance extension.

By configuring a VEX_Port on one of the SAN18B-Rs, the other one will become an edge fabric, thus allow fabric separation. This separation avoids interrupting local traffic if, for instance, the IP link becomes unstable.

Figure 3-20 shows two SAN18B-Rs connected using an FCIP tunnel to form an IFL link. Fabrics are unmerged.

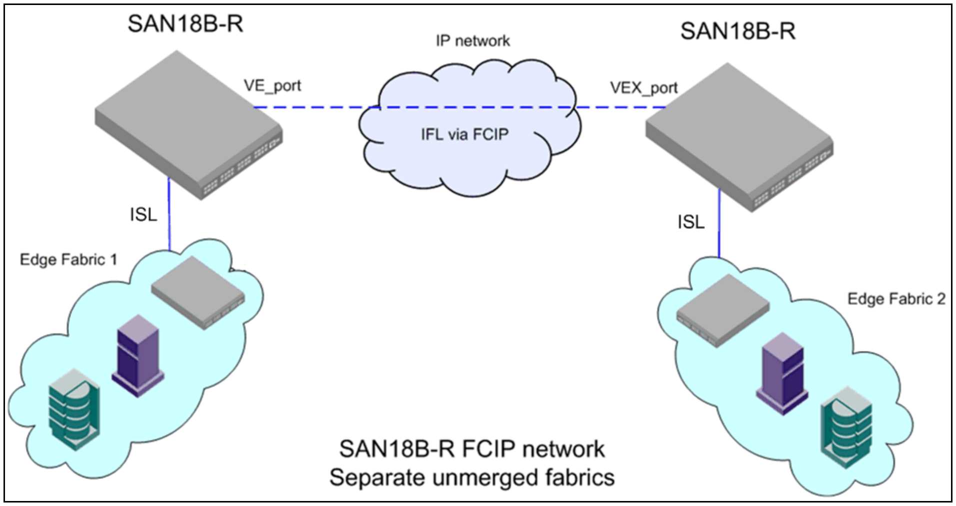


Figure 3-20 FCIP tunnel

3.4.2 FC Routing Blade for SAN768B, SAN384B, or SAN256B

Using the SAN768B (2499-384), SAN384B (2499-192), or SAN256B (2109-M48) directors with one or more FC Routing Blades installed enables the same set of possibilities as with the SAN18B-R. Because these products are director class with a high degree of redundancy and reliability, these features step up a level when compared to the SAN18B-R and SAN04B-R. (This should not be considered a substitute for dual fabrics.)

One of the scenarios where the SAN768B, SAN384B or SAN256B with FC Routing Blades really excel is in the ability to create backbone fabrics while preserving all multiprotocol router ports for edge fabric connectivity. This is possible because all regular FC ports in the director chassis belong to the backbone fabric and can be used for ISLs between switches within the backbone.

Using this capability allows for large metaSAN configurations while preserving design simplicity. These configurations can be made highly redundant and high performing using standard design rules for working with these directors (such as ISLs on more than one blade and trunking for ISL/IFL links). With more than one multiprotocol router blade installed in the director chassis, redundancy towards edge fabrics is possible by configuring IFLs on more than one FC Routing Blade.

Figure 3-21 shows a metaSAN configuration with a dedicated backbone fabric using both SAN768B and SAN256B directors with multiprotocol router blades installed.

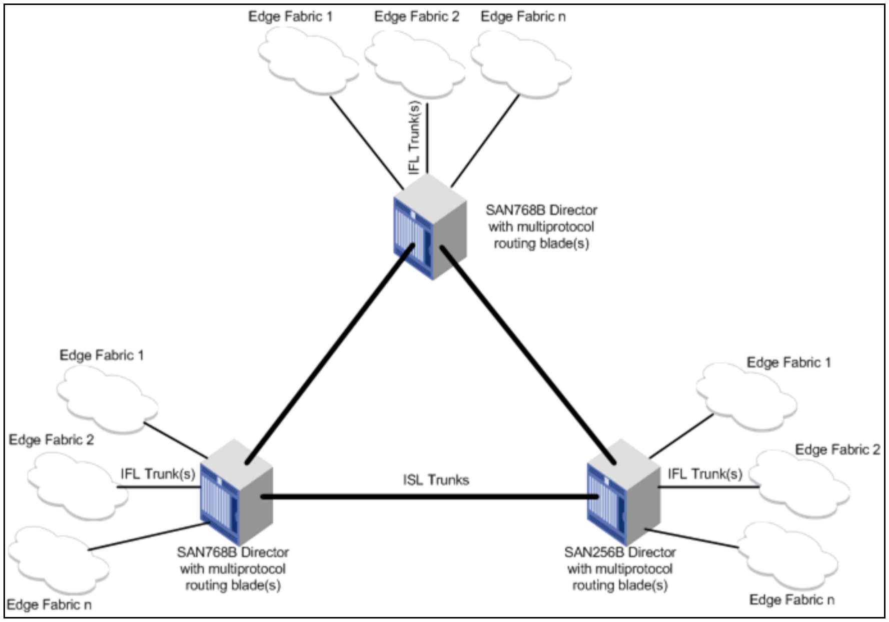


Figure 3-21 MetaSAN with dedicated backbone fabric

3.4.3 iSCSI blade for the SAN256B

With the iSCSI blade, servers are able to access a Fibre Channel storage infrastructure by using the iSCSI gateway service. Although attaching servers directly to the iSCSI blade using a cross-over twisted pair cable is possible, there is normally one or more Ethernet switches in between.

Figure 3-22 shows a basic iSCSI scenario with an iSCSI host connected using an Ethernet switch, and storage connected to the SAN256B (2109-M48) with the iSCSI blade installed.

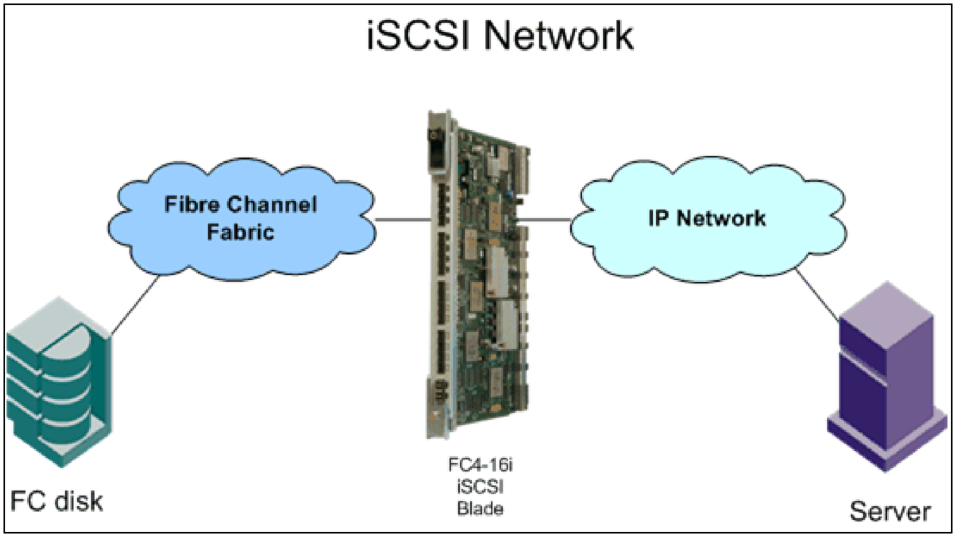


Figure 3-22 Simple iSCSI scenario

Most real-world scenarios are more complex than the one shown in Figure 3-22. The storage might not be attached to the SAN256B with the iSCSI blade and the iSCSI host might not be connected using only a single Ethernet switch. Storage can be attached on other switches as long as it resides in the same FC fabric as the iSCSI blade, effectively meaning that there are no IFLs in between.

The connection of the iSCSI hosts can benefit from the flexibility imposed by IP being a routed protocol supported on a variety of data networking technologies. This means that Ethernet can be combined with other data networking technologies to form the data link layer path between the iSCSI host and the iSCSI gateway service residing on the iSCSI blade. It also means that iSCSI hosts are not required to be on the same IP network as the iSCSI gateway service. If there is an IP route in between, iSCSI connectivity is possible.

Note: Although the network design flexibility imposed by IP is high, keep in mind that storage traffic has more stringent requirements than other IP traffic. Therefore, be careful to ensure adequate bandwidth and low round-trip time (RTT) along the path between iSCSI host and iSCSI blade. Also observe possible maximum transmission unit (MTU) and firewall issues along the IP path.

Figure 3-23 shows an extended iSCSI scenario.

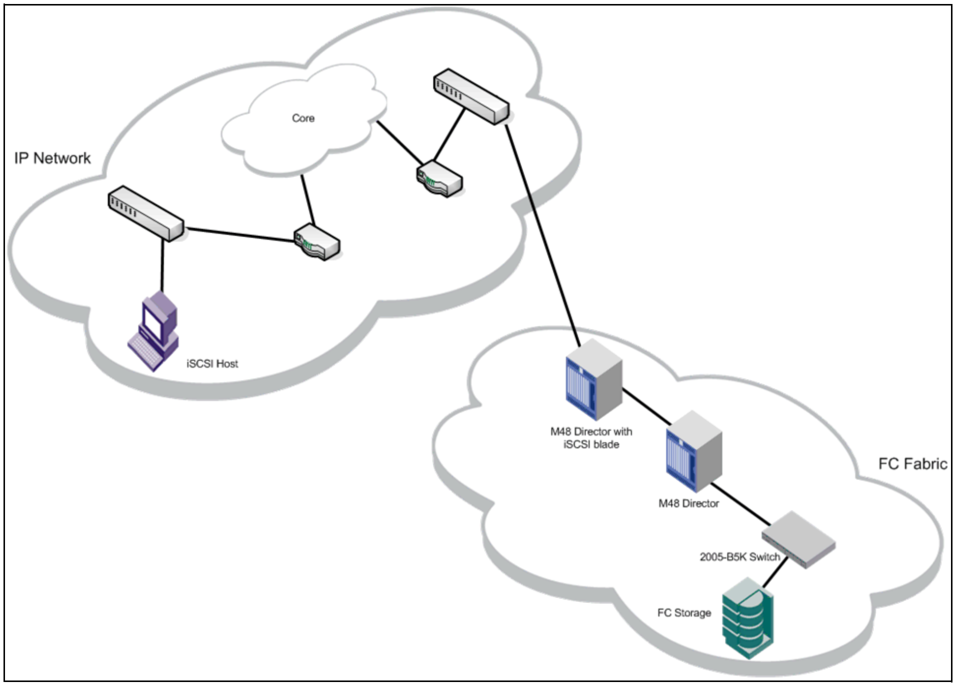


Figure 3-23 Extended iSCSI scenario

4

b-type family routing solutions

This chapter describes the solutions that are available when using the IBM System Storage SAN multiprotocol routers and blade products available from IBM/Brocade.

4.1 FC-FC routing

This section describes the FC-FC routing functionality and possible scenarios where the functionality can be used. FC-FC routing is available on IBM System Storage SAN40B, IBM System Storage SAN80B, and IBM System Storage SAN768B with the Integrated Routing license installed. The IBM System Storage SAN04B-R, IBM System Storage SAN18B-R, and the FC Routing Blade for the IBM System Storage SAN256B, IBM System Storage SAN768B or IBM System Storage SAN384B do not require any additional licenses for this feature.

4.1.1 Local FC-FC routing

The use of FC-FC routing in a local SAN environment gives you a lot of freedom in the connectivity of your environment, but be careful in how you use it. Routing can help with the following situations:

- Scaling of large SANs, giving:
  - More manageability
  - More independent functionality
  - Reduced complexity
- Isolation of SAN fabric services to each independent fabric island can:
  - Separate business units out to their own SAN fabrics.
  - Prevent corporate-wide outages because of changes in one of the fabrics.
  - Lower impact of hardware and micro-code upgrades.
- Sharing devices between functional groups allows:
  - Backup device sharing
  - Storage migration projects
  - Expanding storage needs can be quickly met

Figure 4-1 shows the local FC-FC routing solution between three SAN islands, consisting of redundant fabrics in each.

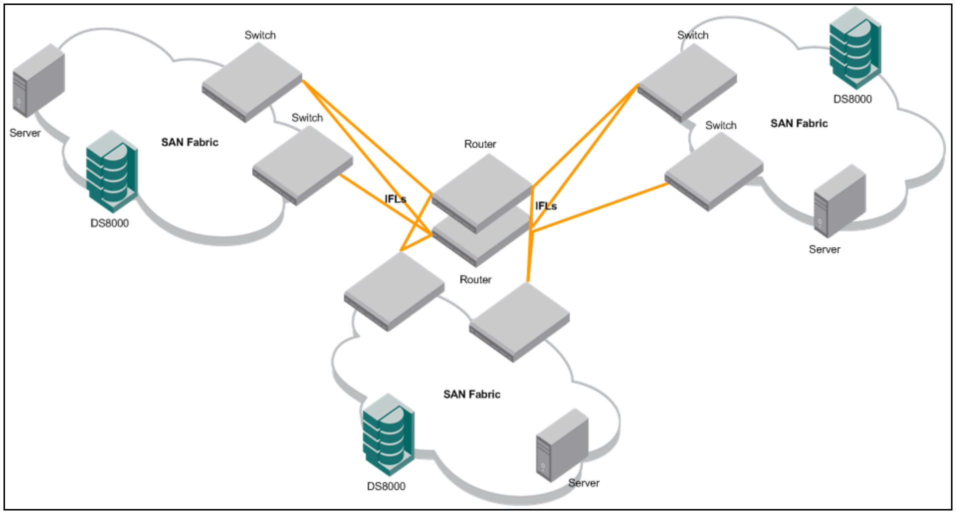


Figure 4-1 Local FC-FC solution

This example has two redundant SAN routers connected to three SAN fabrics. Both routers are connected to all fabrics using two inter-fabric links (IFLs) for redundancy. We can extend this configuration to span up to eight SAN fabrics, or up to 16 fabrics by adding two more routers.

Each edge fabric can be connected to the routers with up to eight IFLs with 4 Gbps products and later and can be trunked. If you have multiple switches in your fabric, we recommend that you distribute the IFL connections across them for maximum availability. If you are using a core-edge fabric design, a best practice is to connect IFLs to the core switches.

Several specific SAN issues can be addressed by local FC-FC routing:

- Scalability

  The Fibre Channel addressing can theoretically support up to 16 million nodes in a single fabric. However, the practical limit for the number of nodes is lower. This is similar to TCP/IP networks, where the network address space is divided into smaller subnets of limited numbers of IP addresses, and traffic is routed between them. Usually, the practical limit of a fabric from both technical and management standpoints is somewhere between 250 and 1,000 nodes.

FC-FC routing enables you to divide large environments into several smaller, more manageable fabrics, while providing access to shared resources between them.

- Multiple SAN administrators

  In many cases, enterprises have several small SAN islands that are managed by different SAN administrators. This might be because of department funding or might be a result of mergers or acquisitions. In any case, using FC-FC routing between the fabrics allows each independent fabric to be managed separately from the others. It also prevents the propagation of different management styles or networking errors being propagated to the other fabrics.

  The logical storage area network (LSAN) configuration of the routers is the only part of the fabric that needs to be coordinated among the SAN administrators. Because the LSAN zones must be defined on all fabrics before they can route traffic, the devices in each fabric are protected against unplanned access from the other fabrics.

- Interoperability between storage vendors

  Several storage vendors offer Brocade SAN products, either as resellers or as OEM products. Although these products are theoretically compatible with each other, each vendor usually only supports specific levels of Fabric OS, and finding a common supported version among multiple storage vendors can be difficult. The fabric-wide parameters and recommended zoning methodologies can also differ among vendors.

  If the different vendors are each separated into their own SAN fabrics, as could be the case in Figure 4-1 on page 73, we can avoid these problems. This solution also allows each edge fabric to be supported and even managed by the corresponding storage vendor, while enabling storage access between different SAN fabrics.

- Interoperability between old and new fabrics

  In many cases, when implementing a new SAN fabric, you already have an existing fabric. The existing fabric can have parameter settings that you want or need to set up differently in the new fabric. One good example is the core PID setting.

  By using FC-FC routing to connect the fabrics, you do not have to change the settings in the old fabric; instead you can choose the settings that you need for the new fabric. You can also use a Fabric OS level in one fabric that differs from the level in another, as long as it is of a level to support FC-FC routing functions. This approach allows older Fabric OS levels that are compatible with some earlier hardware to be used.

- Migration between old and new fabrics

  The storage hardware is usually replaced with new hardware every 3–5 years. When refreshing the disk hardware, a sensible approach might be to refresh the SAN hardware also, especially if the new disk vendor is different from the old vendor.

  FC-FC routing can enable you to implement the new disk subsystems and SAN fabric in the final configuration and connect the complete new environment to the current SAN fabrics. This way, you can have simultaneous access from the servers to both old and new disk subsystems and use server-based tools, such as Logical Volume Manager (LVM), to migrate the data from the old disks to the new disks.

  After you migrate any host to new disks on the new subsystems, you can move the Fibre Channel ports of the server to the new SAN fabric as well. Because you can do this one server at a time, this minimizes downtime and outages needed.

- Secure resource sharing

  In most enterprises, backup processes are conducted to tape. Many of these environments have additional cost to build multiple tape environments to support their needs. With FC-FC routing these needs can be met by sharing the tape devices across the separate fabrics, decreasing the cost of additional hardware. Though it would be possible to share tape and disks on single HBA in a host server, this practice is discouraged because of the different I/O patterns of the two devices. Some HBA vendors even provide specific configuration enhancement settings for tape implementations. Use of FC-FC routing does not mitigate the following of SAN best practices where different device types or data patterns are concerned.

  Another example of storage consolidation is implementing a single IBM System Storage SAN Volume Controller (SVC) cluster across multiple SAN fabrics.

- Metro mirroring with local campus sites

  In some cases, customers might want to mirror their data between storage servers that are fairly local and within acceptable distance limitations (10 Km without extension devices). In these cases, configuring the mirroring application across the FC-FC routing can allow for the mirroring to take place without giving up the security of the independent fabrics. This capability is commonly used with large mail servers and for critical data archiving solutions (tier 2) in high uptime environments.

4.1.2 Fabric extension with FC-FC routing

Figure 4-2 shows a simple SAN fabric extension using the SAN routers.

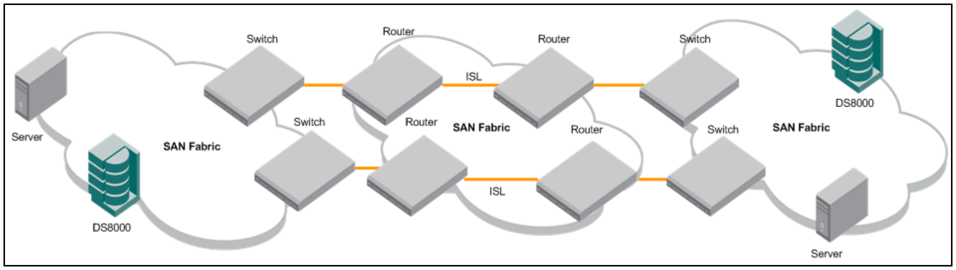


Figure 4-2 Fabric extension with FC-FC routing

This solution takes advantage of the large number of buffer credits available on each port in the router and the Extended Fabrics feature. The long-distance inter-switch links (ISLs) can be implemented with dark fiber, or with dense wavelength division multiplexing (DWDM) technology. Consideration must be given to the distance covered to prevent latency issues impacting application performance.

This design has the advantage that the edge fabrics are separated from each other and from the long-distance ISLs. This isolates any SAN fabric failure in one site to that location only and prevents others from being affected. This is especially important in a disaster recovery environment where the desire is to prevent any outage from affecting the production environment as much as possible. Any link failures on the long-distance links can also be isolated from both edge fabrics.

4.2 QOS, DSCP, and VLANs

Even if Quality of Service (QoS), DSCP and VLANs are not stricticly speaking solutions, we include some information in here, because they can have an impact on how you deploy your solution.

QoS refers to policies for handling differences in data traffic. These policies are based on data characteristics and delivery requirements. For example, ordinary data traffic is tolerant of delays and dropped packets, but voice and video data are not. QoS policies provide a framework for accommodating these differences in data as it passes through a network.

QoS for Fibre Channel traffic is provided through internal QoS priorities. Those priorities can be mapped to TCP/IP network priorities. There are two options for TCP/IP network-based QoS:

- Layer 3 DiffServ code Points (DSCP)
- VLAN tagging and Layer two class of service (L2CoS)

DSCP quality of service

Layer 3 class of service DiffServ Code Points (DSCP) refers to a specific implementation for establishing QoS policies as defined by RFC2475. DSCP uses six bits of the Type of Service (TOS) field in the IP header to establish up to 64 different values to associate with data traffic priority.

DSCP settings are useful only if IP routers are configured to enforce QoS policies uniformly within the network. IP routers use the DSCP value as an index into a Per Hop Behavior (PHB) table. Control connections and data connections might be configured with different DSCP values. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with the WAN administrator to determine the appropriate DSCP values.

VLANs and Layer 2 quality of service

Devices in physical LANs are constrained by LAN boundaries. They are usually in close proximity to each other, and share the same broadcast and multicast domains. Physical LANs often contain devices and applications that have no logical relationship. Also, when logically related devices and applications reside in separate LAN domains, they must be routed from one domain to the other.

A VLAN is a virtual LAN network. A VLAN might reside within a single physical network, or it might span several physical networks. Related devices and applications that are separated by physical LAN boundaries can reside in the same VLAN. Also, a large physical network can be broken down into smaller VLANs. VLAN traffic is routed using 802.1Q-compliant tags within an Ethernet frame. The tag includes a unique VLAN ID, and Class of Service (CoS) priority bits. The CoS priority scheme (also called Layer two Class of Service or L2CoS), uses three Class of Service (CoS or 802.1P) priority bits, allowing eight priorities. Consult with your WAN administrator to determine usage.

When both DSCP and L2CoS are used if an FCIP tunnel or circuit is VLAN tagged, both DSCP and L2CoS are relevant, unless the VLAN is end-to-end, with no intermediate hops in the IP network. This might be helpful when consulting with the network administrator. These values might be modified per FCIP tunnel.

DSCP and VLAN support on FCIP circuits

When a VLAN tag is created on an FCIP circuit, all traffic over that circuit will use the specified VLAN. The options are available on both the **`portcfg fciptunnel`** command to enable VLAN support on circuit 0, and on the **`portcfg fcipcircuit`** command for additional circuits.

> **Note:** For more details on how to get these features configured, refer to the Administration Guide for your switch.

4.3 FCIP tunneling

In situations where dark fiber or DWDM is not available, or the distances are greater than those supported by DWDM, the SAN fabrics can be connected using the FCIP tunneling functionality. The most common use of this method is to create long-distance remote mirroring and Business Continuity/Disaster Recovery (BCDR) sites. This capability frequently is used with Metro Mirror (MM), Global Mirror (GM), and global copy (GC) facilities and applications.

The practice of running shared devices across the tunneled path environment is discouraged because most applications cannot tolerate the latency, which frequently exceeds their expected response times. These site locations can be fairly close (across town) and implement a MM solution, or across the nation and implement a GM or GC build for BCDR environments.

This method is used frequently where distances exceed 100 Km. Figure 4-3 shows a basic configuration of this solution.

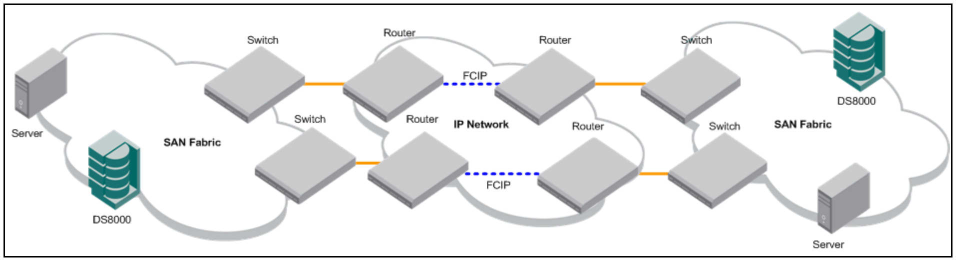


Figure 4-3 FCIP tunneling

To help in decreasing effects of lower stability of the environment on the production fabrics, combine FCIP tunneling with the FC-FC routing feature. This way, you can isolate any SAN fabric failure in one site to that site only, and prevent the other site from being affected. Also, link failures can be restricted to the FCIP links and isolated from all edge fabrics.

4.3.1 FCIP support for IPSec

The Internet Protocol Security (IPSec) uses cryptografic security to ensure private, secure communications over IP networks. The IPSec protocol is used to secure the FCIP tunnel over a public IP WAN by using encryption.

With the latest release of firmware, all the b-type products will be able to handle IPSec. This was already possible with release 6.3.1 with the IBM System Storage SAN06B-R, and now it is also supported in the FC routing blade, and there is no need for an external IPSec appliance.

IPSec feature attributes

The FC routing switches will use the following IPSec attributes:

- The SAN06B-R and the FC routing blade will use the internal FPGA for hardware encryption operations
- IPSec is configured using a pre-configured policy:
  - Internet Key Exchange (IKE) v2 for key negotiation
  - Encapsulating Security Payload (ESP) transport mode for IPSec (only the payload is encrypted)
  - Advanced Encryption Standard (AES) with 256 bit keys of encryption

    AES-CGM-ESP is the mode AES uses
  - Security Asociation (SA) lifetime is approximately 2GB of data sent through the SA
- IPSec will only support IPv4 for Fabric OS release 6.4.0, and IPv6 is not supported at this time

4.4 iSCSI gateway

The iSCSI gateway capability is available only on the IBM System Storage SAN256B with an iSCSI Blade (FC 3460). The IBM System Storage SAN04B-R, IBM System Storage SAN18B-R, and the FC Routing Blade for the IBM System Storage SAN768B/SAN384B (FC 3850) or the IBM System Storage SAN256B (FC 3450) do not support iSCSI.

The iSCSI Blade feature of the IBM System Storage SAN256B enables you to connect host servers with no Fibre Channel adapters to Fibre Channel-attached storage devices through the host’s TCP/IP adapters using the host’s iSCSI initiator driver to provide an iSCSI protocol connection.

Figure 4-4 shows an example of this solution.

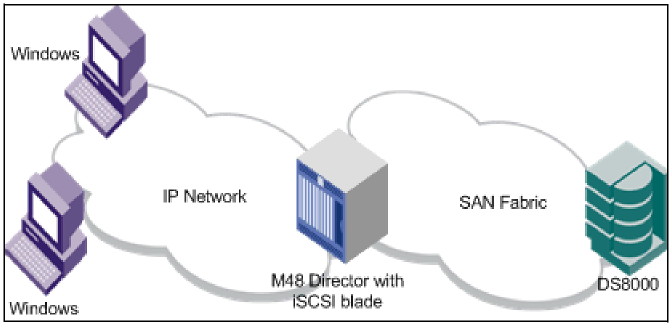


Figure 4-4 iSCSI gateway

Each IBM System Storage SAN256B iSCSI blade port supports up to eight concurrent iSCSI sessions. A total of eight ports are available on the blade.

Note: The iSCSI Virtual Initiator and the Fibre Channel target must be part of the same Fibre Channel fabric. iSCSI Virtual Initiators cannot be used in conjunction with FC-FC routing to export to or from another edge fabric.

5

b-type family multiprotocol routing best practices

This chapter discusses several best practices related to the IBM System Storage b-Type family storage area network (SAN) multiprotocol routing solution. Specifically, this chapter examines:

- Planning considerations
- MetaSAN design
- Availability
- Security
- Performance
- IP network issues

Note: The information in this chapter is based on Fabric OS v6.4.1.

5.1 Planning considerations

This section addresses topics to consider when planning solutions with IBM System Storage b-type SAN multiprotocol router products.

5.1.1 Piloting new technology

Whenever you plan to implement advanced features, such as Fibre Channel (FC) over IP (FCIP) or Fibre Channel to Fibre Channel (FC-FC) routing, implement them initially as a pilot with the understanding that experience gained in your own environment will almost always be unique.

When implementing leading-edge technologies, many clients prefer to avoid the uncertain outcomes that a pilot implies. Instead, they secure implementation guarantees from network service providers. But in fact, the outcome can never be guaranteed, and piloting allows the solution to be tailored, based on lessons learned in your own environment.

5.1.2 FC-FC routing considerations

Because logical storage area networks (LSANs) are created as with any other zones, except for the name, defining all zones as LSAN zones is possible. However, if you do this, each Fibre Channel router (FCR) in the metaSAN will have to keep track of all your zones, limiting the scalability of the metaSAN. Although selective LSAN propagation is possible on a fabric ID (FID) basis, we do not suggest creating all zones as LSANs.

Create zones that enable traffic within a single edge fabric as normal zones. LSANs should only be created when devices must communicate across fabric borders. Also, create single initiator, single storage device LSAN zones across different fabrics in the metaSAN. This approach can help with troubleshooting and minimize unnecessary access between devices. To benefit from hardware-enforced access control (where each FC frame is checked), use worldwide name (WWN) zoning for the zones that enable local traffic. To limit the number of domain IDs in the edge fabrics and ease the coordination effort for the FCRs, use front domain consolidation on IFLs.

If you use FC-FC routing in an environment with servers running an operating system that requires persistent FC IDs (such as AIX 5L without dynamic path tracking, or HP-UX), define the translate domain IDs and virtual slot numbers manually. This approach can help ensure that FC IDs of any devices used by the these servers remain persistent.

5.1.3 FCIP tunneling considerations

When implementing an FCIP connection, the quality of the IP link is critical. When you order the IP link from a vendor, you must have a service level agreement (SLA) that concerns the operation of the link. Ensure that the network service provider accounts for the specific requirements of the storage environment in the provider's design. The SLA should include at least the following parameters:

- Guaranteed link bandwidth (bitrate)
- Round-trip latency
- Maximum packet loss rate
- Whether packet delivery can be out-of-order

You must have an IP address and a subnet mask for both ends of the connection. Usually, these are provided by the vendor to suit the vendor's addressing scheme.

If you have a direct connection with no IP routers in between, the IP addresses should be in the same subnet, and the subnet mask should be the same for both ends. Also, you do not have to specify any default gateway information for the link. Figure 5-1 shows an example of a direct FCIP connection.

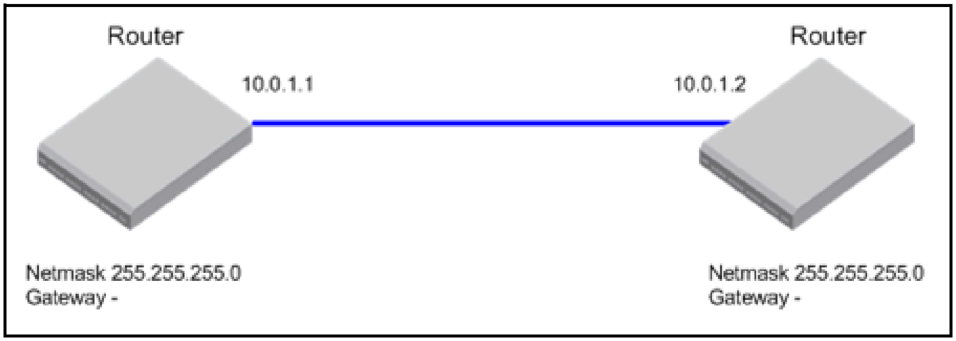


Figure 5-1 Direct FCIP connection

If you use an IP-routed connection, the IP addresses should be in different subnets, and you must specify the correct default gateway address for both routers. The default gateway address is the address of an IP router in the same local IP network as the SAN multiprotocol router.

In the scenario shown in Figure 5-2 where we have the FCIP tunnel over the WAN, as part of day-to-day SAN administration tasks the SAN router configuration will be documented and readily to the SAN support team.

It is important to document all the basic details such as port number, name, location of the WAN network device end to which the multi protocol router is connected, and so on, so that in case of reporting any issue to the network service provider, specific details are available that can help to have quicker resolution of issues.

Figure 5-2 shows an example of a routed FCIP connection.

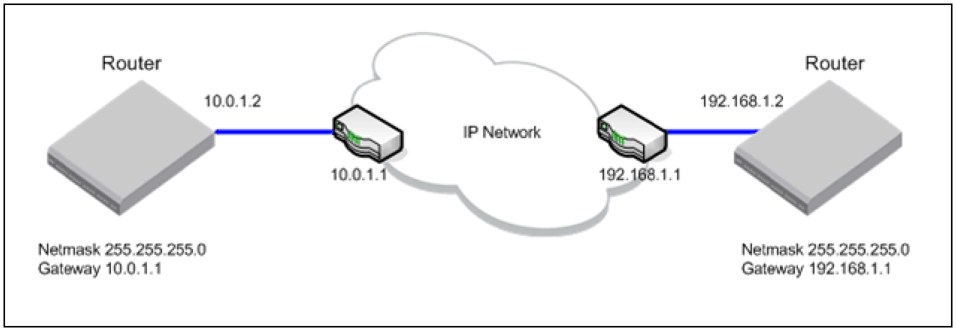


Figure 5-2 Routed FCIP connection

5.1.4 Support services

A best practice is to have the following support services available on the management LAN:

- A reliable Network Time Protocol (NTP) server, to synchronize the internal clocks of the SAN multiprotocol routers with a reliable time source
- A Simple Network Management Protocol (SNMP) trap destination for event monitoring

Another best practice is to have the following support services for larger environments:

- A syslog daemon, for storing log files from the SAN multiprotocol routers
- A remote authentication dial-in user service (RADIUS), for credential validation with a central directory

The capabilities of IBM System Storage Data Center Fabric Manager (DCFM) should also be evaluated for environments with more than a few FCRs.

5.2 MetaSAN design

When planning for a metaSAN, constraints are always imposed by FC SANs that already exist. Only when you are designing and implementing an entirely new metaSAN (with only new fabrics), can you have the freedom to decide on all parameters of the design.

In general, consider the following guidelines. They are, to a large extent, generic to SAN design as a discipline, and can facilitate system flexibility, scalability, and troubleshooting. As the metaSAN increases, the importance of these guidelines increases:

- Create a scheme for parameters such as edge and backbone fabric IDs (FIDs). If manual control is used with domain IDs, front domains, and translate domains, these should be included in the scheme. Always document which values are in use and to what they are assigned. Even if certain values are automatically assigned, this should be documented in the scheme.
- Naming conventions should be used and documented. This includes device names, zoning (both zones and configs), ports, and aliases.
- Exploit the traffic locality principle when port bandwidth is oversubscribed, and plan for connecting devices as close as possible regarding fabric. This approach helps limit ISL and IFL traffic, and can dramatically improve metaSAN performance and scalability.
- Core/edge fabric designs allow for the greatest flexibility and efficiency on a long-term basis.
- Always plan for growth, even though this is unpredictable. This could be to install an IBM System Storage SAN768B director with only a few FC port blades as the fabric core instead of an IBM System Storage SAN80B switch.
- Implement the greatest feasible degree of redundancy to minimize single points of failure. Find an appropriate compromise between cost and complexity. This could be installing two or more FCRs (or installing more than one FC Routing Blade in, for example, a IBM System Storage SAN768B) to ensure availability of the backbone fabric.
- For redundancy, always connect devices to dual FC fabrics.
- Remember to evaluate the IP network when using iSCSI to ensure appropriate performance and reliability.
- Remember that simplicity is the ultimate sophistication.

5.3 Availability

The IBM System Storage SAN04B-R and IBM System Storage SAN18B-R have redundant, hot-swappable power supplies and fans. The FC Routing Blade for the IBM System Storage SAN256B, IBM System Storage SAN768B or IBM System Storage SAN384B and the 8 Gbps Port Blades on the IBM System Storage SAN768B or IBM System Storage SAN384B with Integrated Routing benefit from the redundancy provided by the director chassis, which includes redundant hot-swappable control processors, core switching blades, power supplies, and fans. Although hot-code loading and hot-code activation are available for FC ports on the IBM System Storage SAN04B-R, IBM System Storage SAN18B-R, and the FC Routing Blade options, traffic on the Gigabit Ethernet (GbE) ports is disrupted if the Ethernet controller must be updated. The IBM System Storage SAN40B-R with Integrated Routing has redundant, hot-swappable power supplies and fans. The IBM System Storage SAN80B-R with Integrated Routing has two hot-swappable power supplies and three hot-swappable fans.

For the iSCSI gateway function, the iSCSI blade should be configured to support an iSCSI connection redirects to allow failover between iSCSI portals. However, not all iSCSI clients support such a configuration.

5.4 Security

The SAN multiprotocol routers can be used in various roles. The following sections describe security in each role.

5.4.1 FC-FC routing security

FC-FC routing security is based on the LSAN concept. Each LSAN is a zone in each edge fabric that the LSAN spans, and that contains multiple port worldwide names. It is implemented by defining the zone in each of the edge fabrics involved. The LSAN zones are separated from normal zones by having their name start with “LSAN_”. Note the underscore character after the letters LSAN. The letters in this context are not case-sensitive. When the zones are defined, the SAN multiprotocol router automatically exports any shared devices across the fabrics. LSAN zones can be compared to hardware-enforced inter-fabric access control lists.

Note: An LSAN zone can only contain members from edge fabrics, and none from the backbone fabric. Therefore, the nodes in the backbone fabric are inherently secure from any nodes in edge fabrics

Because the LSAN zone must be separately defined in both edge fabrics, a zoning change in one edge fabric cannot enable unauthorized access to a device in another edge fabric. This approach is especially important in cases where the edge fabrics are managed by different SAN administrators.

5.4.2 FCIP tunneling security

The IBM System Storage SAN04B-R, IBM System Storage SAN18B-R, and the FC Routing Blade for the IBM System Storage SAN384B, IBM System Storage SAN768B and IBM System Storage SAN256B are configured to initiate FCIP tunnels when they detect the presence of a device with matching configuration. The FCIP tunnels use the well-known Transmission Control Protocol (TCP) port 3225 for switch-to-switch management traffic, and TCP port 3226 for the actual data traffic. If not configured, TCP port 3227 is used for the wide area network (WAN) analysis tool, ipPerf.

If you have one or more firewalls in the IP path, you have to allow this traffic in the firewalls. Allow the **ping** command to be used between the devices to make problem determination easier.

Enhance security by configuring each end of the FCIP tunnel with the WWN of the SAN multiprotocol router in the remote end. This approach prevents any other router from connecting to the port.

You might also configure IP security (IPSec) across the FCIP tunnels to increase security.

5.4.3 iSCSI gateway security

When opening the iSCSI session, the iSCSI initiator connects to the iSCSI gateway service using well-known TCP port 3260. If you have a firewall between the iSCSI initiator and the iSCSI blade, you must allow this traffic in the firewall.

The iSCSI gateway function supports the optional use of Challenge Handshake Authentication Protocol (CHAP) in either one-way or two-way configurations.

In a one-way CHAP configuration, the iSCSI initiator is authenticated by the iSCSI gateway. The iSCSI initiator can open an iSCSI session only if the CHAP secret of the initiator matches the CHAP secret configured on the iSCSI gateway. This way, the iSCSI connection is protected against any other iSCSI initiator trying to use the same iSCSI Qualified Name (IQN).

In a two-way CHAP configuration, the iSCSI initiator is first authenticated by the iSCSI gateway, and the iSCSI gateway is then authenticated with the iSCSI initiator. The iSCSI initiator can open an iSCSI session only if the CHAP secret of the initiator matches the CHAP secret configured for the initiator in the iSCSI gateway, and the CHAP secret of the iSCSI gateway matches the CHAP secret configured for the iSCSI gateway in the iSCSI initiator. This way, the iSCSI initiator is also protected against any other device imitating the routers iSCSI portal.

Always use at least one-way CHAP configuration.

5.5 Performance

This section briefly discusses the performance of the products in this book when used in different solutions. Detailed performance guidelines and advice is beyond the scope of this book. Performance should be evaluated on a per-system basis, taking specific system characteristics into account.

Note: FC and FCIP Fast Write performance are not included in this book.

5.5.1 FC-FC routing performance

The IBM System Storage SAN04B-R, IBM System Storage SAN18B-R, and the FC Routing Blade for the IBM System Storage SAN384B, IBM System Storage SAN768B and IBM System Storage SAN256B are capable of routing traffic at full speed of 4 Gbps on all FC ports. Therefore, in an FC-FC routing scenario, the performance of an inter-fabric link (IFL) is practically the same as the performance of a 4 Gbps inter-switch link (ISL).

Implementing FC-FC routing on the IBM System Storage SAN40B, IBM System Storage SAN80B, or the 8 Gbps Port Blades in a IBM System Storage SAN384B or IBM System Storage SAN768B with an Integrated Routing license applied allows full 8 Gbps speeds to be achieved. With ISL/IFL trunking and dynamic load sharing (DLS), overall performance can be increased even further.

Important: IFL/EX_Port trunking should only be enabled if the entire configuration is running Fabric OS v5.2.0 or later.

In high-performance environments where latency budgets are calculated, the values of the switching/routing-imposed delays might be required. For details about this information, consult the data sheets, or contact IBM for assistance while doing the calculations. Per device, the values can be considered to be in the low µs area (at a worst-case).

5.5.2 FCIP tunneling performance

FCIP performance is a complex issue because it is affected by many separate factors, such as performance of the FCIP links and latency caused by the FCIP encapsulation itself.

An FCIP link has significantly lower performance and higher latency than the same link would have if it was a native Fibre Channel link. Therefore, use FCIP tunneling only when a native Fibre Channel link cannot be implemented for technical or financial reasons.

The SAN multiprotocol routers implement a traffic-shaping feature that enables you to limit the amount of bandwidth used for the FCIP link. This way, you can avoid overloading a WAN link slower than the GbE interfaces, and thus limit the effects of the TCP slow start mechanism. If possible, Ethernet jumbo frames should be used across the data path to prevent fragmentation of every FC frame (note that this requires that the entire path supports this).

Note: On the IBM System Storage SAN04B-R, each GbE interface is already rate-limited to 50 Mbps and supports only a single FCIP tunnel.

For more information about FCIP link performance, refer to 5.6, “IP network issues” on page 90.

5.5.3 iSCSI performance

iSCSI gateway functionality allows small servers, which do not have high performance or availability requirements for their storage connection, access to an FC SAN infrastructure.

Although sharing the same network interface on a server between normal TCP/IP traffic and iSCSI traffic is possible, a best practice is to implement a separate IP/Ethernet network for the iSCSI traffic. The iSCSI network should have low latency, less than 15 ms, and minimal packet loss. Because of the network latency requirements, we do not suggest using iSCSI over long-distance connections.

The iSCSI blade performs the iSCSI gateway functionality at wire-speed (1 Gbps per port), which can be affected by the IP network performance, and also by the capabilities of the iSCSI initiator and the attached Fibre Channel storage. In addition, the end nodes must be wire-speed capable.

5.6 IP network issues

This section discusses the following factors that affect the performance of an FCIP link:

- Link bandwidth
- Link latency
- TCP receive window
- Packet loss rate
- Out-of-order packet delivery

Ask your network service provider about quality of service (QoS) managed links, including information about such offerings as IP over SONET/SDH. Work with your telecommunications company so that it understands your network quality expectations, and you understand the cost and management implications of any decisions that you make.

5.6.1 Link bandwidth

The link bandwidth (bitrate) is the most obvious factor affecting performance. It is also one of the key metrics used when provisioning the link. For synchronous storage applications, the solution for provisioning is when the link bandwidth corresponds to the guaranteed bandwidth from the network service provider.

If the link bandwidth is anything less than full Gigabit Ethernet, it must be configured into the routers in both ends of the link, to use the traffic-shaping features and avoid overrunning the link. Set the maximum allowed speed of the FCIP tunnel to 95–96% of the bandwidth of the link on both ends of the link.

5.6.2 Link latency

Link latency is a metric of the round-trip time (RTT) for a packet to cross the link. The key factors contributing to the link latency are as follows:

- Distance
- Router and firewall latencies
- Time of frame in transit

Distance

The speed of light in optical fiber is approximately 208,000 km per second. Therefore, the delay caused by a fiber connection is approximately 4.8 µs/km. To calculate the round-trip latency, count this delay in both directions. For example, for a 100 km link, the round trip latency is as follows:

```
100 km x 4.8 µs/km x 2 = 960 µs
```

Similarly, for a 1000 km link, the round trip latency is 9600 µs, or 9.6 ms.

Router and firewall latencies

Any delay caused by IP routers and firewalls along the network connection must be added to the total latency. The latency varies depending on the routers or firewalls used and the traffic load. It can range from a few microseconds to several milliseconds.

You also must remember that the traffic generally passes the same routers both ways. For round-trip latency, you must count the one-way latency twice.

If you are purchasing the routers or firewalls yourself, include the latency of any particular product among the criteria that you use to choose the products. If you are provisioning the link from a network service provider, include at least the maximum total round-trip latency of the link in the SLA.

Time of frame in transit

The time of frame in transit is the actual time for a given frame to pass through the slowest point of the link. Therefore, it depends on both the frame size and link speed.

The maximum payload size in a Fibre Channel frame is 2112 bytes. The Fibre Channel headers add 36 bytes to this, for a total Fibre Channel frame size of 2148 bytes. When transferring data, Fibre Channel frames at or near the full size are usually used.

> **Note:** The standard ethernet frame is a maximum of 1518 bytes. Contrast that with the maximum FC frame size of 2148 bytes. As you can see, if we were to wrap the frames into an Ethernet frame then some form of fragmentation, or segmentation, would have to occur because of the difference in maximum sizes (1518 versus 2148). Although this is possible, it is not desirable because it would add more processing overhead to the operation. After all, the aim is to enhance performance and not add any performance degradation.

If we assume that we are using jumbo frame support in the Ethernet network, the complete Fibre Channel frame can be sent within one Ethernet packet. The TCP and IP headers and the Ethernet medium access control (MAC) add a minimum of 54 bytes to the size of the frame, for a total Ethernet packet size of 2202 bytes, or 17616 bits.

For smaller frames, such as the Fibre Channel acknowledgement frames, the time in transit is much shorter. The minimum possible Fibre Channel frame is one with no payload. With FCIP encapsulation, the minimum size of a packet with only the headers is 90 bytes, or 720 bits.

Table 5-1 details the transmission times of this FCIP packet over common WAN link speeds.

Table 5-1 FCIP packet transmission times over different WAN links

Link type	Link speed	Large packet	Small packet
Gigabit Ethernet	1250 Mbps	14 µs	0.6 µs
OC-12	622.08 Mbps	28 µs	1.2 µs
OC-3	155.52 Mbps	113 µs	4.7 µs
T3	44.736 Mbps	394 µs	16.5 µs
E1	2.048 Mbps	8600 µs	359 µs
T1	1.544 Mbps	11 400 µs	477 µs

If we cannot use jumbo frames, each large Fibre Channel frame must be divided into two Ethernet packets (fragmented), which doubles the amount of TCP, IP, and Ethernet MAC overhead for the data transfer.

Normally, each Fibre Channel operation transfers data in only one direction. The frames going in the other direction are close to the minimum size.

5.6.3 TCP receive window

In addition to the bandwidth available, the maximum throughput available on any given TCP connection is determined by the TCP receive window of the receiving device. This is similar to the buffer-to-buffer credit flow control used in Fibre Channel networks. To enable the full use of a given FCIP link, the size of TCP window allocated for the link must be large enough for all FCIP packets that are being transferred on the line.

5.6.4 Packet loss rate

In traditional TCP/IP networks, packet loss is a normal and accepted behavior. The built-in retransmission mechanism in the protocols handle retransmitting any dropped packet. Most protocols used in TCP/IP networks can easily handle high packet loss rates, such as 1%, without significant performance degradation.

Because FCIP uses a TCP connection for data transfer, it also uses the same mechanism. However, because latency is usually critical in storage applications, the storage networks do not cope well with retransmissions. Therefore, networks used for storage traffic require a much lower packet loss rate. Even an IP network with a packet loss rate of 0.01% is considered a low-quality network, compared to the baseline of zero frame loss in Fibre Channel networks.

5.6.5 Out-of-order packet delivery

Fibre Channel networks rely on in-order delivery of Fibre Channel frames. The SAN multiprotocol router receiving FCIP traffic must ensure that the Fibre Channel frame order is retained.

If IP packets are received out-of-order, as is often the case with shared IP networks using Multiprotocol Label Switching (MPLS), the SAN multiprotocol router must buffer them until it receives the complete sequence of packets.

Usually, the only effect of out-of-order packet delivery is slightly increased latency. However, in extreme cases, the receiving router can run out of buffer space and have to drop packets.

6

b-type family real-life routing solutions

This chapter presents real-life solutions implemented with the IBM System Storage b-type family routing products. We discuss the following solutions:

- Backup consolidation
- Migration to a new storage environment
- Long-distance disaster recovery over IP
- LAN-based users needing additional storage

> **Important:** The solutions and sizing estimates that we discuss or create in this chapter are unique. Make no assumptions that they are supported on or apply to each environment. Consult IBM to discuss any proposal.

6.1 Backup consolidation

This scenario presents a solution to consolidate LAN-free tape backups from two separate storage area network (SAN) fabrics.

6.1.1 Client environment and requirements

The client has two existing SAN fabrics and is currently using ArcServe software to back up the Microsoft Windows servers in the separate SAN fabrics to their respective tapes. The client also has several application servers that do not have SAN attachment. Figure 6-1 shows the client's environment.

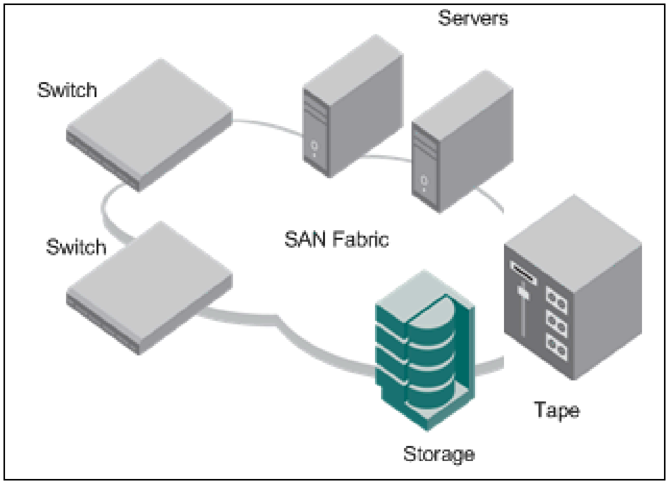


Figure 6-1 Current backup environment

The client has the following requirements for the new solution:

- Consolidate the tape backups to a single Tivoli Storage Manager (TSM) environment.
- Provide for LAN-free backups from both current SAN fabrics.
- Implement the new backup system to a separate location from the computer center about 2 km away.
- Take advantage of the existing investment in SAN hardware.

In the first SAN fabric, the client currently has 160 GB of disk space. This space is projected to grow to 630 GB in the near future. In the second SAN fabric, the client has 100 GB of disk space.

6.1.2 The solution

Our solution has the following new components:

- IBM System p® server for Tivoli Storage Manager
- IBM System Storage TS3310 library
- IBM System Storage SAN40B-4 switch for the backup environment
- IBM System Storage SAN04B-R multiprotocol route

Figure 6-2 shows the new backup environment to be developed.

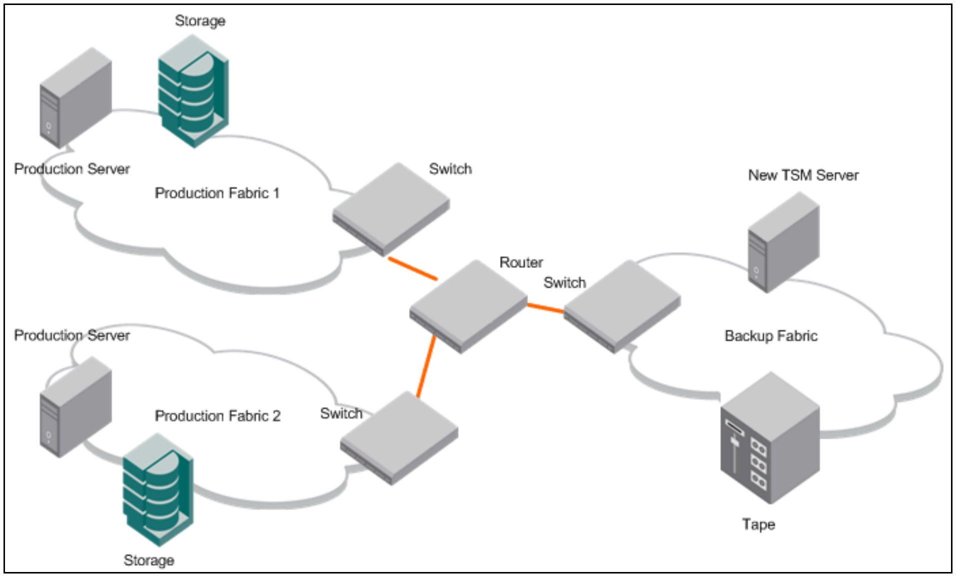


Figure 6-2 New backup environment

We locate the router in the computer center to minimize the number of fiber connections between the computer center and the backup site. All other components are located in a single rack at the backup site.

We connect each of the current fabrics, and the new backup switch, to the router with two inter-fabric links (IFLs) for redundancy. The client provides the two long-wave fiber connections required between the computer center and the backup site.

The Tivoli Storage Manager server will use its internal disks for both Tivoli Storage Manager databases and disk storage pools. Therefore, it does not need any access to the existing client SAN fabrics. The tape drives are divided evenly across the two Fibre Channel adapters in the Tivoli Storage Manager server.

We create a separate logical SAN (LSAN) zone for each server in any SAN fabric that needs access to the tape drives. The LSAN will contain the port worldwide name (pWWN) of the host bus adapter (HBA) of the server and the pWWNs of all the tape drives. We also ask the client to create the same LSANs in the existing SAN fabrics.

Because we use our new environment only for daily backups, it does not have the high availability requirements that SAN fabrics use for disk access. Therefore, having a single backup switch and a single router in the solution is adequate.

The application servers that are not connected to any SAN fabric are backed up to the Tivoli Storage Manager server over a LAN connection.

6.1.3 Failure scenarios

The failure of different components can affect the operation of our solution, as follows:

- Power failure

  The Tivoli Storage Manager server, the tape library, and all SAN fabric components in the environment have dual redundant power supplies connected to different power circuits. Therefore, a power failure in one circuit does not have any effect on operation.

- IFL failure

  If an IFL fails, the system remains operational, but the maximum bandwidth available is reduced by 50%.

- Router failure

  If the SAN router fails, running LAN-free backups is impossible. In this situation, the Tivoli Storage Manager client automatically uses a LAN-based method for any backup and restore activity. The Tivoli Storage Manager server and the servers that are not using LAN-free backups are not affected.

- Backup switch or Tivoli Storage Manager server failure

  The failure of either the backup switch or the Tivoli Storage Manager server prevents any backup and restore activity.

6.2 Migration to a new storage environment

This scenario presents a solution to migrate the client's current storage environment to a new environment.

> **Note:** The steps explained in this book are only basic steps. For a detailed guide for migration, refer to IBM Redbooks publication *Migrating to IBM System Storage DS8000*, SG24-7432.

6.2.1 Client environment and requirements

The client has a Hewlett-Packard (HP) XP512 storage system that is shared between AIX 5.3, HP-UX, and SUN servers. Because of historical reasons, each server platform has its own SAN fabrics and connections to the XP512.

Each SAN fabric consists of a single 16-port, 1 Gbps Brocade 2800 switch. Because the lease period of the environment expires within a few months, the client needs a new solution to replace the current environment. All of the SAN islands consist of two redundant SAN fabrics for high availability. Our process of migration is designed to maintain this redundancy of the environment throughout the work.

Figure 6-3 shows the initial environment. For clarity, we show only some of the servers attached.

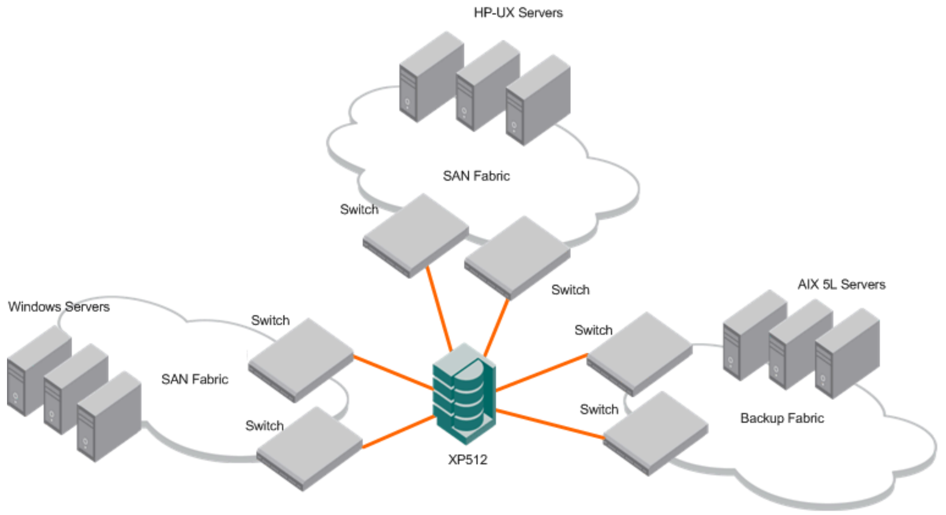


Figure 6-3 Initial storage environment

The client has the following requirements for the new solution:

- New hardware to replace the current disk system and SAN fabric
- Flexibility in allocating ports between different platforms
- Scalability to support future applications
- Minimize the amount of downtime of servers as a result of migration

6.2.2 The solution

Our solution has the following new components:

- IBM System Storage DS8100 disk subsystem
- Two IBM System Storage SAN768B Directors with at least 64 ports each
- Two IBM System Storage SAN04B-R multiprotocol routers

  Alternatively, you can add the SAN768B FCR Blade (FC#3850) or the Integrated Routing License feature to the directors. We chose the routers for flexibility of their future use after the migration is complete.
- Servers that are upgraded with 8 Gbps FC host bus adapters to provide the full value of the new SAN hardware that is being installed. (This is a best practice.)

We install the components of the new storage environment and connect the environment to the old environment FCR routes through IFLs, as shown in Figure 6-4.

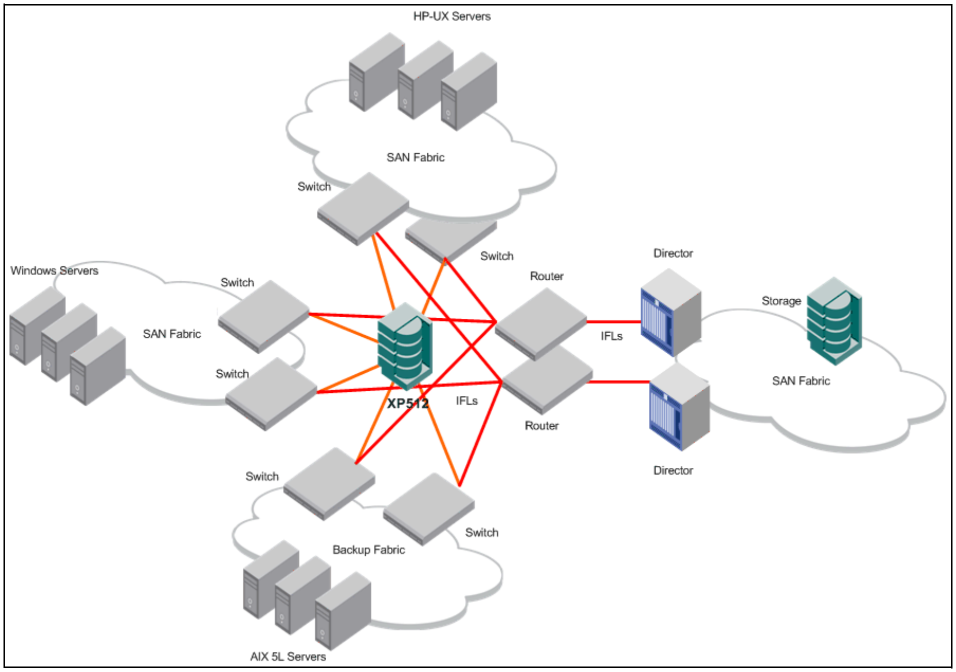


Figure 6-4 Interim environment for migration

In the new environment, all IBM System Storage DS8100 ports are shared among all servers. Because we are only migrating a few servers at the same time, using a limited number of IFLs does not cause any performance degradation to the servers.

When the new storage environment is installed, we start migrating the servers, one server or a small group of servers at a time, using the following procedure:

1. Create LSANs to allow the server to access the IBM System Storage DS8100.
2. Install the IBM Subsystem Device Driver (SDD) package on the server.
3. Allocate new storage in IBM System Storage DS8100 to the servers.
4. Migrate all server data in the old storage to the new storage using the following operating system-based software mirroring tools:
   - Native Logical Volume Manager (LVM) for AIX 5.3
   - LVM HP-UX
   - Veritas Volume Manager for SUN

5. Create non-LSAN zones to allow the server to access the storage from the new SAN fabrics.
6. Disconnect the server from the old switches.
7. Uninstall any remaining old software that is no longer needed (for example, multipathing drivers such as PVLinks or DMP).
8. Move server to the new directors.
9. Delete the LSANs created in step 1 on page 101.

If the customer also chose to upgrade the servers FC HBAs, the outage taken would be at flexible periods for all the servers because the cards could be replaced during whatever outage period was desired prior to the new SAN installation, and the migration process would be completely seamless to the user community.

After the migration of all servers is complete, mirroring can be broken and no servers would have to be connected to the old switches or the XP512 because they would be idling. At this time, we can remove the old storage and SAN fabric hardware from the environment, and if time allows or the slots are needed, remove the old FC HBAs. IBM System Storage SAN18B-R routers are also freed and can be used for another purpose.

Figure 6-5 shows the final storage environment.

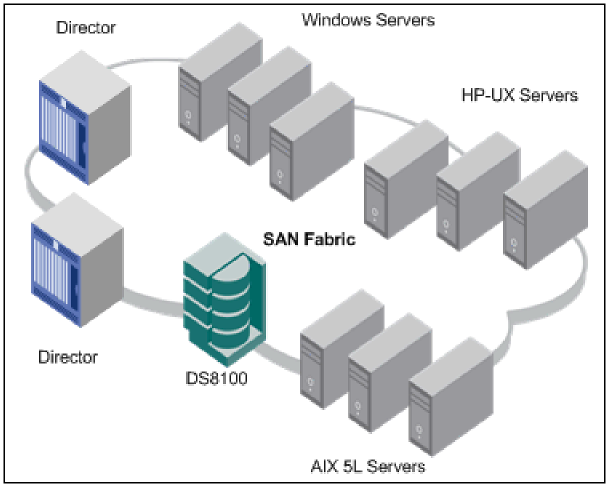


Figure 6-5 Final storage environment

6.3 Long-distance disaster recovery over IP

This scenario presents a solution that provides for long-distance disaster recovery (DR) over an IP connection.

6.3.1 Client environment and requirements

The client has three SAN islands that must be connected:

- Development SAN in the primary site
- Production SAN in the primary site
- DR SAN in the remote DR site

The distance between the primary site and the DR site is 600 km. The amount of data in the production environment is expected to grow to 5 TB within two years, and the customer believes that 3% of the data is changing in the peak hours of the day.

Note: A common approach is that a week’s worth of performance analysis be captured using IBM Tivoli Storage Productivity Center (TPC) during the highest workload period of a week/month, to gather the real level of work to be mirrored. Analysis of this data is available from IBM.

The client has the following requirements for the solution:

- Provide replication for production data from the primary site to the disaster recovery site, with a five minute recovery point objective (RPO) and a five-minute recovery time objective (RTO).
- Keep the dual fabrics of each SAN island both physically and logically separate.
- Provide access to a point-in-time copy of production data for the test environment at the development SAN.
- Provide for LAN-free backup from the development network to the tape library in the production network.

The current environment contains the following components:

- Production environment at the primary site
  - Dual SAN fabrics, based on IBM System Storage SAN256B Directors
  - IBM System Storage DS8100 disk subsystem, eight Fibre Channel ports
  - IBM System Storage 3584 tape library with six IBM 3592 tape drives
  - Eight IBM eServer™ System p servers with dual Fibre Channel adapters
  - Sixteen IBM eServer System x servers with dual Fibre Channel adapters

- Development environment at the primary site
  - Dual SAN fabrics, based on IBM System Storage SAN40B-4 switches
  - IBM System Storage DS6800 disk subsystem, four Fibre Channel ports
  - Eight IBM eServer System p servers with dual Fibre Channel adapters
  - Sixteen IBM eServer System x servers with dual Fibre Channel adapters
- Disaster recovery environment at the disaster recovery site
  - Dual SAN fabrics, based on IBM System Storage SAN256B Directors
  - IBM System Storage DS8100 disk subsystem, eight Fibre Channel ports
  - IBM System Storage 3584 tape library with six IBM 3592 tape drives
  - Eight IBM eServer System p servers with dual Fibre Channel adapters
  - Sixteen IBM eServer System x servers with dual Fibre Channel adapters

Figure 6-6 shows the environment. For clarity, we show only some of the servers and connections.

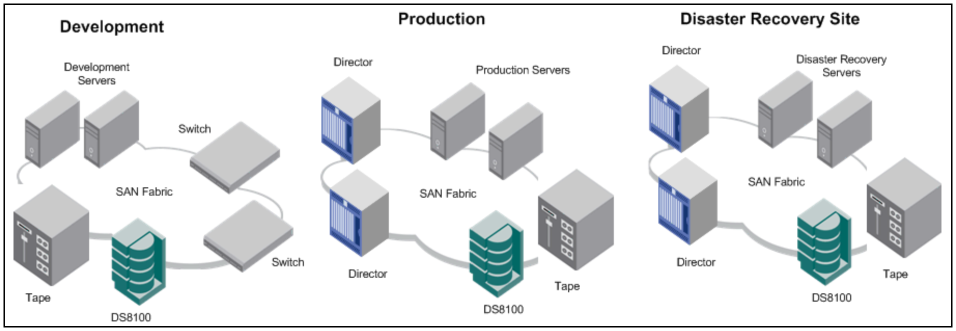


Figure 6-6 Client environment

6.3.2 The solution

Our solution has the following components:

- IBM System Storage DS8100 Global Mirroring feature for asynchronous replication
- Four IBM System Storage SAN256B Director FC Routing Blades (FC 3450), with FCIP tunneling feature activated
- Four IP links between IBM System Storage SAN256B Director FC Routing Blades from the primary site to the DR site
- IBM TotalStorage Rapid Data Recovery (eRCMF) software to provide automatic failover of both System p and System x servers

Figure 6-7 shows the complete solution.

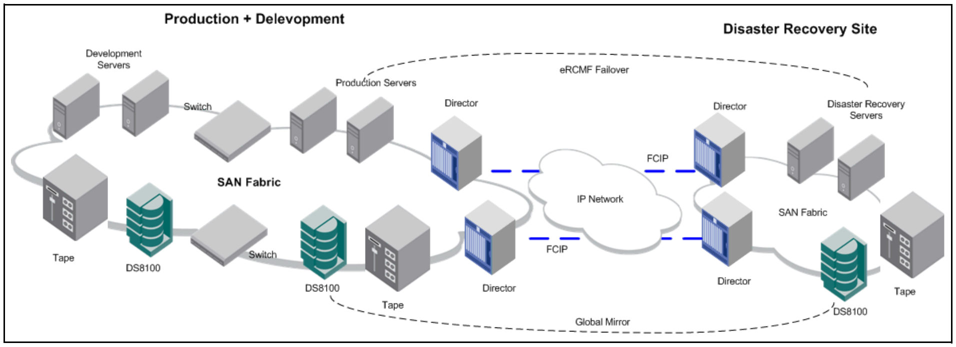


Figure 6-7 Disaster recovery solution

FCIP link sizing

Because we are using only the FCIP links for Global Mirror between the IBM System Storage DS8100 systems (the purple paths in the diagram), we take into account any changes to the data only when sizing the links. We strongly recommend pulling a TPC data capture for analysis and rechecking the expected requirements.

Based on the client's requirements, the amount of data-changing during the peak hour is 3% of 5 TB, or 150 GB. If we assume that this is a throughput-intense environment, and the changes are fairly large block sequential I/Os evenly spread across the hour, then the changes would be 2.5 GB per minute, or approximately 42 MBps, or 336 Mbps. We use this number as the basis for our link-sizing.

Note: A common approach is that a week's worth of performance analysis be run during the highest workload period, to gather the real level of work to be mirrored. The analysis of this data can be performed by IBM with recommended sizing being provided to meet the need.

If we divide this amount evenly across four links, we see traffic of 84 Mbps over each link. However, to allow the loss of one link or any unseen peaks in the traffic, we divide the traffic only across three links, for 33% extra bandwidth and 112 Mbps traffic over each link. We also plan to have a maximum of 90% use on the link, so the minimum link speed we need is 125 Mbps.

Each link can be implemented over an OC-3 line that has the capacity of 155 Mbps. An alternative is to use a shared connection based on Multiprotocol Label Switching (MPLS). However, because of possible router latency issues, we prefer the private OC-3-based connection.

The most significant part of the OC-3 link latency is the propagation time of the light within the fiber. For a 600 km connection, with 1200 km round trip, it is 1200 x 4.8 µs, or 5.8 ms.

We round this to 6 ms to account for the packet transmission time over the 155 Mbps OC-3 link. To ensure that this value is not greatly exceeded, the connection should be tested for actual value. A quick and common tool for this is to test the link with a **`ping`** command.

6.3.3 Normal operation

In normal operation, the production servers only use the IBM System Storage DS8100 disks at the primary site. The disaster recovery servers are connected to the IBM System Storage DS8100 in the disaster recovery site, but do not have the disk mounted or any applications running.

The development servers use IBM System Storage DS6800 disks in the primary site, and some capacity from the IBM System Storage DS8100 in the primary site.

From the IBM System Storage DS8100 disk subsystems, four of the eight ports are used for host attachments and the remaining four are used for Global Mirroring. The ports used for Global Mirroring are directly connected to the routers.

In addition to normal zoning, we define the following LSANs in our environment:

- Separate LSANs for the HBAs of any server in the development fabric that must have access to the IBM System Storage DS8100, containing:
  - The HBA of the server
  - Both Fibre Channel ports of IBM System Storage DS8100 used for host attachment in the fabric
- Separate LSANs for the HBAs of any server in the development fabric that must have access to LAN-free backup, containing:
  - The HBA of the server
  - All Fibre Channel ports of the tape drives in the primary site connected to the fabric

In addition, we define zones for each Global Mirror connection in the backbone fabric of the directors.

6.3.4 Failure scenarios

The failure of different components can affect the operation of our solution, as follows:

- Power failure

  All of the SAN fabric components in the environment have dual redundant power supplies connected to different power circuits. Therefore, a power failure in one circuit does not have any affect on operation.

- FCIP link failure

  The failure of a single FCIP link reduces the available bandwidth between the sites by 25%. However, because we assumed three available links in our sizing, the performance of the system will remain adequate.

- Development fabric switch failure

  The failure of a switch in development fabric reduces the Fibre Channel bandwidth available for development and test servers by 50%. The traffic is automatically routed through the remaining paths by the SDD. The production environment is not affected.

- Primary site router failure

  If one of the routers at the primary site fails, the capacity of the Global Mirror connection is reduced by 50%. Because we rounded up link speed, we still have about 300 Mbps or about 90% of the peak-hour capacity available. This reduces the Fibre Channel bandwidth available between development and test servers, and the storage in the production fabrics, by 50%.

- Primary site director failure

  Director failure at the primary site reduces the Fibre Channel bandwidth available for production servers by 50%. It also reduces the Fibre Channel bandwidth available between development and test servers, and the storage in the production fabrics by 50%.

- Disaster recovery site router failure

  If the router at the disaster recovery site fails, the capacity of the Global Mirror connection is reduced by 50%. However, because we rounded up our link speed, we still have about 300 Mbps, or about 90%, of the peak hour capacity available.

- Disaster recovery site director failure

  Director failure at the disaster recovery site reduces the Fibre Channel bandwidth available for disaster recovery servers by 50%. However, in normal situations, those servers are idling, so this reduction affects the system only in the case where the production workload is already running at the disaster recovery site.

- Primary site IBM System Storage DS8100 port failure

  If a port used for host access in the IBM System Storage DS8100 at the primary site fails, the Fibre Channel bandwidth available for host access is reduced by 25%.

  If a port that is used for Global Mirror in the System Storage DS8100 at the primary site fails, the remaining Fibre Channel ports can sustain the full Global Mirror performance.

- Primary site IBM System Storage DS8100 failure

  If the IBM System Storage DS8100 at the primary site fails, all hosts lose access to it. This event can be promoted to site failure, and production can resume at the disaster recovery site.

- Disaster recovery site IBM System Storage DS8100 port failure

  If a port used for host access in the IBM System Storage DS8100 at the disaster recovery site fails, the Fibre Channel bandwidth available for host access is reduced by 25%. However, in normal operation, those servers are idling, so this reduction affects the system only in the case where the production workload is already running at the disaster recovery site.

  If a port that is used for Global Mirror in the IBM System Storage DS8100 at the disaster recovery site fails, the remaining Fibre Channel ports can sustain the full Global Mirror performance.

- Disaster recovery site IBM System Storage DS8100 failure

  If the IBM System Storage DS8100 at the disaster recovery site fails, the Global Mirror connections change to a suspended state. The IBM System Storage DS8100 at the primary site will accumulate changes to the data, and copy the changed data over to the disaster recovery site when the IBM System Storage DS8100 becomes available.

- Primary site failure

  If the complete primary site fails, IBM eRCMF software starts the production at the disaster recovery site automatically. Although manual failover is also possible, manually reaching the RTO target is difficult.

6.4 LAN-based users needing additional storage

This scenario presents a solution that provides additional storage capacity to LAN-based servers that do not have fabric attachment available, and the added expense is too great for these low-profile uses.

6.4.1 Client environment and requirements

The client has a large SAN fabric with a large IBM System Storage DS8100 storage server providing primary storage for all of the business-critical applications. The IBM System Storage DS8100 is connected to two IBM System Storage SAN256B directors creating two independent SANs, with four ports on each of the directors. The primary host servers are SAN attached through two HBAs, one to each of the two IBM System Storage SAN256B directors.

Two small Windows 2003 servers are used for historical analysis projects and are in need of additional storage space for reference charts used for review and trend comparisons. This group is located a block away at a satellite office with all storage currently on the servers' internal drives, and no SAN hardware in place. The client has stated that SAN attachment is a too costly solution for this small department to bear. The client has also stressed that this is a low priority use, but would help with the client's future planning efforts. A dedicated LAN network is in place and that provides both email and web access to all users at both sites.

Servers that have to be connected are as follows:

- Production servers direct attached to SAN in the primary site
- Analysis servers at a satellite location that are in need of additional capacity

The client has the following requirements for the solution:

- Provide a means by which the remote department can be connected to the large storage server in the corporate SAN to enable the department to have access to the needed capacity, available there for the department's use.
- Use current network links already connecting the two locations to reduce cost.

6.4.2 The solution

Our solution has the following add-on components:

- Two IBM System Storage SAN256B Director iSCSI Blades (FC 3460) added to the current directors at the primary site.
- The required Windows iSCSI initiator driver to support the iSCSI gateway connection for the SAN-based storage to be accessible.
- Configuration of the initiator and gateway for failover paths through the two blades in the two directors.

Because this is a low priority requirement that has no critical impact to primary business continuance and that has a fairly low volume usage model, enabling these servers to have a gateway path to the additional storage is a low-cost solution that will meet this client's needs.

6.4.3 Normal operation

In normal operation, the production servers use only the IBM System Storage DS8100 disks in the primary site as they are currently. The analysis department will have access to additional storage capacity through iSCSI gateway links to the defined LUNs, which have been mapped to the specific host initiator that the analysis department is working on. These LUNs will appear to the user as normal drives for the user's allocation and use.

High I/O dependent applications should not be mapped to these devices because performance can become a factor. For this client's requirements, these devices will perform well and meet the client's needs for capacity growth.

6.4.4 Failure scenarios

The failure of different components can affect the operation of our solution, as follows:

- Power failure at the primary storage site

  All of the SAN fabric components in the environment have dual redundant power supplies connected to different power circuits. Therefore, a power failure in one circuit does not have any affect on operation.

- iSCSI or LAN link failure

  The failure of the LAN connection to the primary site location disrupts the iSCSI storage access completely. Because access to this data is of low priority, the client is willing to accept this as an acceptable risk.

- SAN director failure

  The IBM System Storage SAN256B is a high availability, enterprise class, redundant director. However, because we are designing for a blade to be installed in each of the two fabric directors, failover will be available in case of a fabric outage.

- iSCSI blade gateway failure

  If one of the iSCSI blades in a director at the primary site fails, the iSCSI initiator initiates a failover process to the secondary blade defined to the devices for pathing. The Global Mirror connection will be reduced by 50%. However, because we rounded up our link speed, we still have approximately 300 Mbps, or about 90% of the peak hour capacity available. In addition, it reduces the Fibre Channel bandwidth available between development and test servers, and the storage in the production fabrics, by 50%.

- Primary site IBM System Storage DS8100 port failure

  If a port used for host access in the IBM System Storage DS8100 at the primary site fails, the Fibre Channel bandwidth available for host access is reduced by 25%. This is no different than the original configuration limit.

- Primary site IBM System Storage DS8100 failure

  If the IBM System Storage DS8100 at the primary site fails, all hosts lose access to it. This includes the satellite users using the iSCSI devices for their storage.

Figure 6-8 shows the complete solution that we suggest.

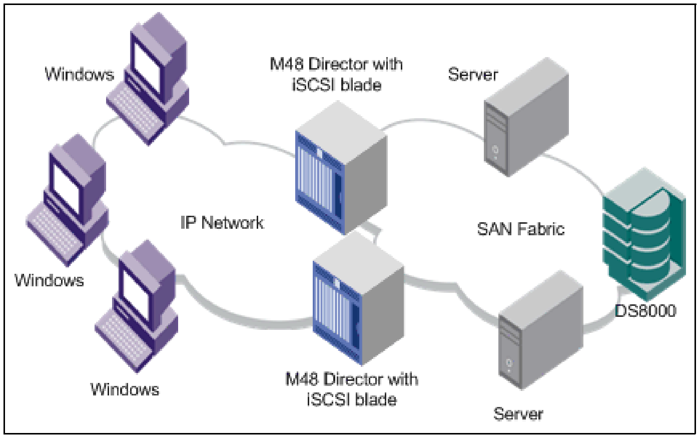


Figure 6-8 Completed solution

7

Multiprotocol routing basic implementation

In this chapter, we discuss the implementation of the IBM System Storage b-type family of storage area network (SAN) multiprotocol routing products. We perform the steps required to complete the initial product set up, and then introduce the various management tools, including Web Tools, Data Center Fabric Manager, and the command-line interface (CLI).

Although this chapter shows how to configure the IBM System Storage b-type multiprotocol routing products, it is not intended to provide an in-depth discussion of the management tools involved. For detailed information about the management tools, which are common to the entire b-type family, refer to IBM Redbooks publication *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

> **Note:** This chapter assumes that Fabric OS v6.4.1 is installed on the SAN multiprotocol routing products. For other software, the specific software versions are stated in the text.

7.1 Initial setup

In this section we show how to perform initial setup tasks using a SAN06B-R multiprotocol router. While we will be using a SAN06B-R, these steps are identical for SAN04B-R and SAN18B-R. The SAN06B-R,SAN04B-R and SAN18B-R multiprotocol routers are standalone products, in contrast to both the FC Routing Blade and the iSCSI blade, which must be installed in a SAN768B, SAN384B, or SAN256B director. Initial setup tasks are only shown for the SAN06B-R product, because installation and basic configuration (such as setting the IP addresses) of the SAN768B and SAN256B directors is beyond the scope of this book. For information about implementing these directors, refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

Physical installation for the SAN06B-R includes rack mounting the device, connecting appropriate power cables, and then powering it up. Regarding the FC Routing Blade and the iSCSI blade physical installation, this is performed by an IBM customer engineer (CE) by installing the blades in the director chassis and then powering them up one at a time.

Note: Physical installation and upgrades to the SAN768B and SAN256B directors should be performed by an IBM CE or by another arrangement agreed upon with IBM.

The power up sequence should take no more than five minutes to complete on any of the products. Self diagnostics are run and the LED lights on the products will flicker during this power on self test (POST). After the POST completes the port LED lights will flash slowly, indicating that the ports are in disabled state. If this change in LED status does not occur, wait one minute and then redo the power-up sequence.

Accessing the CLI through the serial management port

The SAN04B-R needs to have an IP address configured before access is possible through the Ethernet management port. This is done by accessing the CLI through the serial management port.

To connect to the serial port, perform the following steps:

1. To connect to the SAN06B-R/ SAN04B-R / SAN18B-R serial management port, use the provided console cable. It is a rolled RJ45 to DB9 cable. The standard b-type straight-through (non-null modem) serial cable physically will not work. Perform the following steps:

   a. Connect the RJ45 end to the console port on the router, which is the left-most RJ45 connector labeled 10101 in Figure 7-1.

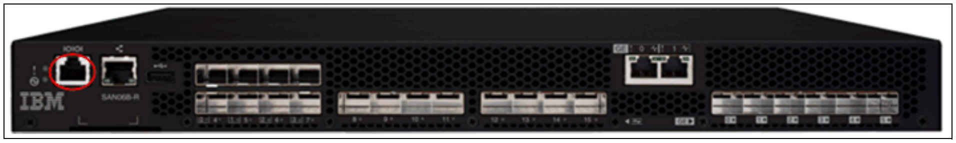
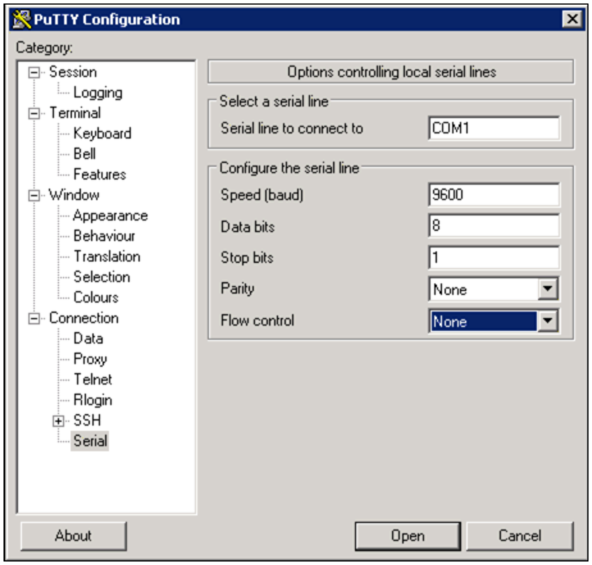


Figure 7-1 IBM SAN06B-R Serial Port

   b. Connect the DB9 end to a mobile computer or desktop equipped with an appropriate serial interface.

2. On a Windows-based PC, launch your serial terminal emulator. We use the Putty program.

3. Select the appropriate COM port associated with the serial connection. Figure 7-2 shows an example where COM1 is used.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

Figure 7-2 Selecting the correct COM port and settings

4. Select the settings, which for this connection are the same as other b-type family products: 9600, 8, None, 1, and None, as shown in Figure 7-2 on page 115.
5. Click **Open**, and then press Enter to get a login prompt.
6. Log in. The default login details are also the same as other b-type products. The login ID is *admin* and the default password is *password*.

   After entering the default login and password details, press Ctrl+C to leave the request to change the default passwords. Until the passwords have been changed, this request appears at every login to the CLI. See Example 7-1.

   Important: In production environments, be sure that passwords are not left at the default. Consult your local security guidelines for password policies. It is suggested to always use a centralized authentication service in larger production environments. Fabric OS v6.2.0e supports the standard RADIUS authentication service.

Example 7-1 Initial login

```
Fabric OS (switch)
Fabos Version 6.4.1


switch 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.
switch:admin>
```

Note: If a Console switch is present, the user can also connect the serial port to a console switch and access the switch through the Console switch for the initial configuration.

Setting the switch name

The switch name of the SAN06B-R can be up to 15 characters long, can include alphanumeric, and underscore characters, and must begin with an alpha character. Setting meaningful names for switches simplifies the management of the SAN. Define an appropriate naming convention and use this naming convention to provide standardized names for switches.

To customize the name, follow these steps:

1. Enter the **switchName** command with the new name, as in Example 7-2. The change will be committed but the prompt does not change until the Telnet session is reconnected.

   Example 7-2 Changing the SAN768B name

   ```
   switch:admin> switchname IBM_2498_R06
   Committing configuration...
   Done.
   switch:admin>
   ```

2. Record the new name for future reference.

Setting the IP address

The next task is to set the IP address so that we can access the SAN06B-R from the LAN. Use the **ipaddrshow** command, shown in Example 7-3, to display the current IP settings. Use the **ipaddrset** command to change these settings.

Example 7-3 Displaying the IP address

```
IBM_2498_R06:admin> ipaddrshow

SWITCH
Ethernet IP Address: 10.77.77.77
Ethernet Subnetmask: 255.255.255.0
Gateway IP Address:
DHCP: Off
IPv6 Autoconfiguration Enabled: Yes
Local IPv6 Addresses:
IPv6 Gateways:
IBM_2498_R06:admin>
```

From the output of the **ipaddrshow** command, see that the default IP address is 10.77.77.77, the default subnet mask is 255.255.255.0, and the default gateway is not defined.

Use the **ipaddrset** command to change this to your specific IP settings, as in Example 7-4. This command is interactive and prompts the user for each line of input. Accept the defaults or input new values.

Example 7-4 Changing the IP address (output shortened)

```
IBM_2498_R06:admin> ipaddrset
Ethernet IP Address [10.77.77.77]:10.18.228.31
Ethernet Subnetmask [255.255.255.0]:255.255.255.0
Gateway IP Address [0.0.0.0]:10.18.228.1
DHCP [Off]:
IP address is being changed...Done.
```

Physically connect the Ethernet management interface to the LAN and point the web browser at the router's IP address to access the Web Tools management GUI. IP connectivity is also necessary for upgrading the Fabric OS, because this is downloaded from a file server. If you cannot reach the newly configured IP interface, first try sending a ping from a device located on the same IP subnet as the SAN06B-R. If this fails, check cables and the IP configuration by using the **ipaddrshow** command. Check for any firewalls on the IP network that is blocking the access.

Upgrading the Fabric OS

The multi protocol routers use the same Fabric OS package as the rest of the b-type family. To download the latest firmware for the router, go to the following web page:

http://www.ibm.com/storage/support/san/

From here, select the correct Router model and select the download page. Follow the links to download the 6.x firmware. Be aware that following the download link from the IBM support web site redirects you to the Brocade web site, which lists the code packages supported by IBM for download.

To upgrade the FOS, you must have either an FTP server that is reachable from the SAN06B-R, or you can use the Data Centre Fabric Manager application. Starting with FOS v.5.3.0, a secure copy (SCP) option is also supported. After download, extract the code package to a directory available through the FTP / SCP server to access during the upgrade with CLI. If using DCFM, the firmware will be imported to the DCFM firmware repository and can be used during the upgrade process.

> **Important:** Always read the release notes for the version of Fabric OS that you are installing. For release notes, select the **6.x release notes** link from the link mentioned previously.

We use the **version** command from the router CLI to display the currently running code level. See Example 7-5.

Example 7-5 Displaying the code version

```
IBM_2498_R06:admin> version
Kernel:     2.6.14.2
Fabric OS:  v6.4.1
Made on:    Thu Oct 7 00:35:44 2010
Flash:      Sat Oct 30 00:02:37 2010
BootProm:   1.0.9
IBM_2498_R06:admin>
```

From here, we see that Version 6.4.1 is installed, which is the latest version at the time of writing. If the router has an older firmware versions, we need to plan for version upgrades as required. The release notes of the new firmware need to be checked for details of pre-requisites and enhancement changes provided by the later FOS firmware versions.

> **Tip:** Make a backup of the configuration prior to performing the firmware update. Use the **configupload** command to upload the configuration to the FTP server.

Before starting the firmware download process, alter the 10-minute Telnet session timeout value. By setting the value to 0 (zero), the session will never timeout. Use the **timeout** command, as in Example 7-6, and then log out and log in again.

Example 7-6 Setting the idle timeout value

```
IBM_2498_R06:admin> timeout
Current IDLE Timeout is 10 minutes
IBM_2498_R06:admin> timeout 0
IDLE Timeout Changed to 0 minutes
The modified IDLE Timeout will be in effect after NEXT login
IBM_2498_R06:admin>
................................
Logout then re-login
............................

IBM_2498_R06:admin> timeout
Current IDLE Timeout is 0 minutes
```

The upgrade is nondisruptive to FC ports, but FCIP traffic might be disrupted if the Ethernet controller needs to be upgraded. The SAN06B-R control processor

(CP) will reboot during **firmwaredownload**, meaning that the IP CLI session will be disconnected. You are able to re-log in almost immediately, although the upgrade will still be ongoing and the process status can be checked using the **firnmwaredownloadstatus** command. The entire upgrade process can take up to 30 minutes.

> **Tip:** Prior to performing the upgrade, note the relative path to the directory where the FOS files reside when logged into the FTP server. Upgrading from FOS versions prior to v5.2.x requires the `release.plist` suffix to the path.

Initial device settings

Before starting the process of adding a router device into a metaSAN configuration, confirm the following settings:

- Device time

  All devices in the metaSAN should have their local time set correctly. This can be done using the **date** and **tstimezone** commands. Afterwards, a network time protocol (NTP) server should be configured to ensure that the device clock does not drift. This can be done through the **tsclockserver** command.

  > **Tip:** Configure a known, good NTP server. A local server is ideal, but an Internet server works as well.

- Licenses

  To display the currently installed licenses, use the **licenseshow**. command. Licenses are added or removed using either the **licenseadd** or **licenseremove** command.

- SNMP

  Simple network management protocol (SNMP) can automatically send device events to a central trap. A common practice is for event monitoring always to be implemented in production environments. SNMP can be configured using the **snmpconfig** command.

- RADIUS

  For centralized user validation when logging into the SAN04B-R, configure one or more remote authentication dial-in user service (RADIUS) servers. This can be done using the **aaaconfig** command.

- Syslog

  For uploading logs to a system logging daemon (syslog) use the **syslogdipadd** command. To show current syslog configuration use the **syslogdipshow** command. Fabric Manager can also be used for this.

- Security banner

  For security reasons, set a login banner. Setting the banner can be done by using the **bannerset** command, which is interactive and allows you to type in the banner text. Use a periond (.) at the beginning of a new line to finish input.

  Example 7-7 shows how to set a security banner.

Example 7-7 Setting the banner

```
IBM_2498_R06:admin> bannerset
Please input content of security banner (press "." and RETURN at the beginning
of a newline to finish input):
                =======   ============      ======       ======
                =======   ==============    =======     =======
                  ===       ===     ====      ======   ======
                  ===       ===========       ======= =======
                  ===       ===========       === ======= ===
                  ===       ===     ====      ===  =====  ===
                =======    =============    =====   ===   =====
                =======    ===========      =====    =    =====

        This system is private and only for purposes autorised by IBM,
                Any unauthorised use may be subject to legal actions.
.
IBM_2498_R06:admin>
```

Initial setup is now completed.

7.2 Management tools introduction

The SAN multiprotocol routers, and the blade options for the SAN768B and SAN256B directors can be managed by the tools used for B type switches.

- CLI
- Web Tools
- Data Center Fabric Manager

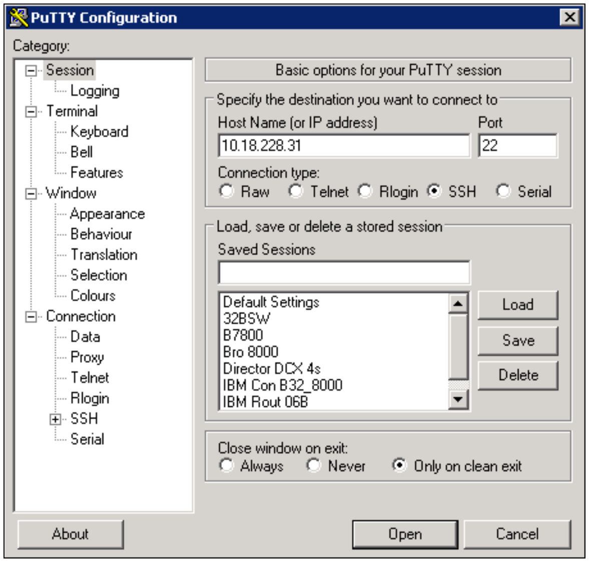
7.2.1 Command-line interface

The CLI can be accessed in a number of ways:

- Terminal emulation through the serial management port
- Telnet
- Secure shell (SSH)

To start an SSH session with the switch, follow these steps:

1. Start PuTTY by clicking the desktop icon. The PuTTY Configuration window displays (Figure 7-3).



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.18.228.31

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

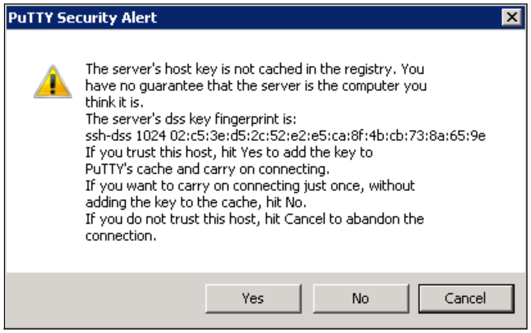
Default Settings
32BSW
B7800
Bro 8000
Director DCX 4s
IBM Con B32_8000
IBM Rout 06B

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 7-3 Starting a SSH Session

2. Enter the IP address of the switch in the Host Name (or IP address) text box.
3. Select the **SSH** radio button.
4. Click **Open**.

For a first-time connection, the Security Alert dialog box opens, as shown in Figure 7-4. Click **Yes** to accept the certificate and add it to your registry.



PuTTY Security Alert

The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's dss key fingerprint is:
ssh-dss 1024 02:c5:3e:d5:2c:52:e2:e5:ca:8f:4b:cb:73:8a:65:9e
If you trust this host, hit Yes to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the
connection.

Figure 7-4 SSH Security Alert

Example 7-8 shows the CLI interface accessed through SSH.

Example 7-8 CLI through SSH

```
login as: admin
admin@10.18.228.31's password:
                =======   ============      ======       ======
                =======   ==============    =======     =======
                  ===       ===     ====      ======   ======
                  ===       ===========       ======= =======
                  ===       ===========       === ======= ===
                  ===       ===     ====      ===  =====  ===
                =======    =============    =====   ===   =====
                =======    ===========      =====    =    =====

        This system is private and only for purposes autorised by IBM,
                Any unauthorised use may be subject to legal actions.

-----------------------------------------------------------------
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.
IBM_2498_R06:admin>
```

> **Note:** Always use SSH for accessing the CLI. Telnet is an older generation protocol with no built-in security. Use the serial management port only for certain maintenance tasks or if the IP network is down.

The CLI can be used for all configuration tasks and is the preferred way to do advanced configuration. A help function is available by typing the **help** command followed by an argument, which is the name of the command that you want help about. The help pages are displayed as standard UNIX manual (man) pages. If no argument is given, a list of possible FOS commands is listed. Newer versions of FOS support piping to **grep**, which is useful if you are searching for a particular command, or want to limit command output.

Example 7-9 shows the commands that are listed when we issue **grep help** for the **fcr** command.

Example 7-9 grep and help

```
IBM_2498_R06:admin> help | grep fcr
fcrbcastconfig             Configure interfabric broadcast frame
forwarding
fcrchiptest                Functional Test of FCR FPGA.
fcrconfigure               Sets FC Router configuration parameters.
fcredgeshow                Displays FIDs assigned to defined EX_Port
fcrfabricshow              Displays FC Routers on a backbone fabric.
fcrlsan                    Configure LSAN policies
fcrlsancount               Display maximum LSAN zone limit.
fcrlsanmatrix              Manage LSAN fabric matrix configuration.
fcrpathtest                Data Path Test on Connection between FCR
FPGA and
fcrphydevshow              Displays FC Router physical device
information.
fcrproxyconfig             Displays or configures proxy devices
presented by
fcrproxydevshow            Displays FC Router proxy device information.
fcrresourceshow            Displays FC Router physical resource usage.
fcrrouterportcost          Modify FC Router port cost configuration.
fcrrouteshow               Displays FC Router route information.
fcrxlateconfig             Displays or persistently configures a
translate
IBM_2498_R06:admin>
```

7.2.2 Web Tools

After completing the initial setup of the router, including the assignment of an IP address to the Ethernet interface, we can access the Web Tools GUI management interface. Web Tools offers a GUI that provides an easy-to-use method for performing almost all management tasks. Web Tools is preferred to the CLI when you want a system overview.

Web Tools requires an Internet browser that conforms to Hypertext Markup Language (HTML) Version 4.0 and JavaScript Version 1.0. It also requires a Java™ runtime plug-in Version 1.6.0 or later.

Web Tools is supported on the following platforms: Microsoft Windows 2000 SP4, Microsoft Windows XP SP2, Microsoft Windows 2003 Server SP1, Sun Solaris 10, and Red Hat Linux AS3 and AS4. Supported browsers include: Internet

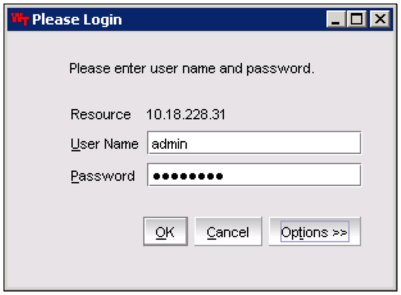
Explorer 6.0 and 7.0, and Mozilla Firefox 2.0. When using platforms based on non-English software versions, set the user locale to English (United States).

Note: Web Tools requirements change frequently as new browser and Java versions are released. Always check with Web Tools documentation for requirements and support information.

For the best performance, an adequate amount of system memory (RAM) is recommended:

- 256 MB or more RAM for fabrics comprising 15 or fewer switches/multiprotocol routers
- 512 MB or more RAM for fabrics comprising more than 15 switches/multiprotocol routers
- A minimum of 8 MB of video RAM

To launch Web Tools, point your Internet browser to the IP (or DNS name if available) of the device that will be managed. A Java applet will be downloaded, and then a login dialog box (Figure 7-5) opens.



Please enter user name and password.

Resource 10.18.228.31

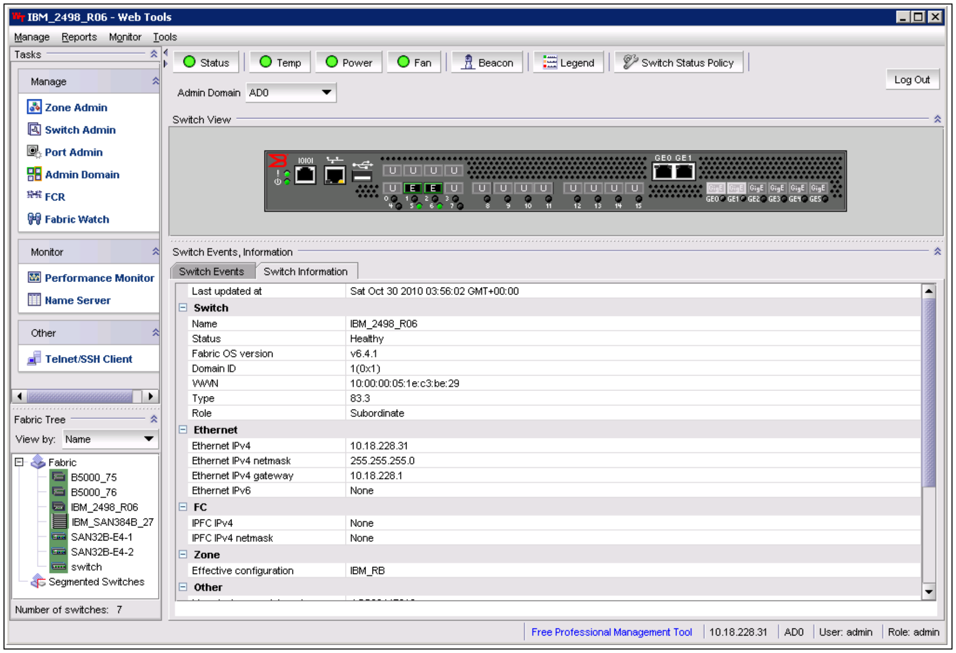
User Name admin

Password •••••••••

Figure 7-5 Login dialog box

After you log in, the Web Tools main view is loaded.

Figure 7-6 shows the Web Tools main view for a SAN06B-R.



Last updated at	Sat Oct 30 2010 03:56:02 GMT+00:00
Switch	
Name	IBM_2498_R06
Status	Healthy
Fabric OS version	v6.4.1
Domain ID	1(0x1)
WWN	10:00:00:05:1e:c3:be:29
Type	83.3
Role	Subordinate
Ethernet	
Ethernet IPv4	10.18.228.31
Ethernet IPv4 netmask	255.255.255.0
Ethernet IPv4 gateway	10.18.228.1
Ethernet IPv6	None
FC	
IPFC IPv4	None
IPFC IPv4 netmask	None
Zone	
Effective configuration	IBM_RB
Other	

Figure 7-6 SAN06B-R Web Tools

Web Tools is similar to other GUIs, with clickable buttons, drop-down menus, and so forth. For details of the Web Tools application, refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

7.2.3 Data Center Fabric Manager

A key component of the IBM DCF (Data Center Fabric) architecture is the IBM System Storage Data Center Fabric Manager (DCFM). This component is an end-to-end fabric management software platform that combines capabilities of two existing fabric management software packages from IBM:

- Enterprise Fabric Connectivity Manager (EFCM)
- Fabric Manager

The DCFM architecture integrates the best management features of EFCM and Fabric Manager. It is based on EFCM's GUI, and Fabric Manager's messaging and data management design for improved performance and scalability.

The two versions of the DCFM product are as follows:

- DCFM Professional, free with IBM b-type switches
- DCFM Enterprise Licensed Product by Server

DCFM Professional

DCFM Professional is free product and is targeted at customers seeking a less extensive management solution for smaller SANs. This software is included with IBM b-type switches and has the following functionality:

- Allows management of a single Fabric OS (FOS) fabric (up to a 1,000 switch ports) at a time.
- Performs group switch management beyond the scope of Web Tools.

DCFM Professional is available with the purchase of any IBM b-type switch and is also available for download from the IBM web site.

```
http://www.ibm.com
```

Note: DCFM Professional does not allow use as Fusion Agent proxy for management applications such as IBM TPC.

Features not supported but available in Enterprise Edition are as follows:

- Full IBM/Brocade Backbone management with features such as QoS and end-to-end performance monitoring
- Support for up to 24 physical fabrics, 9,000 switch ports, and 20,000 end devices
- IBM FICON management for mainframe environments
- Comprehensive FCR (Fibre Channel Routing) and FCIP management
- Advanced Call Home Support
- Support for security schemes (RADIUS, LDAP, Active Directory, NIS/NIS+, and more)
- Historical performance data collection
- Data persistence for up to two years of data, out-of-box Open Database Connectivity (ODBC), and Java Database Connectivity (JDBC) access
- M-EOS support
- Remote clients
- Other features are not necessarily supported but they are supported in Enterprise Edition

Note: DCFM Professional does not support IBM System Storage SAN768B, SAN384B, Brocade DCX and m-EOS.

DCFM Enterprise Edition

DCFM Enterprise Edition is an enterprise-class product targeted at customers that demand a management software solution with comprehensive support for:

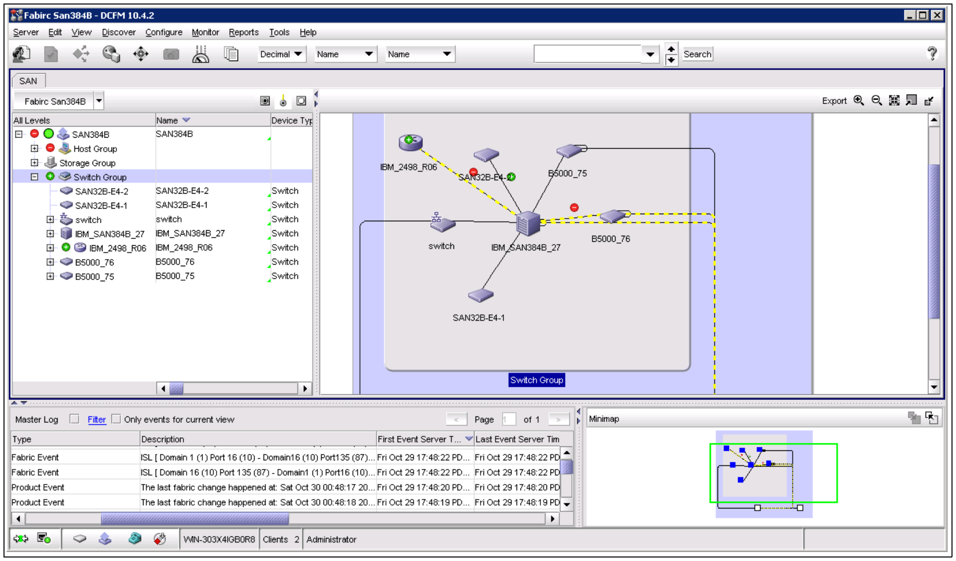
- IBM/Brocade Backbone switches: Data Center Fabric (DCF)
- Fabric-based encryption support for data-at-rest solutions
- End-to-end manageability of the data center fabric from HBA ports through switch ports to storage ports

> **Note:** DCFM Enterprise Edition allows the use of a Fusion Agent proxy for management applications such as IBM TPC.

DCFM Enterprise Edition provides multiprotocol networking support for:

- Fibre Channel
- Fiber Connectivity (FICON)
- Fibre Channel over IP (FCIP)
- Fibre Channel Routing (FCR)
- Internet SCSI (iSCSI)
- Fibre Channel over Ethernet (FCoE) and Converged Enhanced Ethernet (CEE)

Figure 7-7 shows the Data Center Fabric Manager application initial view with a router introduced to Fabric with only the ISL to core director switch.



All Levels	Name	Device Typ
SAN384B	SAN384B	
Host Group		
Storage Group		
Switch Group		
SAN32B-E4-2	SAN32B-E4-2	Switch
SAN32B-E4-1	SAN32B-E4-1	Switch
switch	switch	Switch
IBM_SAN384B_27	IBM_SAN384B_27	Switch
IBM_2498_R06	IBM_2498_R06	Switch
B5000_76	B5000_76	Switch
B5000_75	B5000_75	Switch

Master Log □ Filter □ Only events for current view Page 1 of 1

Type	Description	First Event Server T...	Last Event Server Tim
Fabric Event	ISL [Domain 1 (1) Port 16 (10) - Domain16 (10) Port135 (87)...	Fri Oct 29 17:48:22 PD...	Fri Oct 29 17:48:22 PD
Fabric Event	ISL [Domain 16 (10) Port 135 (87) - Domain1 (1) Port16 (10)...	Fri Oct 29 17:48:22 PD...	Fri Oct 29 17:48:22 PD
Product Event	The last fabric change happened at: Sat Oct 30 00:48:17 20...	Fri Oct 29 17:48:20 PD...	Fri Oct 29 17:48:20 PD
Product Event	The last fabric change happened at: Sat Oct 30 00:48:18 20...	Fri Oct 29 17:48:19 PD...	Fri Oct 29 17:48:19 PD

WIN-303X4IGB0R8 | Clients 2 | Administrator

Figure 7-7 Data Center Fabric Manager initial view

For more details about DCFM, refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

8

Routing in virtual fabrics

The FC-FC routing service provides Fibre Channel routing (FCR) between two or more fabrics without merging those fabrics. With virtual fabrics, physical switches can be partitioned into independently managed logical switches, each with their own data, control, and management paths.

In this chapter, we discuss the issues that arise when combining the functionality of routing within a virtual fabric environment.

8.1 Routing and virtual fabrics

IBM/Brocade Virtual Fabric is available on the SAN40B-4, SAN80B-4, SAN384B, and SAN768B switches with Fabric OS version 6.2.0 and later. In-depth details about virtual fabrics is beyond the intended scope of this book.

For comprehensive details about implementing virtual fabrics in an IBM/Brocade environment, refer toIBM Redbooks publication *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116 and to your router's administration guide.

During this chapter, we describe FC-FC routing, logical switch configuration, backbone to edge, virtual fabrics on FCIP, lossless dynamic load sharing, and provide an example of routing over virtual fabrics.

8.1.1 FC-FC routing and virtual fabrics

If virtual fabrics are not enabled, the FC-FC routing behavior is unchanged. If virtual fabrics are enabled, then in the FC-FC routing context, a base switch acts as a backbone switch. A base fabric is similar to a backbone fabric.

If virtual fabrics are enabled, the following rules apply:

- EX_Ports and VEX_Ports can be configured only on the base switch.
  - When you enable virtual fabrics, the chassis is automatically rebooted. When the switch comes up, only one default logical switch is present, with the default fabric ID (FID) of 128.
  - All previously configured EX_Ports and VEX_Ports are persistently disabled with the reason "ExPort in non base switch." You must explicitly create a base switch and move the EX_ and VEX_Ports to the base switch. The ports are then automatically enabled.
  - If you move existing EX_Ports or VEX_Ports to any logical switch other than the base switch, these ports are automatically disabled.
  - If you want to change an EX_Port or VEX_Port on the logical switch to be a non-EX or VEX_Port, you must use the **portCfgDefault** command. You cannot use the **portCfgExPort** command because that command is allowed only on the base switch.
- EX_Ports can connect to a logical switch that is in the same chassis or a different chassis. However, the FID of the EX_Port must be set to a different value from the FID of the logical switch to which it connects. That is, the EX_Port and the logical switch to which it connects must be in different fabrics.

- EX_Ports and VEX_Ports in FC routers and those in a base switch cannot connect to any edge fabric with logical switches configured to use XISLs.
  - If you connect an EX_Port or VEX_Port to an edge fabric, you must ensure that no logical switches are enabled with XISL use in that edge fabric.
  - If any logical switch in the edge fabric allows XISL use, then the EX_Port or VEX_Port is disabled.
  - Because XISL use is disallowed, dedicated links must be configured to route traffic across fabrics. Backbone-to-edge routing is not supported in the base switch.
- If you connect an FC router in legacy mode to a base switch, set the backbone FID of the FC router to be the same as that of the base switch.
- All FCR commands can be executed only on the base switch.
- The `fcrConfigure` command is not allowed when virtual fabrics is enabled. Instead, use the `lsCfg` command to configure the FID.

Note: If you connect an EX_Port or VEX_Port from an FC router running Fabric OS v6.1.x or earlier to a logical switch that allows XISL use, the EX_Port or VEX_Port is not disabled. This configuration is not supported and you should avoid it.

8.1.2 Logical switch configuration for FC routing

As an example, Figure 8-1 shows two chassis' partitioned into logical switches. This configuration allows the device in Fabric 128 to communicate with the device in Fabric 15 without merging the fabrics.

- The base switch in Physical chassis 1 serves as an FC router and contains EX_Ports that connect to logical switches in the two edge fabrics, Fabric 128 and Fabric 15.
- The logical switches in Fabric 128 and Fabric 15 are connected with physical ISLs, and do not use the XISL connection in the base fabric.
- The logical switches in Fabric 1 are configured to allow XISL use. You cannot connect an EX_Port to these logical switches, so the device in Fabric 1 cannot communicate with anything outside Fabric 1.

Figure 8-1 also shows that EX_Ports exist only in the base switch.

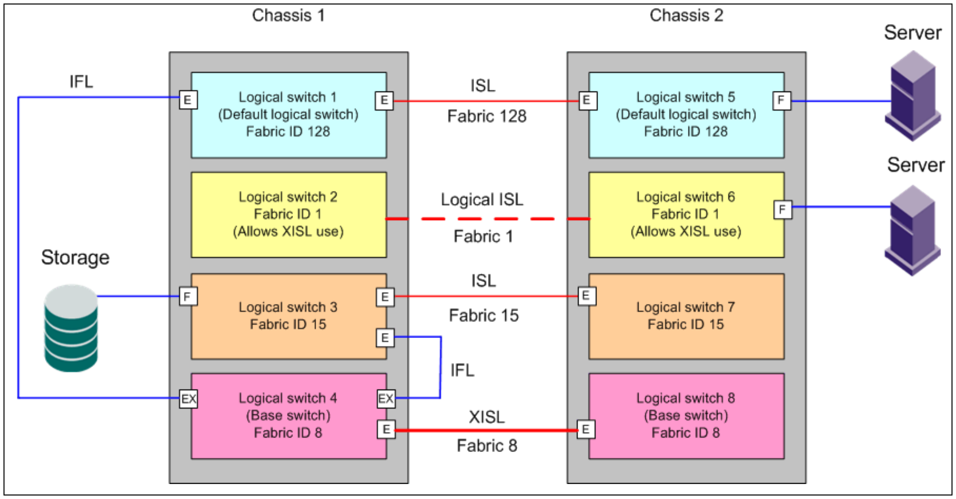


Figure 8-1 EX_Ports in a base switch

Figure 8-2 shows the following information:

- A logical representation of the physical chassis and devices of Figure 8-1 on page 132
- Fabric 128 and Fabric 15 are edge fabrics connected to a backbone fabric. Fabric 1 is not connected to the backbone, so the device in Fabric 1 cannot communicate with any of the devices in the other fabrics.
- The logical representation of EX_Ports in the base switch

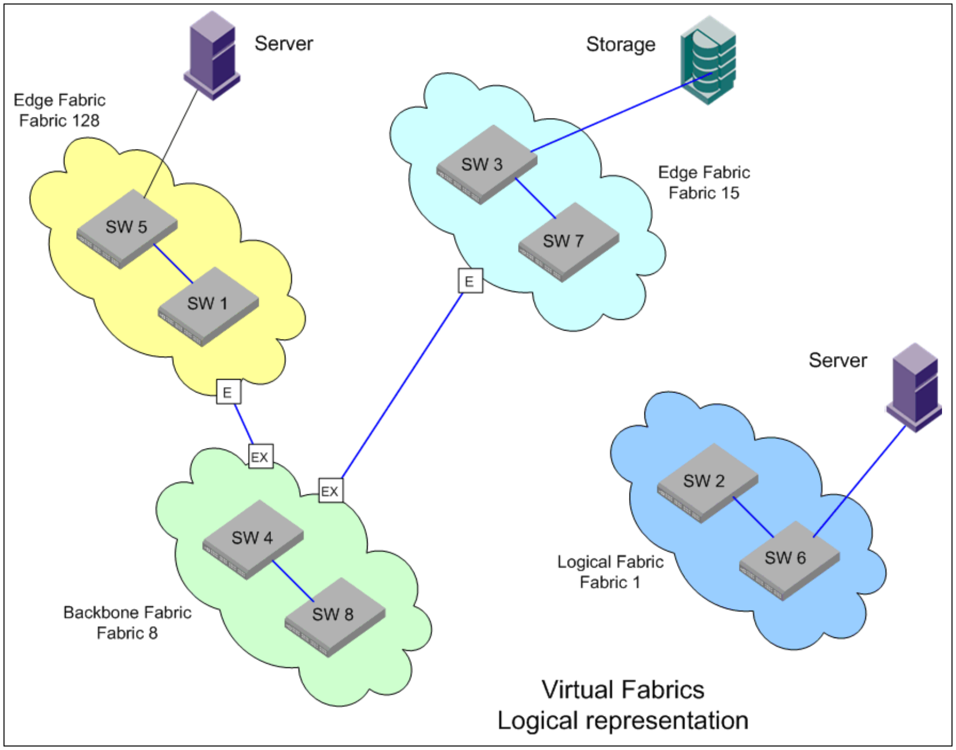


Figure 8-2 Logical representation of EX_Ports in a base switch

8.1.3 Backbone-to-edge routing with virtual fabrics

Because the base switch does not allow F_Ports, you cannot have devices connected to the base switch. Although F_Ports are not allowed in the base switch, they are allowed in an FC router in legacy mode (Fabric OS v6.1.x or earlier, or Fabric OS v6.2.0 or later with virtual fabrics disabled). If you connect an FC router in legacy mode to the base switch, backbone-to-edge routing is supported on that FC router.

In Figure 8-1 on page 132, no devices can be connected to the backbone fabric (Fabric 8) because base switches cannot have F_Ports. Figure 8-3 shows an FC router in legacy mode connected to a base switch. This FC router can have devices connected to it, and so you can have backbone-to-edge routing through this FC router. In this example, Host A in the backbone fabric can communicate with device B in the edge fabric with FID 20; however, host A cannot communicate with device C, because the base switches do not support backbone-to-edge routing.

Figure 8-3 shows backbone-to-edge routing across the base switch using the FC router in legacy mode.

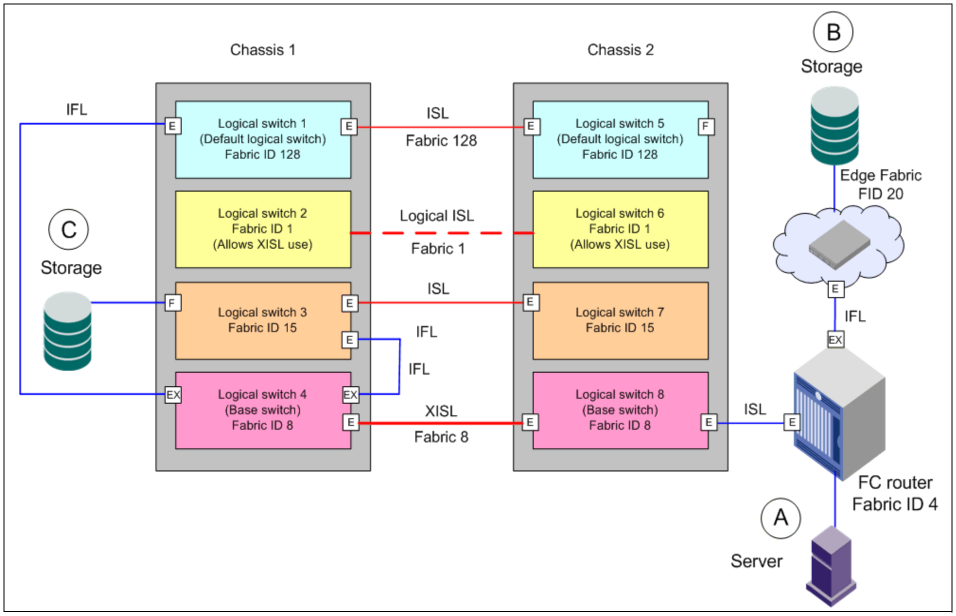


Figure 8-3 Backbone-to-edge routing using FC router in legacy mode

8.1.4 Virtual fabrics and FCIP

Certain factors must be considered when you implement FCIP in a virtual fabric environment. The following rules apply for the Gigabit Ethernet ports (GbE ports) when enabling virtual fabrics:

- Any GbE port and all of its associated FCIP tunnels on a chassis can be assigned to any logical switch. As with the current Fabric OS, the port types supported by FCIP are either VE_Port or VEX_Port.
- When a GbE port is moved to a logical switch, all eight VE_Port and VEX_Ports are automatically moved. No interaction is required to assign or move them.

The following constraints apply to VE_Ports and VEX_Ports:

- All VEX_Ports are persistently disabled when virtual fabric mode is enabled. You must create a logical switch with the base switch attribute turned on and move the ports to the new base switch.
- The ports must be offline before they are moved from one logical switch to another.
- A logical switch is independent of the base switch. Therefore, all GbE port based protocol addresses, such as IP addresses, must be unique within a logical switch.
- FCIP tunnels working as an extended ISL can carry traffic for multiple fabrics. Therefore, a GbE port used as an extended ISL must be assigned to the base switch.

8.1.5 Lossless Dynamic Load Sharing in virtual fabrics

It is possible to enable Lossless Dynamic Load Sharing in a virtual fabric environment. This feature is optional on the logical switches that we can define in the virtual fabric. When enabling this feature, make sure it is done on a per logical switch basis,. Be aware that it can affect the other logical switches in the fabric. XISL use must be disabled for Lossless DLS to be enabled.

Note: Downgrading to Fabric OS v6.2.0 is not supported if Lossless DLS is enabled.

If you have Lossless DLS enabled, but in the same switch DLS, IOD and port-based are not enabled, the downgrade will fail, because Fabric OS v6.2.0 does not support this combination.

The exchange-based routing policy depends on the Fabric OS Dynamic Load Sharing feature (DLS) for dynamic routing path selection. When using the exchange-based routing policy, DLS is enabled by default and cannot be disabled. In other words, you cannot enable or disable DLS when the exchange-based routing policy is in effect.

When the port-based policy is in force, you can enable DLS to optimize routing. When DLS is enabled, it shares traffic among multiple equivalent paths between switches. DLS recomputes load sharing when any of the following occurs:

- A switch boots up
- An E_Port goes offline and online
- An EX_Port goes offline
- A device goes offline

8.2 An example of routing in virtual fabrics

In **Chapter 9, “FC-FC routing implementation” on page 149** and Chapter 10, “FCIP implementation” on page 195, we discuss how to create routes over FC-FC and FCIP connections in a SAN that is not enabled for virtual fabric.

In this section, we explain how to establish routed connections in a virtual fabrics enabled environment, using the methods discussed previously in this chapter.

The goal is to make a connection between a server and storage. The server is connected to one logical switch, and the storage device is connected to another logical switch. These logical switches are in different fabrics, and merging the fabrics is not allowed.

In our scenario, we use two switches, a SAN384B and a SAN80B both capable of implementing virtual fabrics and performing internal routing over FC connections.

For details about creating and managing virtual fabrics, refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

8.2.1 Scenario description

Virtual fabrics are enabled on a two-chassis SAN. A UNIX server in one virtual fabric needs to access storage connected to a different virtual fabric as shown in Figure 8-4. Because the storage and server are connected to different virtual fabrics that cannot be merged, we have to create a route from one fabric to the other.

In the initial scenario, we do not have base switches because all switch interconnect links are ISLs. base switches are used for XISL connections, which are physical connections between switches. The base switches together with XISL connections provide Logical ISL (LISL) connections to logical fabrics.

Figure 8-4 shows the initial UNIX scenario.

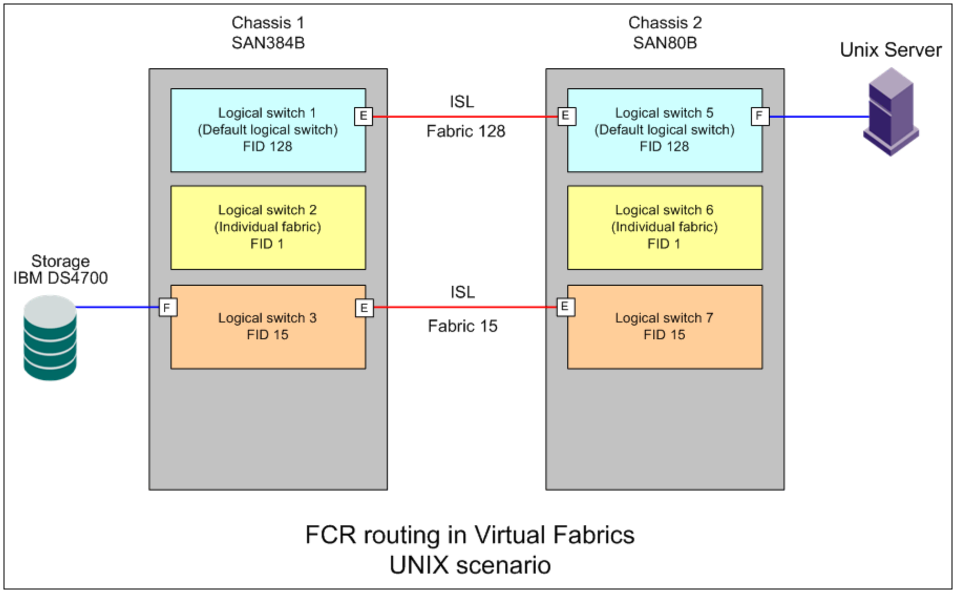


Figure 8-4 Initial UNIX setup

Because EX_Ports in a virtual fabric environment can only be applied to core switches, we must create a virtual fabric base switch acting as the core switch. On the base switch, we can make IFL connections to the respective fabrics where server and storage is connected. The IFL connections must be physical connections because a logical switch cannot be allowed to use XISLs if it connects to an EX_Port.

Figure 8-5 shows the solution for the routed connection for the UNIX scenario.

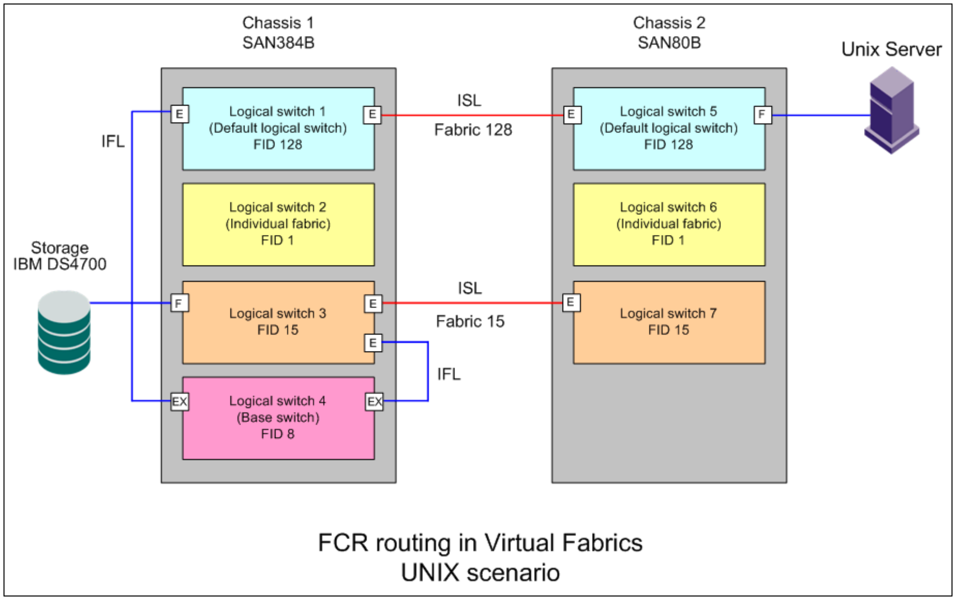


Figure 8-5 The UNIX solution

In “Reconfiguration steps” on page 139, we describe how to perform the reconfiguration that is made in Figure 8-5. We demonstrate this by using the command-line interface (CLI).

When a virtual switch is created, XISL use is allowed by default. The logical switches in Fabric 15 and Fabric 128, as shown in Figure 8-5, are all connected using ISL connections.

As mentioned earlier, logical switches cannot be allowed to use XISL connections, and must be configured to disallow XISL. This can be examined with the **`switchshow`** command, and changed with the **`configure`** command, after disabling the switch. In our example, we ensure that XISL-use is disallowed, before we begin the reconfiguration steps described in “Reconfiguration steps” on page 139.

In case the use of XISLs are enabled on a logical switch, all connections to E_Ports (ISLs), connections to EX_Ports (IFLs), will be automatically disabled.

Reconfiguration steps

Perform the following steps to reconfigure:

1. Create the base switch as in Example 8-1.

Example 8-1 Creating the base switch

```
IBM_SAN384B_213:FID128:admin> lscfg --create 8 -base
Creation of a Base Switch requires that the proposed new Base Switch on
this system be disabled.
Would you like to continue [y/n]?: y
About to create switch with fid=8. Please wait...
Logical Switch with FID (8) has been successfully created.

Logical Switch has been created with default configurations.
Please configure the Logical Switch with appropriate switch
and protocol settings before activating the Logical Switch.
```

2. Configure the switch domain ID of the newly created base switch as in Example 8-2.

Example 8-2 Configuring Domain ID for the base switch

```
switch_8:FID8:admin> switchdisable
switch_8:FID8:admin> configure

Configure...

  Fabric parameters (yes, y, no, n): [no] y

    Domain: (1..239) [1] 4

CTRL-D

COMMAND OUTPUT REMOVED FOR CLARITY

switch_8:FID8:admin>switchenable
```

We are adding ports to the base switch. These ports are going to be used for the IFL connections to the logical switches. The ports are enabled so that they can be used in the base switch, as in Example 8-3.

Example 8-3 Adding ports to the base switch at backbone

```
switch_8:FID8:admin> lscfg --config 8 -slot 2 -port 25
This operation requires that the affected ports be disabled.
Would you like to continue [y/n]?: y
Making this configuration change.  Please wait...
Configuration change successful.
Please enable your ports/switch when you are ready to continue.
switch_8:FID8:admin> lscfg --config 8 -slot 2 -port 6
This operation requires that the affected ports be disabled.
Would you like to continue [y/n]?: y
Making this configuration change.  Please wait...
Configuration change successful.
Please enable your ports/switch when you are ready to continue.

switch_8:FID8:admin> portenable 2/25
switch_8:FID8:admin> portenable 2/6
```

3. Enable FCR as in Example 8-4.

Example 8-4 Enabling FCR at backbone (the base switch)

```
switch_8:FID8:admin> fosconfig --enable fcr
FC Routing service is enabled
```

4. Configuring the routed ports at the backbone. Routed ports must be disabled prior to setting EX_Port attributes. The ports must be enabled before the port can become active following EX_Port parameter changes. Use the **portDisable** or **portEnable** command respectively to disable or enable the port.

   With the **portcfgexport** command, specify the FID of the link to the edge fabric, and specify front domain ID, as in Example 8-5.

Example 8-5 Configuring EX_Ports at backbone (the base switch)

```
switch_8:FID8:admin> portdisable 2/25
switch_8:FID8:admin> portdisable 2/6

switch_8:FID8:admin> portcfgexport 2/25 -a 1 -f 41 -d 120
switch_8:FID8:admin> portcfgexport 2/6 -a 1 -f 42 -d 121

switch_8:FID8:admin> portenable 2/25
switch_8:FID8:admin> portenable 2/6
```

5. Check the new status of the ports, as in Example 8-6.

Example 8-6 Checking port status

```
switch_8:FID8:admin> portshow 2/25
portName:
portHealth: HEALTHY

Authentication: None

EX_Port Mode:   Enabled
Fabric ID:      41

switch_8:FID8:admin> portshow 2/6
portName:
portHealth: HEALTHY

Authentication: None

EX_Port Mode:   Enabled
Fabric ID:      42

COMMAND OUTPUT REMOVED FOR CLARITY
```

Our routed connections (IFL connections) are now configured.

6. Check the result with the **fabricshow** command, as in Example 8-7.

Example 8-7 Fabricshow at the backbone

```
switch_8:FID8:admin> fabricshow
Switch ID   Worldwide Name          Enet IP Addr Name
-----------------------------------------------------------------------
  4: fffc04 10:00:00:05:1e:94:3a:03 10.64.210.213 >"switch_8"

COMMAND OUTPUT REMOVED FOR CLARITY
```

The backbone switch (the base switch) is only aware of itself in the fabric. The edge switches are aware of themselves, the ISL-connected switches, and now also the front domain specified in Example 8-5 on page 140, which represents the routed fabric. See Example 8-8.

Example 8-8 Fabricshow at the edge FID 128

```
IBM_SAN384B_213:FID128:admin> fabricshow
Switch ID   Worldwide Name          Enet IP Addr Name
-----------------------------------------------------------------------
  1: fffc01 10:00:00:05:1e:94:3a:00 10.64.210.213 "IBM_SAN384B_213"
  5: fffc05 10:00:00:05:1e:09:97:01 10.64.210.217 >"IBM_SAN80B_217"
120: fffc78 50:00:51:e9:43:a0:3e:29 0.0.0.0 "fcr_fd_120"

The Fabric has 3 switches

COMMAND OUTPUT REMOVED FOR CLARITY
```

Example 8-9 shows a **fabricshow** command at the edge FID 15.

Example 8-9 Fabricshow at the edge FID 15

```
switch_15:FID15:admin> fabricshow
Switch ID   Worldwide Name          Enet IP Addr Name
-----------------------------------------------------------------------
  3: fffc03 10:00:00:05:1e:94:3a:02 10.64.210.213 >"blue_1"
  7: fffc07 10:00:00:05:1e:09:97:03 10.64.210.217 "blue_2"
121: fffc79 50:00:51:e9:43:a0:3e:2a 0.0.0.0 "fcr_fd_121"

The Fabric has 3 switches

COMMAND OUTPUT REMOVED FOR CLARITY
```

Our IFL connections are now completed

7. Configure LSAN zones so that the server can see the storage. The creation of LSAN zones can be done by using CLI, Web Tools, and DCFM. (In 10.4.3, “Creating LSAN zones” on page 228, we show how to create LSAN zones.)

   Example 8-10 shows LSAN-zone creation at FID15.

Example 8-10 Creating LSAN-zones at the edge fabric FID 15

```
switch_15:FID15:admin> alicreate AIX_1, 10:00:00:00:c9:4c:8c:1c
switch_15:FID15:admin> alicreate DS4000_A, 20:06:00:a0:b8:48:58:a1
switch_15:FID15:admin> zonecreate LSAN_AIX_1_DS4000_A, "AIX_1;DS4000_A"
switch_15:FID15:admin> cfgcreate FID15_cfg, LSAN_AIX_1_DS4000_A
switch_15:FID15:admin> cfgsave
```

```
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no,
n): [no] y
Updating flash ...

switch_15:FID15:admin> cfgenable FID15_cfg
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'FID15_cfg' configuration  (yes, y, no, n): [no] y
zone config "FID15_cfg" is in effect
Updating flash ...
```

Example 8-11 shows LSAN-zone creation at FID128.

Example 8-11 Creating LSAN-zones at the edge fabric FID 128

```
IBM_SAN80B_217:FID128:admin> alicreate AIX_1, 10:00:00:00:c9:4c:8c:1c
IBM_SAN80B_217:FID128:admin> alicreate DS4000_A, 20:06:00:a0:b8:48:58:a1
IBM_SAN80B_217:FID128:admin> zonecreate LSAN_AIX_1_DS4000_A, "AIX_1;DS4000_A"
IBM_SAN80B_217:FID128:admin> cfgcreate FID128_cfg, LSAN_AIX_1_DS4000_A
IBM_SAN80B_217:FID128:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no, n): [no] y
Updating flash ...

IBM_SAN80B_217:FID128:admin> cfgenable FID128_cfg
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'FID128_cfg' configuration  (yes, y, no, n): [no] y
zone config "FID128_cfg" is in effect
Updating flash ...
```

8. Log on to the base switch and execute the **lsanzoneshow** command. The output shows the devices in the LSAN zones and their status, as in Example 8-12.

Example 8-12 Checking the LSAN-zones

```
switch_8:FID8:admin> lsanzoneshow -s
Fabric ID: 41 Zone Name: LSAN_AIX_1_DS4000_A
        10:00:00:00:c9:4c:8c:1c  EXIST
        20:06:00:a0:b8:48:58:a1  Imported
Fabric ID: 42 Zone Name: LSAN_AIX_1_DS4000_A
        10:00:00:00:c9:4c:8c:1c  Imported
        20:06:00:a0:b8:48:58:a1  EXIST
```

9. Check using **fabricshow** command. The output now also shows the routing domain, as in Example 8-13.

Example 8-13 Fabricshow now also shows the routing domain

```
blue_1:FID15:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr Name
-----------------------------------------------------------------------
  1: fffc01 50:00:51:e9:43:aa:3f:01 0.0.0.0 "fcr_xd_1_41"
  3: fffc03 10:00:00:05:1e:94:3a:02 10.64.210.213 >"blue_1"
  7: fffc07 10:00:00:05:1e:09:97:03 10.64.210.217 "blue_2"
121: fffc79 50:00:51:e9:43:a0:3e:2a 0.0.0.0 "fcr_fd_121"

The Fabric has 4 switches

blue_1:FID15:admin> setcontext 128

-----------------------------------------------------------------
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.

IBM_SAN384B_213:FID128:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr Name
-----------------------------------------------------------------------
  1: fffc01 10:00:00:05:1e:94:3a:00 10.64.210.213 "IBM_SAN384B_213"
  2: fffc02 50:00:51:e9:43:aa:3f:02 0.0.0.0 "fcr_xd_2_42"
  5: fffc05 10:00:00:05:1e:09:97:01 10.64.210.217 >"IBM_SAN80B_217"
120: fffc78 50:00:51:e9:43:a0:3e:29 0.0.0.0 "fcr_fd_120"

The Fabric has 4 switches
```

We now show several additional useful commands for checking connectivity in routed fabrics, as in Example 8-14.

Example 8-14 Additional commands for checking the IFL-connections.

```
switch_8:FID8:admin> fcrfabricshow
FC Router WWN: 10:00:00:05:1e:94:3a:03, Dom ID:   4,
Info: 10.64.210.213, "switch_8"
   EX_Port       FID    Neighbor Switch Info (enet IP, WWN, name)
-----------------------------------------------------------------------
      89        41     10.64.210.213    10:00:00:05:1e:94:3a:00
"IBM_SAN384B_213"
      70        42     10.64.210.213    10:00:00:05:1e:94:3a:02
"blue_1"

switch_8:FID8:admin> fcrphydevshow
 Device           WWN           Physical
 Exists                           PID
in Fabric
-----------------------------------------
   41    10:00:00:00:c9:4c:8c:1c  051300
   42    20:06:00:a0:b8:48:58:a1  03e8c0
Total devices displayed: 2

switch_8:FID8:admin> fcrproxydevshow
  Proxy           WWN             Proxy      Device   Physical    State
 Created                           PID       Exists     PID
in Fabric                                   in Fabric
-----------------------------------------------------------------------
    41   20:06:00:a0:b8:48:58:a1  02f001       42      03e8c0
Imported
    42   10:00:00:00:c9:4c:8c:1c  01f001       41      051300
Imported

Total devices displayed: 2
```

The UNIX system can now see the two LUNs that were presented to the system from the DS4700 storage system, as in Example 8-15.

Example 8-15 UNIX now see the DS4700 LUNs presented to it.

```
root@Atlantic:/root # lspv
hdisk0         0009cdcaeb48d3a3                    rootvg
active
hdisk1         0009cdcac26dbb7c                    rootvg
active
hdisk2         0009cdcab5657239                    None
hdisk3         0009cdcae725b306                    testvg
active
hdisk4         0009cdcae725b44a                    testvg
active
root@Atlantic:/root # lsdev -Cc disk
hdisk0 Available 1S-08-00-8,0  16 Bit LVD SCSI Disk Drive
hdisk1 Available 1S-08-00-9,0  16 Bit LVD SCSI Disk Drive
hdisk2 Available 1S-08-00-10,0 16 Bit LVD SCSI Disk Drive
hdisk3 Available 1D-08-02      MPIO Other DS4K Array Disk
hdisk4 Available 1D-08-02      MPIO Other DS4K Array Disk
```

8.3 Summary

In this chapter, we have demonstrated how to enable FC-FC routing in a virtual fabrics-enabled environment.

The primary difference from traditional FC-routing, is that in a virtual fabrics-enabled environment, the base switch acts as the backbone, and EX_ports can only be created at the backbone. Because of that, a base switch must be enabled to perform routing.

The IBM 8 Gbps products that are virtual fabrics-capable are as follows:

- IBM SAN768B
- IBM SAN384B
- IBM SAN80B
- IBM SAN40B

Because a limitation exists for how many logical switches that a specified switch can enable, on the IBM SAN80B and the IBM SAN40B, the default switch can be used as the base switch, which saves one logical switch. Refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116.

Another important difference is that logical switches cannot be XISL-enabled. These and other constraints must be considered in a virtual fabrics-enabled environment, as explained in this chapter.

Virtual fabrics also support dynamic path selection (DPS) on all partitions. DPS is limited where multiple paths are available for a logical fabric frame entering a virtual fabric chassis from a base fabric that is sent out using one of the dedicated ISLs in a logical switch.

The appliance policy affecting the DPS behavior, whether it is exchange-based, device-based, or port-based, is configured on a per logical switch basis. IOD and DLS settings are set per logical switch as well. IOD and DLS settings for the base switch affect all traffic going over the base fabric including any logical fabric traffic that uses the base fabric. It is beyond the intended scope of this book, but it is documented in the administration guide of your switch/router.

9

FC-FC routing implementation

In this chapter, we show how to implement the Fibre Channel to Fibre Channel (FC-FC) routing service offered by the IBM System Storage b-type family of storage area network (SAN) multiprotocol routing products using the SAN384B and SAN32B-3 switches.

In particular, we discuss the following implementation topics:

- Edge fabrics connected through a backbone fabric
- Advanced configuration tasks

In the beginning of the scenario, we provide a setup diagram with important parameters.

The implementation topics primarily show configuration first with the CLI, and then with Web Tools. DCFM is also shown, especially when it provides a management advantage.

> **Note:** This chapter assumes that Fabric OS v6.4.1 is installed on the SAN multiprotocol routing products. For DCFM, the version is v10.4.2

9.1 Integrated Routing feature on 8 Gbps switches

Fabric OS v6.1 or later provides the Integrated Routing (IR) EX_Ports feature on the Condor2/GoldenEye2 ASICs. IR is a licensed feature that allows 8 Gbps ports to be configured as EX_Ports supporting FC routing. On the SAN18B-R routing blade, the IR license was not required for FCR because that functionality was directly associated with the hardware.

> **Note:** The newer 8 Gbps switches require the IR license per chassis to allow configuration of EX_Ports.

The IR license provides the following functionalities:

- Eliminates the need to add an FR4-18i blade to the SAN768B or SAN384B for FC-FC routing.
- Eliminates use of the SAN18B-R or any multi protocol router for FC_FC routing.
- Provides the same FCR functionality without having to buy the additional hardware for Fibre Channel Routing purposes.

Using 8 Gbps ports for FCR provides double the bandwidth for each FCR connection (when connected to another 8 Gbps-capable port).

> **Note:** Generally, Condor2/GoldenEye2 ASICs performance is better than SAN18B-R routing blade in terms of latency and full bandwidth support.
>
> Integrated Routing on 8 Gbps switches uses the same CLI commands as the SAN18B-R routing blade. There is no difference in protocol.

9.2 Edge fabrics connected to backbone fabric through FCR

In this scenario, we show how to connect two FC fabrics by using the FCR feature. The edge fabric contains a FC-attached server. To describe the FC-FC routing feature, we use only one server. The second backbone fabric has an FC-attached disk controller that provides our disk LUNs. We have also other switches connected to this backbone fabric, which are not considered in this topic.

The fabric that has the server connected is built using an IBM System Storage SAN32B-3. The fabric with the disk comprises of an IBM System Storage SAN384B switch. The connections are presented from a non-redundant disk controller configuration, and with two connections to the FC switch. Figure 9-1 shows the scenario we are using to describe the FC-FC routing service.

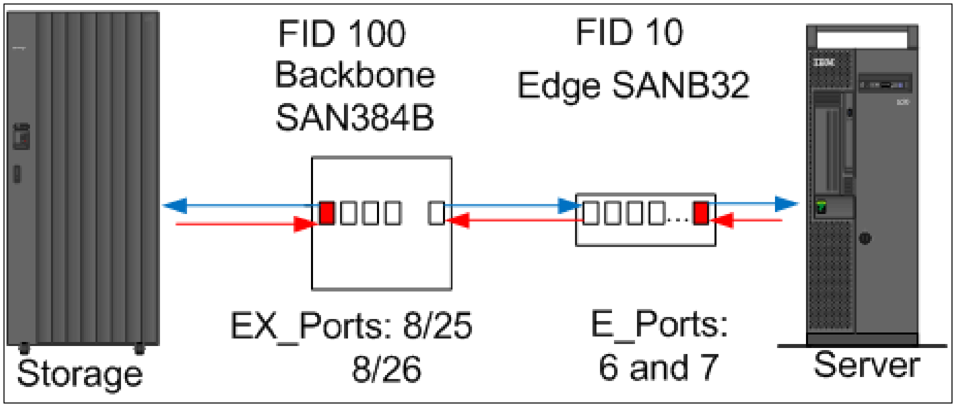


Figure 9-1 Scenario Backbone-Edge Connection using FC-FC routing

Terms used in Figure 9-1:

FID 100	FID of the backbone fabric
FID 10	FID of the EX_ports of the Backbone switch which are connected to Edge fabric
8/25, 8/26	Ex_Ports (trunk master is port 8/26)
6, 7	E_Ports (trunk master is port 6)
Server 1	Windows server (Dual HBA connected)
Storage	DS4000® (one controller connected; non-redundant configuration)

9.3 FC-FC routing service with CLI

In this topic, we use the command-language interface (CLI) to set up the FC-FC routing service.

9.3.1 Verifying the setup for FC-FC routing

To verify the setup for FC-FC routing, perform the following steps:

1. Verify that Fabric OS v6.1 or later is installed on the switch that will be the FC router (or on the FC router), as shown in Example 9-1.

Example 9-1 Verifying FOS version

```
IBM_SAN384B_27:admin> version
Kernel:     2.6.14.2
Fabric OS:  v6.4.1
Made on:    Thu Oct 7 00:20:49 2010
Flash:      Mon Oct 18 18:32:33 2010
BootProm:   1.0.15
IBM_SAN384B_27:admin>
```

We are configuring EX_Ports on an 8 Gbps port blade and we have to verify whether the FC8-16, FC8-32, or FC8-48 blade is present, in Example 9-2.

Example 9-2 Verifying if we have FC blades on SAN384B for FC-FC routing

```
IBM_SAN384B_27:admin> slotshow -m

Slot   Blade Type     ID    Model Name     Status
--------------------------------------------------
  1     AP BLADE     75     FX8-24         ENABLED
  2     UNKNOWN                            VACANT
  3     CORE BLADE   46     CR4S-8         ENABLED
  4     CP BLADE     50     CP8            ENABLED
  5     CP BLADE     50     CP8            ENABLED
  6     CORE BLADE   46     CR4S-8         ENABLED
  7     AP BLADE     43     FS8-18         ENABLED
  8     SW BLADE     55     FC8-32         ENABLED
```

2. If you are configuring EX_Ports on the 8 Gbps port blades on the SAN768B or the SAN384B (FC8-16, FC8-32, or FC8-48), enter the **licenseShow** command to verify that the Integrated Routing license is installed, as in Example 9-3.

Example 9-3 Licenseshow command

```
IBM_SAN384B_27:admin> licenseshow
bec9cb9bebefdAdv:
    Fabric Watch license
bec9cb9bebgfdAdx:
    Performance Monitor license
bec9cb9bebkfdAd1:
    Trunking license
bec9cb9bebcffAdv:
    Integrated Routing license
EYWQQtQMtKC4JAS39TSX43TmMra7BKJmBJgXF:
    Adaptive Networking license
YG93GSrWrmBW3ZC3XrCKD9Ja9JLRTYZtBAf4Q:
    Enhanced Group Management license
GrSQHNrDJBHfPBPBRTDY4YYmT3LZRFMJBANBC:
    Server Application Optimization license
IBM_SAN384B_27:admin>
```

3. The switch interoperability mode must be disabled. The **interopmode** command enables or disables IBM/Brocade switch interoperability with switches from other manufacturers. Show the switch interoperability mode with the command, shown in Example 9-4.

Example 9-4 interopmode command

```
IBM_SAN384B_27:admin> interopmode
InteropMode: Off

usage: InteropMode [0|2|3 [-z McDataDefaultZone] [-s McDataSafeZone]]
       0: to turn interopMode off
       2: to turn McDATA Fabric mode on
           Valid McDataDefaultZone: 0 (disabled), 1 (enabled)
           Valid McDataSafeZone: 0 (disabled), 1 (enabled)
       3: to turn McDATA Open Fabric mode on
IBM_SAN384B_27:admin>
```

4. Enter the **msplatshow** command to verify that Management Server Platform database is disabled in the backbone fabric. See Example 9-5.

Example 9-5 msplatshow command

```
IBM_SAN384B_27:admin> msplatshow
*MS Platform Management Service is NOT enabled.
```

5. The Management Server Platform must be disabled if in case it is noticed in the enabled state. Use the command **msplmgmtdeactivate** to deactivate Management Server, as in Example 9-6.

Example 9-6 msplmgmtdeactivate

```
IBM_SAN384B_27:admin> msplmgmtdeactivate

MS Platform Service is currently enabled.

This will erase MS Platform Service configuration
information as well as database in the entire fabric.

Would you like to continue this operation? (yes, y, no, n): [no] y

Request to deactivate MS Platform Service in progress......

*Completed deactivating MS Platform Service in the fabric!

IBM_SAN384B_27:admin>
```

6. Check the **msplatshow** command again to confirm the disabled state, as in Example 9-7.

Example 9-7 msplatshow

```
IBM_SAN384B_27:admin> msplatshow
*MS Platform Management Service is NOT enabled.
```

Note: The Management Server (MS) platform service must be deactivated on backbone fabric only.

7. Check that the edge fabric and the router fabric (backbone) are not configured in Access Control List (ACL) strict mode by performing the following steps:

   a. Check the edge fabric, as shown in Example 9-8.

Example 9-8 Checking ACL strict mode on the edge fabric

```
IBM_B32_23:admin> fddcfg --showall
Local Switch Configuration for all Databases:-
     DATABASE  -  Accept/Reject
---------------------------------
          SCC  -        accept
          DCC  -        accept
          PWD  -        accept
          FCS  -        accept
         AUTH  -        accept
     IPFILTER  -        accept

Fabric Wide Consistency Policy:- "SCC"

IBM_B32_23:admin>
```

   b. Check the backbone fabric, as shown in Example 9-9.

Example 9-9 Checking ACL strict mode on the backbone fabric

```
IBM_SAN384B_27:admin> fddcfg --showall
Local Switch Configuration for all Databases:-
     DATABASE  -  Accept/Reject
---------------------------------
          SCC  -        accept
          DCC  -        accept
          PWD  -        accept
          FCS  -        accept
         AUTH  -        accept
     IPFILTER  -        accept

Fabric Wide Consistency Policy:- ""

IBM_SAN384B_27:admin>
```

Note: If the Fabric Wide Consistency Policy contains the letter “S” on either the edge fabric or the backbone fabric, do not connect to the FC router. The letter “S” indicates that the policy is strict.

Tolerant policies display as follows:

- SCC
- DCC

Strict policies display as:

- SCC:S
- DCC:S

9.3.2 Configuring backbone fabric ID

All switches in a backbone fabric must have the same backbone fabric ID. Configure the backbone fabric ID using the **fcrConfigure** command as follows:

1. Disable the FC routing service with the **fosconfig** command.
2. Set the fabric ID with the **fcrconfigure** command. If virtual fabric mode is enabled it should be also disabled with **fosconfig** command. These steps are shown in Example 9-10

Example 9-10 fcrconfigure command

```
IBM_SAN384B_27:admin> fosconfig --show
FC Routing service:             enabled
iSCSI service:                  Service not supported on this Platform
iSNS client service:            Service not supported on this Platform
Virtual Fabric:                 disabled
Ethernet Switch Service:        disabled
IBM_SAN384B_27:admin> fosconfig --disable fcr
FC Routing service is disabled
IBM_SAN384B_27:admin> fosconfig --show
FC Routing service:             disabled
iSCSI service:                  Service not supported on this Platform
iSNS client service:            Service not supported on this Platform
Virtual Fabric:                 disabled
Ethernet Switch Service:        disabled
IBM_SAN384B_27:admin> fcrconfigure
FC Router parameter set. <cr> to skip a parameter
Please make sure new Backbone Fabric ID does not conflict with any
configured EX-Port's Fabric ID
Backbone fabric ID: (1-128)[128] 100
IBM_SAN384B_27:admin>
```

Note: If the backbone fabric ID is to be changed, the switch must be disabled first. Only then can the backbone fabric ID be changed.

3. Enable FC Routing Service in Fabric OS, as shown in Example 9-11.

Example 9-11 Enabling FC Routing Service

```
IBM_SAN384B_27:admin> fosconfig --enable fcr
FC Routing service is enabled
IBM_SAN384B_27:admin>
```

> **Remember:** Top Talker (TT) is not supported on VE_Ports, EX_Ports, and VEX_Ports. If TT is configured FCR cannot be enabled and vice-versa. TT can be disabled with the **`perfttmon --delete fabricmode`** command.

9.3.3 Configuring inter-fabric link (IFL)

Before configuring an inter-fabric link (IFL), be aware that you cannot configure both the following items from a backbone fabric to the same edge fabric:

- Both IFLs (EX_Ports, VEX_Ports)
- ISLs (E_Ports)

> **Note:** To configure an 8 Gbps IFL, both the EX_Port and the connecting E_Port must be 8-Gbps ports.
>
> To ensure that fabrics remain isolated, disable the port prior to inserting the cable. If you are configuring an EX_Port, disable the port prior to making the connection.

To configure an IFL, perform the following steps:

1. Disable the port on the backbone switch, as in Example 9-12.

Example 9-12 Disabling two ports

```
IBM_SAN384B_27:admin> portdisable 8/25
IBM_SAN384B_27:admin> portdisable 8/26
```

2. Configure an EX_Port with the **`portcfgexport`** command, as in Example 9-13.

Example 9-13 Configuring port 8/25 as an EX_Port

```
IBM_SAN384B_27:admin> portcfgexport 8/25 -a 1 -f 10
IBM_SAN384B_27:admin> portcfgexport 8/25
        Port   8/25   info
Admin:                  enabled
State:                  NOT OK
Pid format:             Not Applicable
Operate mode:           Brocade Native
```

```
Edge Fabric ID:         10
Preferred Domain ID:    160
Front WWN:              50:00:51:e9:43:a0:0e:0a
Fabric Parameters:      Auto Negotiate
R_A_TOV:                Not Applicable
E_D_TOV:                Not Applicable
Authentication Type: None
DH Group: N/A
Hash Algorithm: N/A
Edge fabric's primary wwn: N/A
Edge fabric's version stamp: N/A
```

In Example 9-14, we configure 8/29 as an EX_Port.

Example 9-14 Configuring 8/29 port as EX_Port

```
IBM_SAN384B_27:admin> portcfgexport 8/26 -a 1 -f 10
IBM_SAN384B_27:admin> portcfgexport 8/26
        Port   8/26   info
Admin:                  enabled
State:                  NOT OK
Pid format:             Not Applicable
Operate mode:           Brocade Native
Edge Fabric ID:         10
Preferred Domain ID:    160
Front WWN:              50:00:51:e9:43:a0:0e:0a
Fabric Parameters:      Auto Negotiate
R_A_TOV:                Not Applicable
E_D_TOV:                Not Applicable
Authentication Type: None
DH Group: N/A
Hash Algorithm: N/A
Edge fabric's primary wwn: N/A
Edge fabric's version stamp: N/A

IBM_SAN384B_27:admin>
```

The syntax of the important **portcfgexport** command is:

```
portcfgexport   [slotnumber/]portnumber
                [slotnumber/]portnumber
                [-a admin]
                [-f fabricid]
                [-r ratov]
                [-e edtov]
                [-d domainid]
                [-p pidformat]
                [-t fabric_parameter]
                [-m port mode]
                [-i mode]
```

The port must be disabled prior to setting EX_Port attributes. The port must be enabled before the port can become active following EX_Port parameter changes.

The important parameter is the fabric ID (FID). Note the following caveats:

- The FID must be the same for every router port connected to the same edge fabric, and different for every edge fabric.
- If two ports are connected to the same fabric but have been assigned different FIDs, one of them will be disabled because of a FID oversubscription.
- If two fabrics have been assigned the same FID, one of them will be disabled because of a FID conflict.

Note: FID is the number you must assign to the EX_Port. You do not have to set the FID on the edge switch.

3. Enable EX_Ports, as in Example 9-15.

Example 9-15 Enabling EX_Ports

```
IBM_SAN384B_27:admin> portenable 8/25
IBM_SAN384B_27:admin> portenable 8/26
IBM_SAN384B_27:admin> portshow 8/25
portIndex: 217
portName:
portHealth: HEALTHY

Authentication: None

EX_Port Mode:   Enabled
```

```
Fabric ID:      10
Front Phantom:  State: OK       Cur Dom ID: 160 WWN:
50:00:51:e9:43:a0:0e:0a
Pr Switch Info:         Dom ID: 1       WWN: 10:00:00:05:1e:34:02:4d
Fabric params:  R_A_TOV: 0      E_D_TOV: 0      PID fmt: auto
...............................
............Rest of output deleted for clarity
IBM_SAN384B_27:admin> portshow 8/26
portIndex: 218
portName:
portHealth: HEALTHY

Authentication: None

EX_Port Mode:   Enabled
Fabric ID:      10
Front Phantom:  State: OK       Cur Dom ID: 160 WWN:
50:00:51:e9:43:a0:0e:0a
Pr Switch Info:         Dom ID: 1       WWN: 10:00:00:05:1e:34:02:4d
Fabric params:  R_A_TOV: 10000  E_D_TOV: 2000   PID fmt: core
.........................................
.........Rest of output deleted for clarity
```

4. Verify Connectivity at the Edge fabric. Notice that only one front domain is displayed as `fcr_fd_160` in Example 9-16.

Example 9-16 Connectivity checked at the edge fabric

```
IBM_B32_23:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr
Name
-----------------------------------------------------------------------
--
  1: fffc01 10:00:00:05:1e:34:02:4d 10.18.228.23    0.0.0.0
>"IBM_B32_23"
160: fffca0 50:00:51:e9:43:a0:0e:0a 0.0.0.0         0.0.0.0
"fcr_fd_160"

The Fabric has 2 switches

IBM_B32_23:admin>
```

5. Use the **`switchshow`** and **`islshow`** command to verify E_Ports. Trunking is enabled by default in Example 9-17 on page 161.

Example 9-17 Verifying of the E_Port connection on edge switch.

```
IIBM_B32_23:admin> switchshow | grep E
  6   6   id    N4   Online          E-Port  50:00:51:e9:43:a0:0e:0a
"fcr_fd_160" (downstream)(Trunk master)
  7   7   id    N4   Online          E-Port  (Trunk port, master is
Port  6 )
```

In Example 9-18, we can see ISLs on the edge switch.

Example 9-18 islshow at the edge switch

```
IBM_B32_23:admin> islshow
  1:  6->218 50:00:51:e9:43:a0:0e:0a 160 fcr_fd_160      sp:  4.000G
bw:  8.000G TRUNK QOS
IBM_B32_23:admin>
```

A **switchshow** command at the backbone switch, which has ports connected to the edge switch as EX ports, will not be listed in the **islshow**. See Example 9-19 for how to display the EX port state.

Example 9-19 switchshow at the backbone

```
IBM_SAN384B_27:admin> switchshow | grep EX
217    8   25   10d900   id    N4   Online      FC  EX-Port  (Trunk port,
master is Slot  8 Port 26 )
218    8   26   10da00   id    N4   Online      FC  EX-Port
10:00:00:05:1e:34:02:4d "IBM_B32_23" (fabric id = 10 )(Trunk master)
```

EX_Port trunk appears as E_Port trunks in the edge fabric's **switchshow** output and **trunkshow** shows the trunk state of the IFL between the E and EX port as shown in Example 9-20.

Example 9-20 switchshow and trunkshow at the edge

```
IBM_B32_23:admin> switchshow | grep E
  6   6   id    N4   Online          E-Port  50:00:51:e9:43:a0:0e:0a
"fcr_fd_160" (downstream)(Trunk master)
  7   7   id    N4   Online          E-Port  (Trunk port, master is Port  6 )
IBM_B32_23:admin>

IBM_B32_23:admin> trunkshow
  1:  6->218 50:00:51:e9:43:a0:0e:0a 160 deskew 15 MASTER
      7->217 50:00:51:e9:43:a0:0e:0a 160 deskew 15
```

Example 9-21 on page 162 shows the **trunkshow** command at the backbone indicating the trunking of the EX ports as similar to the trunks of E_Ports of the backbone

Example 9-21 trunkshow

```
IBM_SAN384B_27:admin> trunkshow
  1:134-> 17 10:00:00:05:1e:54:16:53  56 deskew 15 MASTER

  2:135-> 16 10:00:00:05:1e:54:16:53  56 deskew 15 MASTER

  3:138-> 17 10:00:00:05:1e:54:17:10  54 deskew 15 MASTER

  4:139-> 16 10:00:00:05:1e:54:17:10  54 deskew 15 MASTER

  5:195-> 24 10:00:00:05:1e:90:16:e9  23 deskew 16 MASTER
    194-> 25 10:00:00:05:1e:90:16:e9  23 deskew 15

  6:197->  5 10:00:00:05:1e:c3:be:29   1 deskew 15 MASTER
    198->  6 10:00:00:05:1e:c3:be:29   1 deskew 15

  7:211-> 24 10:00:00:05:1e:90:16:57  98 deskew 15 MASTER
    210-> 25 10:00:00:05:1e:90:16:57  98 deskew 15

  8:218->  6 10:00:00:05:1e:34:02:4d   1 deskew 15 MASTER
    217->  7 10:00:00:05:1e:34:02:4d   1 deskew 15
```

9.3.4 Creating LSAN zones

LSAN creation commands are similar to the normal zone creation in a fabric. Note the following specific requirements for LSAN:

- LSAN zone must be defined and enabled in each fabric that will be sharing a particular device, in our case we need to create a separate LSAN zone in each switch (IBM_B32_23 and IBM_SAN384B_27) as shown in Example 9-22 on page 163.
- LSAN zone names do not have to match in the edge and backbone fabric.
- LSAN zone members must be identified by their PWWN.
- LSAN zones begin with the characters `LSAN_` (`LSAN_ZoneName`), `lsan_` (`lsan_ZoneName`), or `Lsan_` (`Lsan_ZoneName`)

> **Note:** Use the tool you normally use for creating zones (CLI, Web Tools, DCFM). When configuring LSAN zones with the DCFM LSAN zone creation wizard, LSAN zones are automatically created in both edge fabrics.

Creation of LSAN zone in Edge fabric

Example 9-22 shows the creation of a zone with CLI commands in the edge fabric switch IBM_B32_23 where we have the host initiator with WWPN 10:00:00:05:1e:0c:1c:cc connected. This initiator is zoned with targets connected to the backbone switch IBM_SAN384B_27 with its WWPN as 20:36:00:a0:b8:47:39:b0 and 20:37:00:a0:b8:47:39:b0. This target WWPN has to be identified from the other switch IBM_SAN384B_27.

Example 9-22 Creation of LSAN zone in Edge fabric switch

```
IBM_B32_23:admin> zonecreate "lsan_IBM_B32_23", "10:00:00:05:1e:0c:1c:cc;
20:36:00:a0:b8:47:39:b0; 20:37:00:a0:b8:47:39:b0"

IBM_B32_23:admin> cfgcreate "cfg_IBM_B32_23", "lsan_IBM_B32_23"

IBM_B32_23:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no, n): [no] y
Updating flash ...

IBM_B32_23:admin> cfgenable cfg_IBM_B32_23
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'cfg_IBM_B32_23' configuration  (yes, y, no, n): [no] y
zone config "cfg_IBM_B32_23" is in effect
Updating flash ...
IBM_B32_23:admin>
```

Example 9-23 shows visibility of the Initiator in the backbone fabric after LSAN zone creation in the edge fabric switch. Also, the **`lsanzoneshow -s`** command from the backbone fabric will show the LSAN created in the edge fabric. This confirms the edge switch LSAN zone creation is valid and identified as an LSAN zone by the backbone fabric.

Example 9-23 Backbone fabric device visibility check

```
IBM_SAN384B_27:admin> fcrphydevshow
 Device           WWN            Physical
 Exists                            PID
in Fabric
-----------------------------------------
   10    10:00:00:05:1e:0c:1c:cc  010400
Total devices displayed: 1

IBM_SAN384B_27:admin> lsanzoneshow -s
Fabric ID: 10 Zone Name: lsan_IBM_B32_23
        10:00:00:05:1e:0c:1c:cc  EXIST
        20:36:00:a0:b8:47:39:b0  Configured
        20:37:00:a0:b8:47:39:b0  Configured
IBM_SAN384B_27:admin>
```

Creation of LSAN zone in the backbone fabric

Example 9-24 shows the creation of a zone using CLI commands in the backbone fabric switch IBM_SAN384B_27 , where we have the targets with WWPN “20:36:00:a0:b8:47:39:b0 and 20:37:00:a0:b8:47:39:b0” connected. These targets are zoned with the host initiator with WWPN “10:00:00:05:1e:0c:1c:cc” that are connected to edge fabric Switch IBM_B32_23.

Example 9-24 Creation of LSAN zone at the backbone fabric

```
IIBM_SAN384B_27:admin> zonecreate "lsan_IBM_SAN384B"
"10:00:00:05:1e:0c:1c:cc; 20:36:00:a0:b8:47:39:b0;
20:37:00:a0:b8:47:39:b0"
error: Usage: zonecreate "lsan_IBM_SAN384B", "10:00:00:05:1e:0c:1c:cc;
20:36:00:a0:b8:47:39:b0; 20:37:00:a0:b8:47:39:b0"
IBM_SAN384B_27:admin> zonecreate "lsan_IBM_SAN384B",
"10:00:00:05:1e:0c:1c:cc; 20:36:00:a0:b8:47:39:b0;
20:37:00:a0:b8:47:39:b0"

IBM_SAN384B_27:admin> cfgadd "IBM_RB", "lsan_IBM_SAN384B"

IBM_SAN384B_27:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no,
n): [no] y
Updating flash ...

IBM_SAN384B_27:admin> cfgenable IBM_RB
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'IBM_RB' configuration  (yes, y, no, n): [no] y
zone config "IBM_RB" is in effect
Updating flash ...
IBM_SAN384B_27:admin>
```

Verifying final device routing

Example 9-25 shows the device status verification at the backbone fabric with the **lsanzoneshow -s** and **fcrphydevshow** commands. The output of **lsanzoneshow -s** indicates that the LSAN zone creation in the backbone fabric is also valid and identified as an LSAN. Also from the **lsanzoneshow** output, we can see which device exists in the fabric and which one is imported. Notice the fabric Id (FID) for the edge and the backbone. We can see that the FCR device list in the **fcrphydevshow** output has all the devices defined in the LSAN_Zones of both edge and backbone fabric.

Example 9-25 Displaying LSAN zone at the backbone

```
IIBM_SAN384B_27:admin> lsanzoneshow -s
Fabric ID: 10 Zone Name: lsan_IBM_B32_23
        10:00:00:05:1e:0c:1c:cc  EXIST
        20:36:00:a0:b8:47:39:b0  Imported
        20:37:00:a0:b8:47:39:b0  Imported
Fabric ID: 100 Zone Name: lsan_IBM_SAN384B
        10:00:00:05:1e:0c:1c:cc  Imported
        20:36:00:a0:b8:47:39:b0  EXIST
        20:37:00:a0:b8:47:39:b0  EXIST

IBM_SAN384B_27:admin> fcrphydevshow
 Device          WWN            Physical
 Exists                           PID
in Fabric
-----------------------------------------
   10    10:00:00:05:1e:0c:1c:cc  010400
  100    20:36:00:a0:b8:47:39:b0  10dc00
  100    20:37:00:a0:b8:47:39:b0  10c800
Total devices displayed: 3
IBM_SAN384B_27:admin>
```

Verifying the translate domain

The translate domain should appear in the **`fabricshow`** command output as in Example 9-26.

Example 9-26   fabricshow at the backbone

```
IBM_SAN384B_27:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr
Name
-----------------------------------------------------------------------
--
  1: fffc01 10:00:00:05:1e:c3:be:29 10.18.228.31    0.0.0.0
"IBM_2498_R06"
  2: fffc02 50:00:51:e9:43:ae:0f:18 0.0.0.0         0.0.0.0
"fcr_xd_2_10"
  5: fffc05 10:00:00:05:1e:b0:81:80 10.18.228.18    0.0.0.0
"switch"
 16: fffc10 10:00:00:05:1e:94:3a:00 10.18.228.27    0.0.0.0
"IBM_SAN384B_27"
 23: fffc17 10:00:00:05:1e:90:16:e9 10.18.229.77    0.0.0.0
"B5000_75"
 54: fffc36 10:00:00:05:1e:54:17:10 10.18.235.54    0.0.0.0
"SAN32B-E4-1"
 56: fffc38 10:00:00:05:1e:54:16:53 10.18.235.56    0.0.0.0
>"SAN32B-E4-2"
 98: fffc62 10:00:00:05:1e:90:16:57 10.18.229.78    0.0.0.0
"B5000_76"

The Fabric has 8 switches

IBM_SAN384B_27:admin>
```

Verifying translate domain at the edge

Verify the translate domain at the edge, as in Example 9-27.

Example 9-27 fabricshow at the edge

```
IBM_B32_23:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr
Name
-----------------------------------------------------------------------
--
  1: fffc01 10:00:00:05:1e:34:02:4d 10.18.228.23    0.0.0.0
>"IBM_B32_23"
  2: fffc02 50:00:51:e9:43:ae:0f:17 0.0.0.0         0.0.0.0
"fcr_xd_2_100"
160: fffca0 50:00:51:e9:43:a0:0e:0a 0.0.0.0         0.0.0.0
"fcr_fd_160"

The Fabric has 3 switches

IBM_B32_23:admin>
```

Verifying translate domain connectivity

Verify translate domain connectivity at the backbone by using the **switchshow** command, shown in Example 9-28.

Example 9-28 Switchshow command - connectivity at the backbone

```
IBM_SAN384B_27:admin> switchshow | more
switchName:     IBM_SAN384B_27
switchType:     77.3
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   16
switchId:       fffc10
switchWwn:      10:00:00:05:1e:94:3a:00
zoning:         ON (IBM_RB)
switchBeacon:   OFF
FC Router:      ON
FC Router BB Fabric ID: 100
Address Mode:   0

Index Slot Port Address Media Speed State     Proto
===================================================

truncated output

217    8   25   10d900   id    N4   Online      FC  EX-Port  (Trunk
port, master is Slot  8 Port 26 )
218    8   26   10da00   id    N4   Online      FC  EX-Port
10:00:00:05:1e:34:02:4d "IBM_B32_23" (fabric id = 10 )(Trunk master)
                                     E-Port   50:00:51:e9:43:ae:0f:18
"fcr_xd_2_10"


truncated output
```

Displaying the backbone

Display the backbone with **fcrfabricshow** command, as in Example 9-29.

Example 9-29 Displaying backbone with fabricshow

```
IBM_SAN384B_27:admin> fcrfabricshow
FC Router WWN: 10:00:00:05:1e:94:3a:00, Dom ID:  16,
Info: 10.18.228.27, "IBM_SAN384B_27"
   EX_Port       FID    Neighbor Switch Info (enet IP, WWN, name)

-----------------------------------------------------------------------
-
     218         10     10.18.228.23     10:00:00:05:1e:34:02:4d
"IBM_B32_23"

IBM_SAN384B_27:admin>
```

Verifying proxy devices

Verify proxy devices as in Example 9-30. This provides the list of imported devices

Example 9-30 Proxy Devices

```
IBM_SAN384B_27:admin> fcrproxydevshow
  Proxy           WWN             Proxy      Device   Physical    State
 Created                           PID       Exists     PID
in Fabric                                  in Fabric
-----------------------------------------------------------------------
-----
    10   20:36:00:a0:b8:47:39:b0  02f101      100      10dc00
Imported
    10   20:37:00:a0:b8:47:39:b0  02f201      100      10c800
Imported
   100   10:00:00:05:1e:0c:1c:cc  02f201       10      010400
Imported
Total devices displayed: 3
```

9.4 Quality of Service (QOS) over FC-FC routing

QOS is an adaptive networking feature introduced in FOS 6.0 to provide prioritized service levels for selective critical application traffic. From FOS 6.30 and later versions, QOS is supported for fabrics that use FC-FC routing.

9.4.1 Requirements for QOS over FCR

The following list details requirements for QOS over FCR:

- QOS requires the adaptive networking license on all switches in the path configured for QOS including edge and backbone fabrics.
- QOS over FC routers is supported in Brocade native mode only.
- QOS over FC routers is supported only in an edge-to-edge fabric configuration, it is not supported in a backbone-to-edge fabric configuration.
- QoS over FC routers is supported only if virtual fabrics is disabled in the backbone fabric.
- Both the QOS zone and LSAN zone must have the port WWN of the host or target in the fabric or the proxy device.
- QOS over FC routers is supported on both EX_Ports and VEX_Ports (FCIP), however the 4 Gbps routing blade FC3850 / 3450 is not supported with QOS.
- All switches between QOS devices must be running FOS6.3.0 or later.
- Similar to LSAN zones, QOS zones also use WWPN notations only.

9.4.2 Steps to establish QOS over FCR

The flow of steps required to establish QOS over FCR is as follows:

1. Define QoS zones in each edge fabric.
2. Define LSAN zones in each edge fabric.
3. Enable QoS on the E_Ports in each edge fabric.
4. Enable QoS on the EX_Ports (or VEX_Ports) in the backbone fabric.

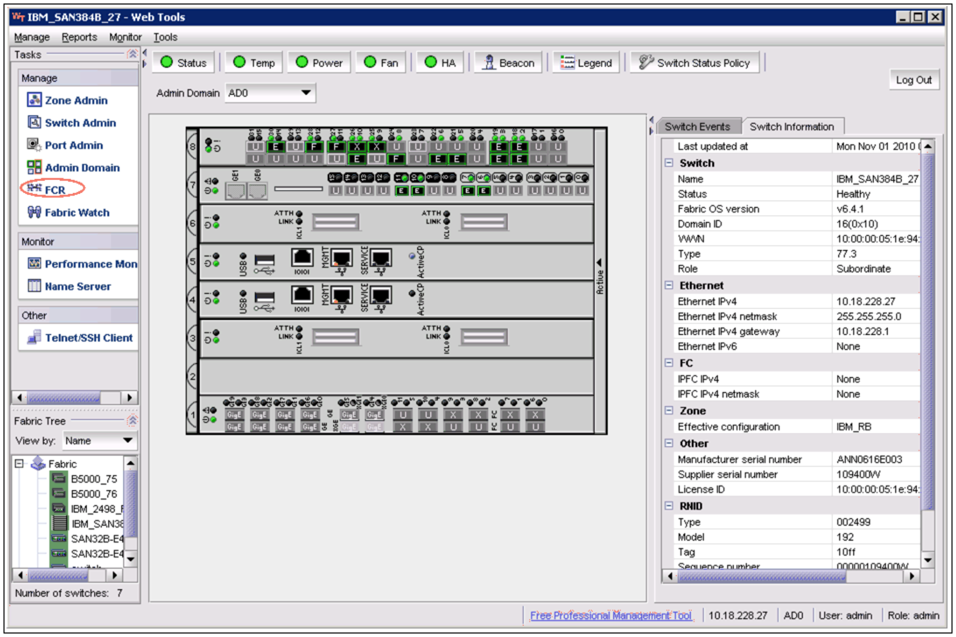
For more details on QOS and configuration steps refer to *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116

9.5 FC-FC routing service with Web Tools

This section explains how to set up the FC-FC routing service by using Web Tools. Before you proceed, check all the requirements as described in 9.3.1, “Verifying the setup for FC-FC routing” on page 152. In our case we had already configured the FCR, hence we are just indicating the way to configure with web tools in the following sections.

9.5.1 Configuring backbone fabric ID

You can find the application named FCR in the main window of Web Tools, shown in Figure 9-2.



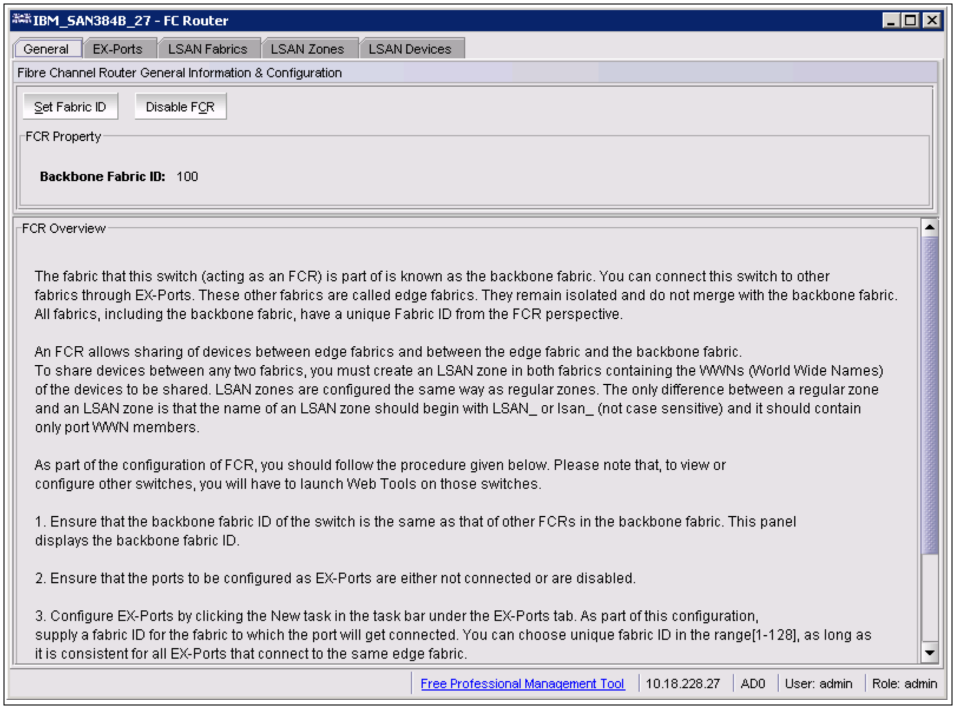
Last updated at	Mon Nov 01 2010 (
Switch	
Name	IBM_SAN384B_27
Status	Healthy
Fabric OS version	v6.4.1
Domain ID	16(0x10)
WWN	10:00:00:05:1e:94:
Type	77.3
Role	Subordinate
Ethernet	
Ethernet IPv4	10.18.228.27
Ethernet IPv4 netmask	255.255.255.0
Ethernet IPv4 gateway	10.18.228.1
Ethernet IPv6	None
FC	
IPFC IPv4	None
IPFC IPv4 netmask	None
Zone	
Effective configuration	IBM_RB
Other	
Manufacturer serial number	ANN0616E003
Supplier serial number	109400W
License ID	10:00:00:05:1e:94:
RNID	
Type	002499
Model	192
Tag	10ff
Sequence number	00000109400W

Figure 9-2 FCR in Web Tools

To configure the backbone fabric ID, follow these steps:

1. Click **FCR**.

   The window shown in Figure 9-3 on page 173 opens. Disable FCR (if it is enabled). This must be done when starting configuring FCR.



Backbone Fabric ID: 100

The fabric that this switch (acting as an FCR) is part of is known as the backbone fabric. You can connect this switch to other fabrics through EX-Ports. These other fabrics are called edge fabrics. They remain isolated and do not merge with the backbone fabric. All fabrics, including the backbone fabric, have a unique Fabric ID from the FCR perspective.

An FCR allows sharing of devices between edge fabrics and between the edge fabric and the backbone fabric. To share devices between any two fabrics, you must create an LSAN zone in both fabrics containing the WWNs (World Wide Names) of the devices to be shared. LSAN zones are configured the same way as regular zones. The only difference between a regular zone and an LSAN zone is that the name of an LSAN zone should begin with LSAN_ or lsan_ (not case sensitive) and it should contain only port WWN members.

As part of the configuration of FCR, you should follow the procedure given below. Please note that, to view or configure other switches, you will have to launch Web Tools on those switches.

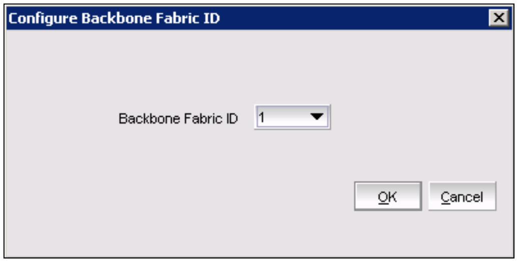
1. Ensure that the backbone fabric ID of the switch is the same as that of other FCRs in the backbone fabric. This panel displays the backbone fabric ID.

2. Ensure that the ports to be configured as EX-Ports are either not connected or are disabled.

3. Configure EX-Ports by clicking the New task in the task bar under the EX-Ports tab. As part of this configuration, supply a fabric ID for the fabric to which the port will get connected. You can choose unique fabric ID in the range[1-128], as long as it is consistent for all EX-Ports that connect to the same edge fabric.

Figure 9-3 FCR window in Web Tools

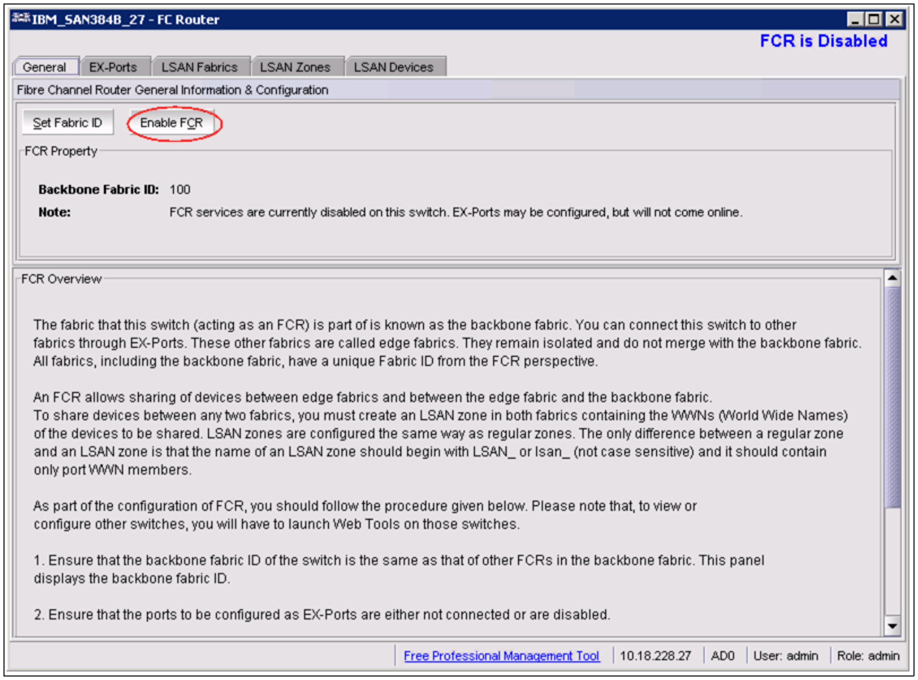
2. Click **Set Fabric ID** to open the window shown in Figure 9-4. Select the Fabric ID for the backbone fabric and click **OK**.



Backbone Fabric ID: 1

Figure 9-4 Setting Backbone Fabric ID

3. Enable FCR by clicking **Enable FCR**, as shown in Figure 9-5.



Backbone Fabric ID: 100

Note: FCR services are currently disabled on this switch. EX-Ports may be configured, but will not come online.

The fabric that this switch (acting as an FCR) is part of is known as the backbone fabric. You can connect this switch to other fabrics through EX-Ports. These other fabrics are called edge fabrics. They remain isolated and do not merge with the backbone fabric. All fabrics, including the backbone fabric, have a unique Fabric ID from the FCR perspective.

An FCR allows sharing of devices between edge fabrics and between the edge fabric and the backbone fabric. To share devices between any two fabrics, you must create an LSAN zone in both fabrics containing the WWNs (World Wide Names) of the devices to be shared. LSAN zones are configured the same way as regular zones. The only difference between a regular zone and an LSAN zone is that the name of an LSAN zone should begin with LSAN_ or lsan_ (not case sensitive) and it should contain only port WWN members.

As part of the configuration of FCR, you should follow the procedure given below. Please note that, to view or configure other switches, you will have to launch Web Tools on those switches.

1. Ensure that the backbone fabric ID of the switch is the same as that of other FCRs in the backbone fabric. This panel displays the backbone fabric ID.

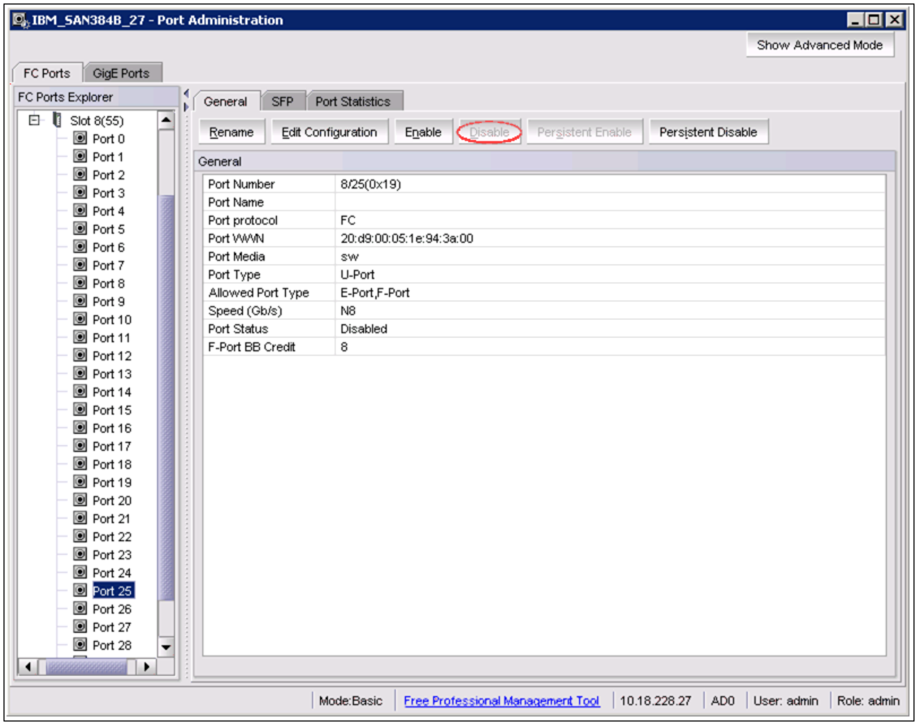
2. Ensure that the ports to be configured as EX-Ports are either not connected or are disabled.

Figure 9-5 Enabling FCR

9.5.2 Configuring inter-fabric link

To configure inter-fabric link, follow these steps:

1. Disable the port on the backbone switch, as shown in Figure 9-6. In our scenario, we also disabled also port 8/26.



General

Port Number	8/25(0x19)
Port Name	
Port protocol	FC
Port WWN	20:d9:00:05:1e:94:3a:00
Port Media	sw
Port Type	U-Port
Allowed Port Type	E-Port,F-Port
Speed (Gb/s)	N8
Port Status	Disabled
F-Port BB Credit	8

Figure 9-6 Disabling port 8/25 in the backbone

2. Configure EX_Ports by selecting the EX_Ports tab in the FCR administration panel, shown in Figure 9-7. Note that slot 8 does not have an EX_Port now.

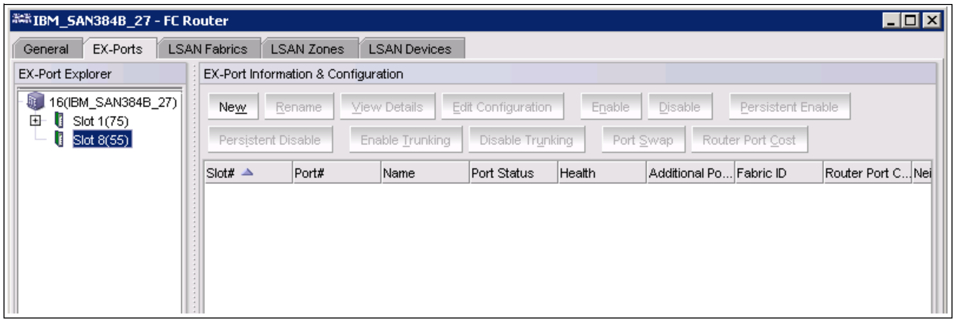


Figure 9-7 EX_Ports panel

To define the EX_Port, we click **New**, which opens the EX_Port configuration wizard, shown in Figure 9-8.

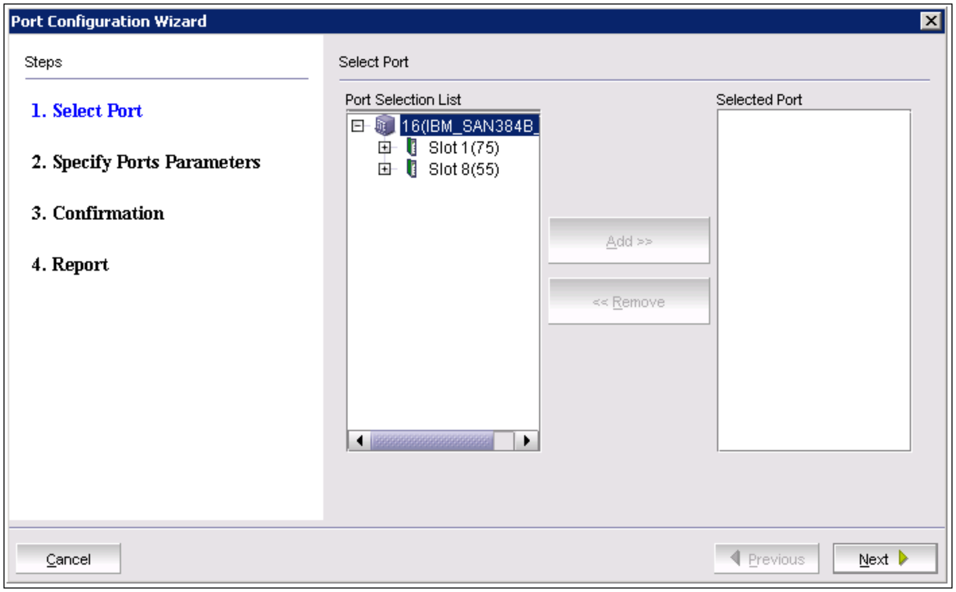


Figure 9-8 Port Configuration Wizard

3. Select the slot/port that we want to configure. Figure 9-9 shows that we selected port 8/25 from the Port Selection List in the center of the panel. Click **Add** to put the port in the Selected Port list. Click **Next**.

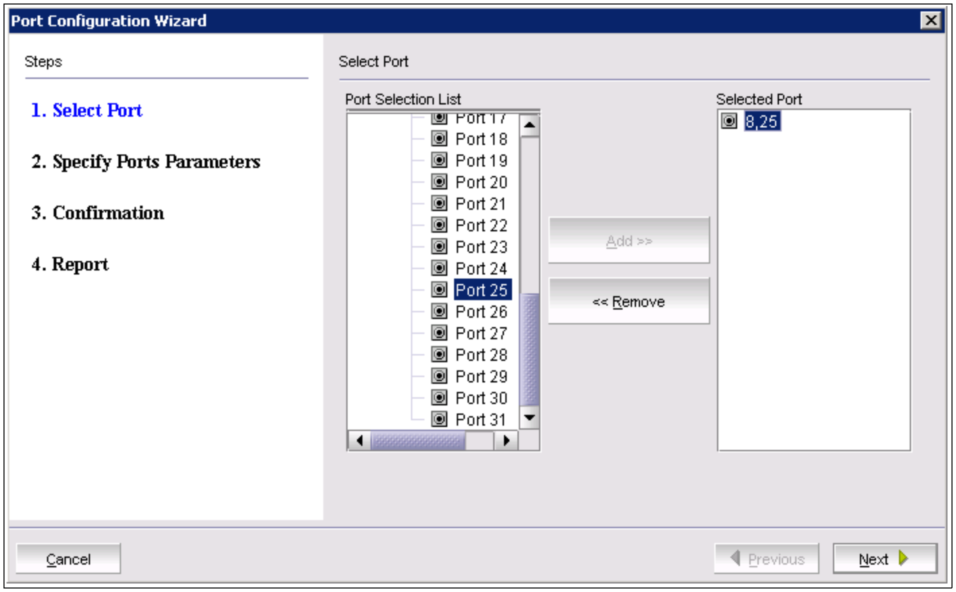
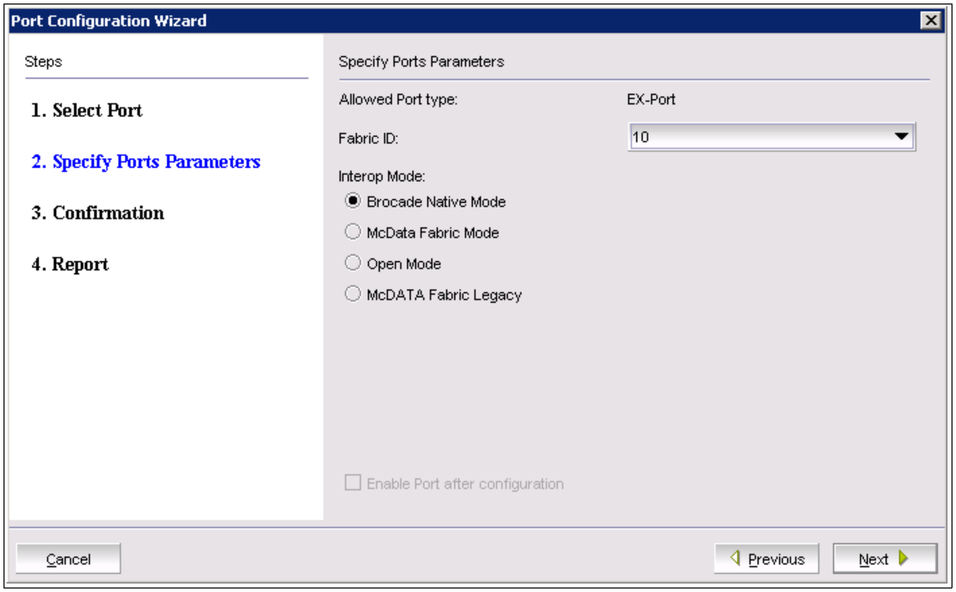


Figure 9-9 Selecting port 8/25 for EX_Port

4. The next window opens, as shown in Figure 9-10. Set the Fabric ID (FID) to **10** and the interop Mode to **Brocade Native Mode**. Click **Next**.



Port Configuration Wizard

Specify Ports Parameters

Allowed Port type: EX-Port

Fabric ID: 10

Interop Mode:

● Brocade Native Mode

○ McData Fabric Mode

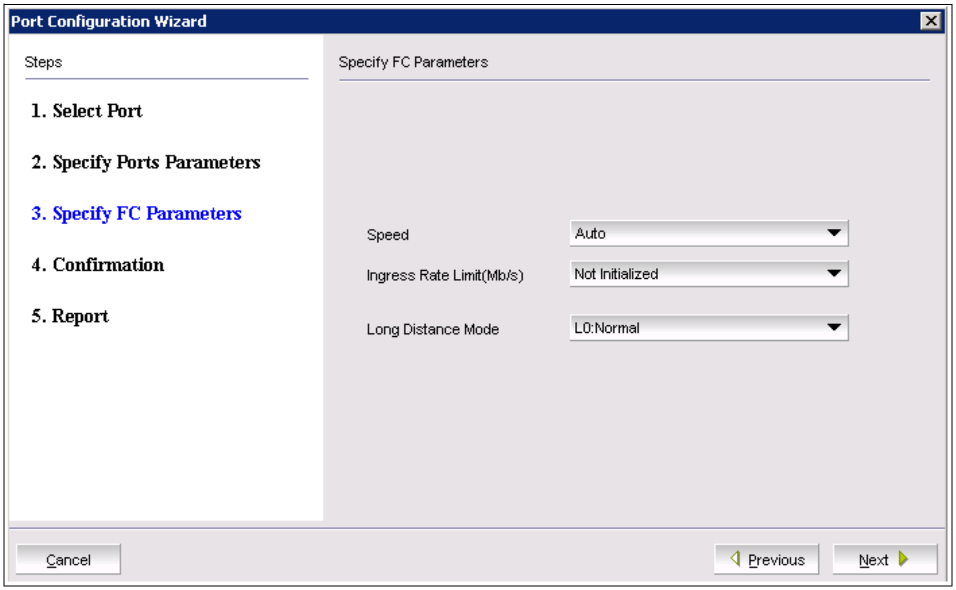
○ Open Mode

○ McDATA Fabric Legacy

□ Enable Port after configuration

Figure 9-10 Selecting FID for the port and Interop Mode

5. As Figure 9-11 shows, the FC parameter’s speed and long distance mode are defined. We chose **Auto** for speed and **L0** as the distance mode because all devices in our setup are closely located. Click **Next**.



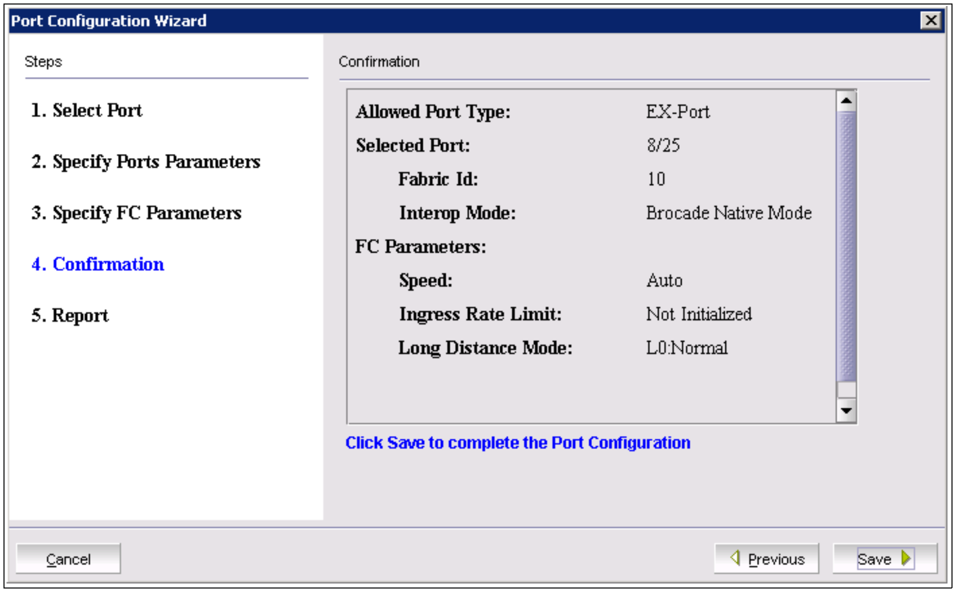
Speed: Auto

Ingress Rate Limit(Mb/s): Not Initialized

Long Distance Mode: L0:Normal

Figure 9-11 FC Parameters dialog box for EX_Ports

6. The final window of the wizard displays a summary, as shown in Figure 9-12. Click **Save** and **Close** to apply the configuration.



Allowed Port Type: EX-Port
Selected Port: 8/25
Fabric Id: 10
Interop Mode: Brocade Native Mode
FC Parameters:
Speed: Auto
Ingress Rate Limit: Not Initialized
Long Distance Mode: L0:Normal

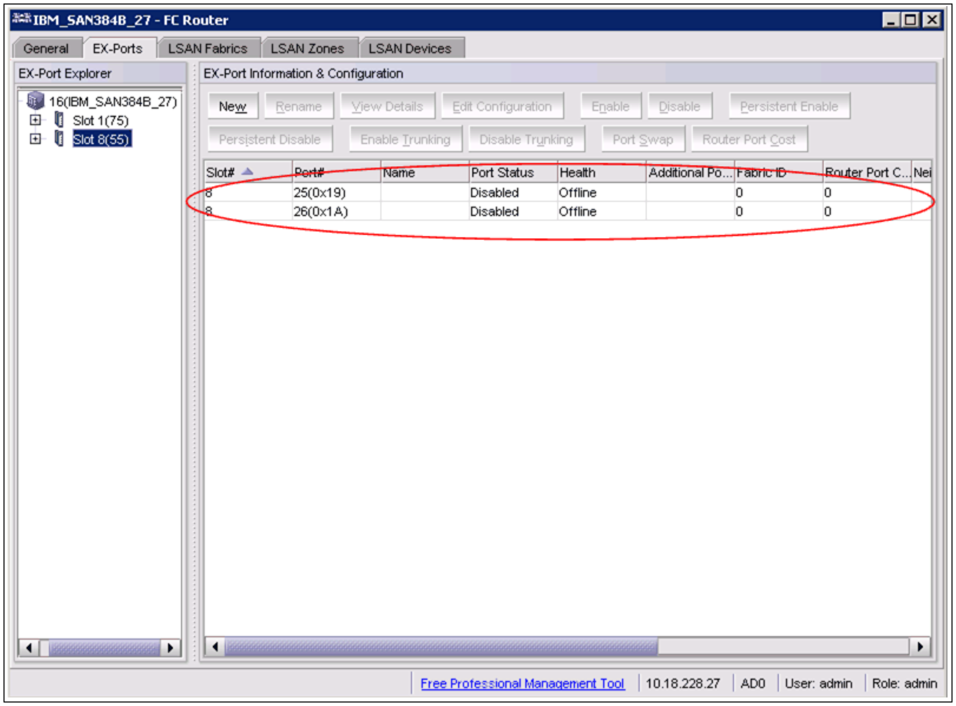
Click Save to complete the Port Configuration

Figure 9-12 Saving Configuration

7. Repeat step 6 to configure the EX_Ports for port 8/26.

Note: Both ports will connect to the edge fabric which is FID=10.

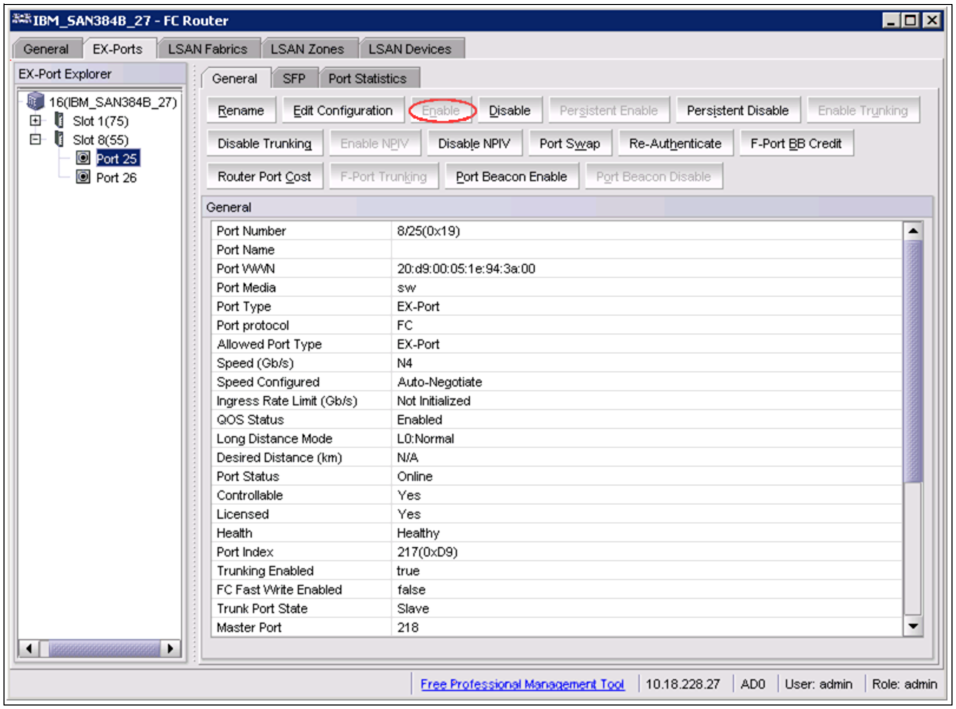
After configuring all EX_Ports, the window shown in Figure 9-13 opens.



Slot#	Port#	Name	Port Status	Health	Additional Po...	Fabric ID	Router Port C...	Nei
8	25(0x19)		Disabled	Offline		0	0	
8	26(0x1A)		Disabled	Offline		0	0	

Figure 9-13 Ports 8/28, 8/29 are shown as EX_Ports

8. Enable the ports. Click the port number in the list and click **Enable** or **Persistent Enable** in the “EX-Port Information and Configuration” panel. Clicking **Enable** causes the EX_Port to enter the enabled state and disables the enablement boxes. See Figure 9-14.

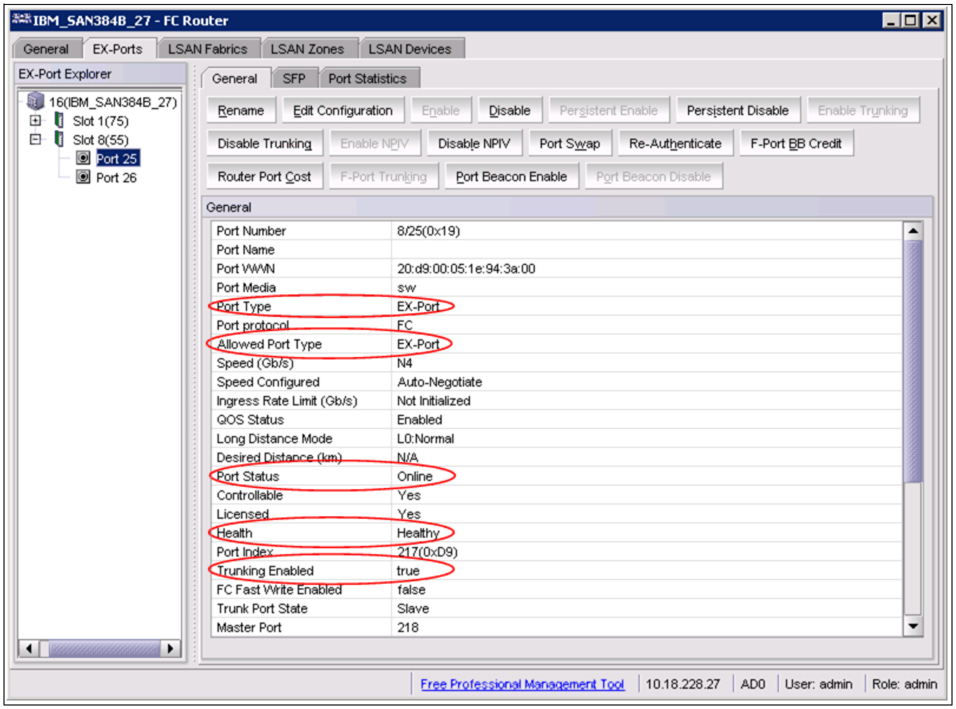


Port Number	8/25(0x19)
Port Name	
Port WWN	20:d9:00:05:1e:94:3a:00
Port Media	sw
Port Type	EX-Port
Port protocol	FC
Allowed Port Type	EX-Port
Speed (Gb/s)	N4
Speed Configured	Auto-Negotiate
Ingress Rate Limit (Gb/s)	Not Initialized
QOS Status	Enabled
Long Distance Mode	L0:Normal
Desired Distance (km)	N/A
Port Status	Online
Controllable	Yes
Licensed	Yes
Health	Healthy
Port Index	217(0xD9)
Trunking Enabled	true
FC Fast Write Enabled	false
Trunk Port State	Slave
Master Port	218

Figure 9-14 Enabling EX_Port

9. Repeat step 8 for port 8/26.

10. Verify the Port status at the backbone. Check the fields connected to all your EX_Ports, which are circled in Figure 9-15.



Port Number	8/25(0x19)
Port Name	
Port WWN	20:d9:00:05:1e:94:3a:00
Port Media	sw
Port Type	EX-Port
Port protocol	FC
Allowed Port Type	EX-Port
Speed (Gb/s)	N4
Speed Configured	Auto-Negotiate
Ingress Rate Limit (Gb/s)	Not Initialized
QOS Status	Enabled
Long Distance Mode	L0:Normal
Desired Distance (km)	N/A
Port Status	Online
Controllable	Yes
Licensed	Yes
Health	Healthy
Port Index	217(0xD9)
Trunking Enabled	true
FC Fast Write Enabled	false
Trunk Port State	Slave
Master Port	218

Figure 9-15 Checking EX_Port status

9.5.3 Creating LSAN zones

To create the LSAN zones, follow these steps:

1. Create the LSAN zones. The LSAN zone must be defined and enabled in each fabric that will be sharing a particular device.

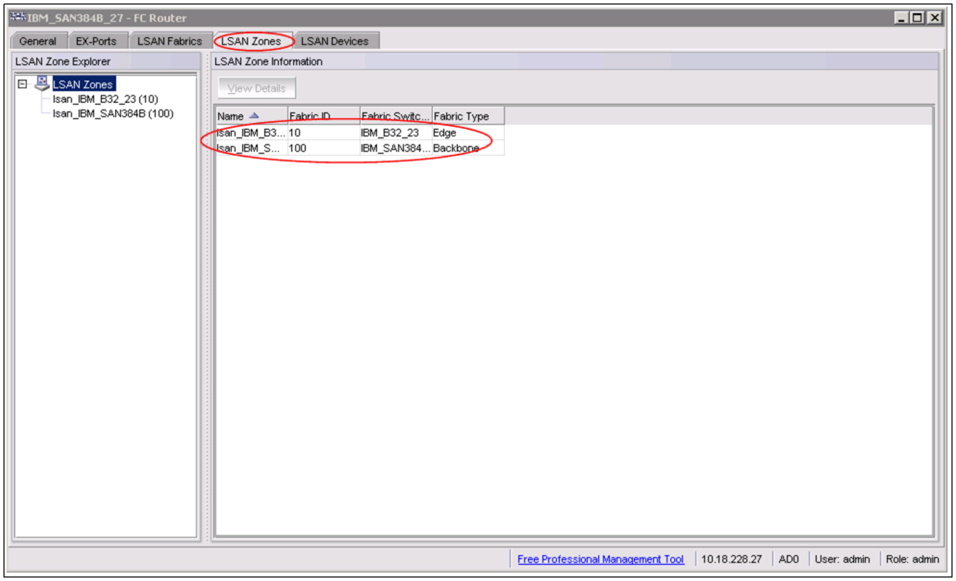
> **Note:** Create the LSAN zone with the prefix LSAN, using the tool you normally use for creating zones (CLI, Web Tools, DCFM).
>
> LSAN zone members must be identified by their PWWN.

We created one LSAN zone on each fabric:

- Backbone
- Edge

For LSAN zone creation examples, refer to 9.3.4, “Creating LSAN zones” on page 162.

Verify the LSAN zones on the tab LSAN_Zones as shown in Figure 9-16. In Figure 9-16, two LSAN_zones are shown: one defined in the Backbone (SAN384B) and one defined in the Edge (SAN32B-2).

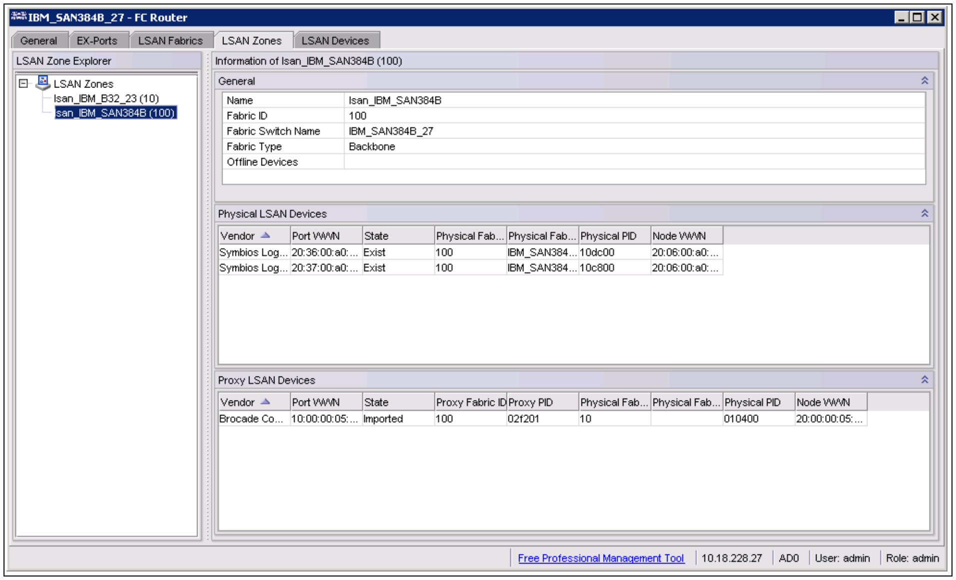


LSAN Zones
- lsan_IBM_B32_23 (10)
- lsan_IBM_SAN384B (100)

Name	Fabric ID	Fabric Switc...	Fabric Type
lsan_IBM_B3...	10	IBM_B32_23	Edge
lsan_IBM_S...	100	IBM_SAN384...	Backbone

Figure 9-16 LSAN zones at the edge and backbone

2. Verify LSAN Fabric at the backbone. Select the LSAN Fabric tab, as shown in Figure 9-17, and select the backbone fabric.



Information of lsan_IBM_SAN384B (100)

General

Name	lsan_IBM_SAN384B
Fabric ID	100
Fabric Switch Name	IBM_SAN384B_27
Fabric Type	Backbone
Offline Devices	

Physical LSAN Devices

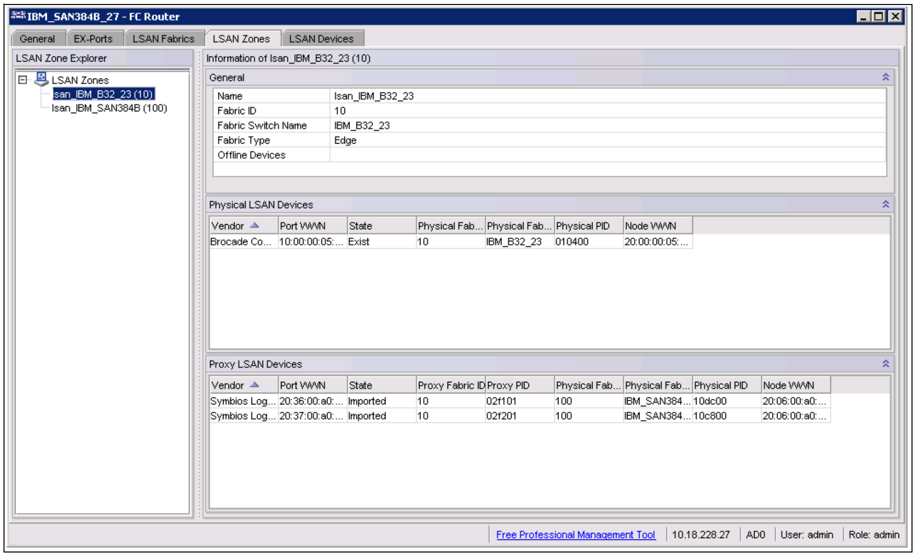
Vendor ▲	Port WWN	State	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Symbios Log...	20:36:00:a0:...	Exist	100	IBM_SAN384...	10dc00	20:06:00:a0:...
Symbios Log...	20:37:00:a0:...	Exist	100	IBM_SAN384...	10c800	20:06:00:a0:...

Proxy LSAN Devices

Vendor ▲	Port WWN	State	Proxy Fabric ID	Proxy PID	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Brocade Co...	10:00:00:05:...	Imported	100	02f201	10		010400	20:00:00:05:...

Figure 9-17 LSAN Fabric at the backbone

3. Verify the LSAN Fabric at the edge. See Figure 9-18.



Information of lsan_IBM_B32_23 (10)

General

Name	lsan_IBM_B32_23
Fabric ID	10
Fabric Switch Name	IBM_B32_23
Fabric Type	Edge
Offline Devices	

Physical LSAN Devices

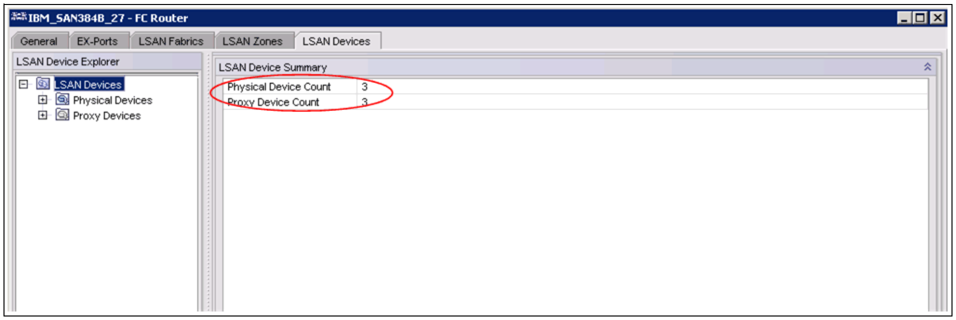
Vendor ▲	Port WWN	State	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Brocade Co...	10:00:00:05:...	Exist	10	IBM_B32_23	010400	20:00:00:05:...

Proxy LSAN Devices

Vendor ▲	Port WWN	State	Proxy Fabric ID	Proxy PID	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Symbios Log...	20:36:00:a0:...	Imported	10	02f101	100	IBM_SAN384...	10dc00	20:06:00:a0:...
Symbios Log...	20:37:00:a0:...	Imported	10	02f201	100	IBM_SAN384...	10c800	20:06:00:a0:...

Figure 9-18 LSAN Fabric at the edge

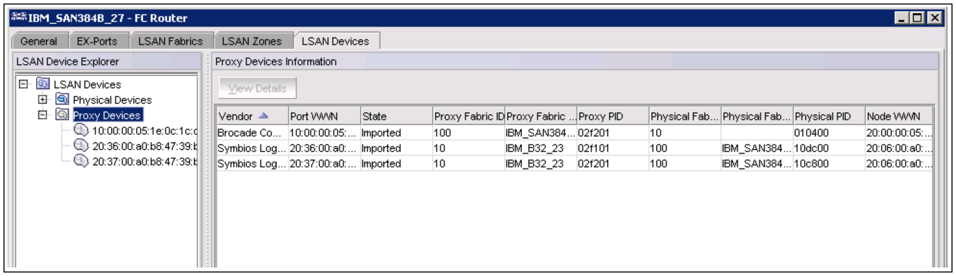
4. Determine the connected devices. Determine which device exists in the fabric and which device is imported. Notice the fabric ID (FID) for edge and the backbone. See Figure 9-19.



Physical Device Count	3
Proxy Device Count	3

Figure 9-19 LSAN Devices

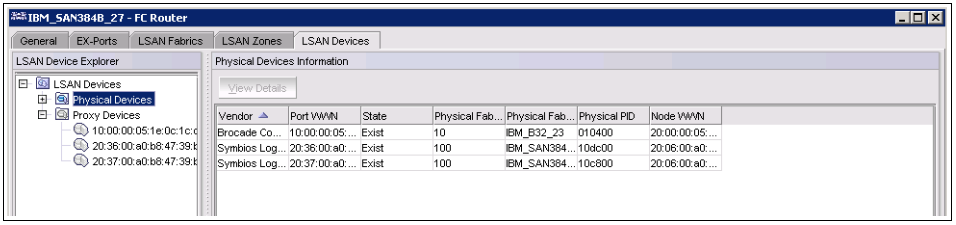
The proxy devices are shown in Figure 9-20.



Vendor	Port WWN	State	Proxy Fabric ID	Proxy Fabric ...	Proxy PID	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Brocade Co...	10:00:00:05:...	Imported	100	IBM_SAN384...	02f201	10		010400	20:00:00:05:...
Symbios Log...	20:36:00:a0:...	Imported	10	IBM_B32_23	02f101	100	IBM_SAN384...	10dc00	20:06:00:a0:...
Symbios Log...	20:37:00:a0:...	Imported	10	IBM_B32_23	02f201	100	IBM_SAN384...	10c800	20:06:00:a0:...

Figure 9-20 Proxy devices

The physical devices are shown in Figure 9-21.



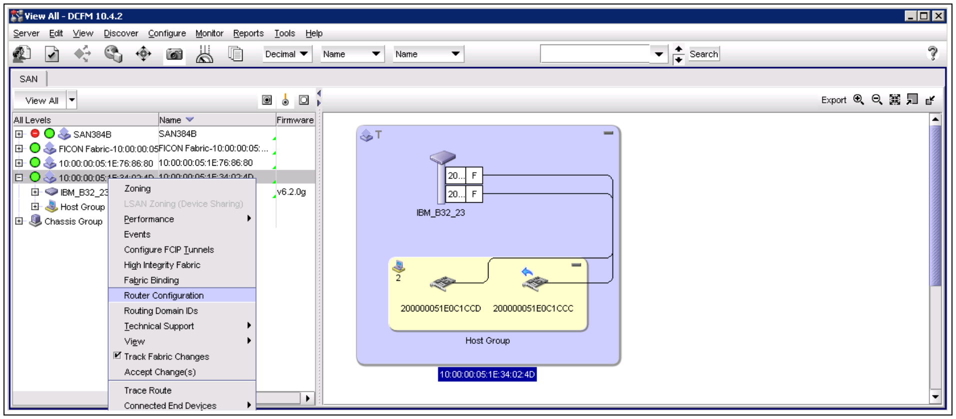
Vendor	Port WWN	State	Physical Fab...	Physical Fab...	Physical PID	Node WWN
Brocade Co...	10:00:00:05:...	Exist	10	IBM_B32_23	010400	20:00:00:05:...
Symbios Log...	20:36:00:a0:...	Exist	100	IBM_SAN384...	10dc00	20:06:00:a0:...
Symbios Log...	20:37:00:a0:...	Exist	100	IBM_SAN384...	10c800	20:06:00:a0:...

Figure 9-21 Physical devices

9.6 FC-FC routing service with DCFM

To set up the routing service with DCFM, follow these steps:

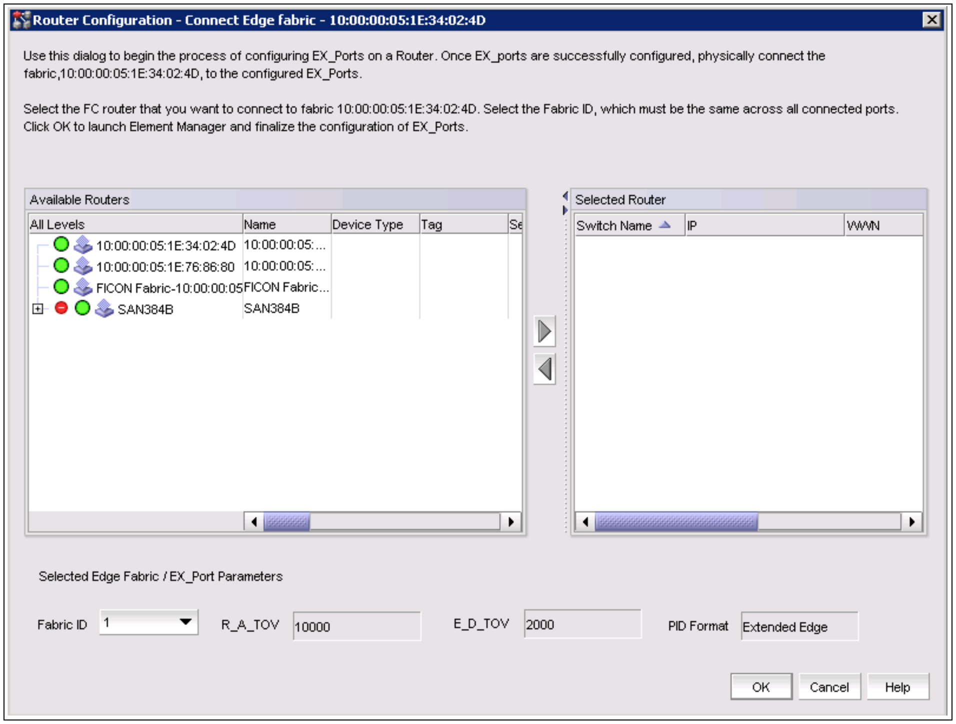
1. Select the edge switch to be connected to the router, then right click **Configure** →**Routing** → **Configuration**, or right-click the edge fabric in the connectivity map or the Product List, shown in Figure 9-22.



All Levels	Name	Firmware
SAN384B	SAN384B	
FICON Fabric-10:00:00:05	FICON Fabric-10:00:00:05:...	
10:00:00:05:1E:76:86:80	10:00:00:05:1E:76:86:80	
10:00:00:05:1E:34:02:4D	10:00:00:05:1E:34:02:4D	
IBM_B32_23		v6.2.0g
Host Group		
Chassis Group		

Figure 9-22 DCFM FC-FC routing menu

2. Select **Router Configuration option**. The “Router Configuration - Connect Edge Fabric” dialog box opens, as shown in Figure 9-23.



Router Configuration - Connect Edge fabric - 10:00:00:05:1E:34:02:4D

Use this dialog to begin the process of configuring EX_Ports on a Router. Once EX_ports are successfully configured, physically connect the fabric,10:00:00:05:1E:34:02:4D, to the configured EX_Ports.

Select the FC router that you want to connect to fabric 10:00:00:05:1E:34:02:4D. Select the Fabric ID, which must be the same across all connected ports. Click OK to launch Element Manager and finalize the configuration of EX_Ports.

Available Routers

All Levels	Name	Device Type	Tag	Se
10:00:00:05:1E:34:02:4D	10:00:00:05:...			
10:00:00:05:1E:76:86:80	10:00:00:05:...			
FICON Fabric-10:00:00:05	FICON Fabric...			
SAN384B	SAN384B			

Selected Router

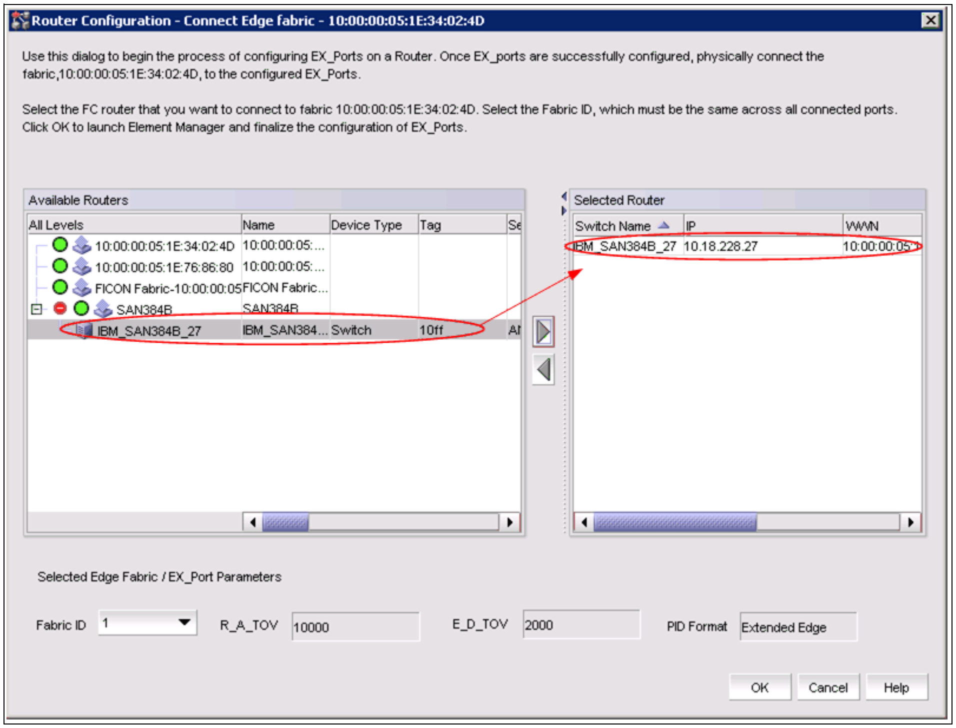
Switch Name	IP	WWN

Selected Edge Fabric / EX_Port Parameters

Fabric ID: 1 R_A_TOV: 10000 E_D_TOV: 2000 PID Format: Extended Edge

Figure 9-23 Connect Edge Fabric dialog box

3. Select the FC router from Available Routers table. Click the right arrow to move the FC router you selected to the Selected Router table, as shown in Figure 9-24.



Router Configuration - Connect Edge fabric - 10:00:00:05:1E:34:02:4D

Use this dialog to begin the process of configuring EX_Ports on a Router. Once EX_ports are successfully configured, physically connect the fabric,10:00:00:05:1E:34:02:4D, to the configured EX_Ports.

Select the FC router that you want to connect to fabric 10:00:00:05:1E:34:02:4D. Select the Fabric ID, which must be the same across all connected ports. Click OK to launch Element Manager and finalize the configuration of EX_Ports.

Available Routers

All Levels	Name	Device Type	Tag	Se
10:00:00:05:1E:34:02:4D	10:00:00:05:...			
10:00:00:05:1E:76:86:80	10:00:00:05:...			
FICON Fabric-10:00:00:05	FICON Fabric...			
SAN384B	SAN384B			
IBM_SAN384B_27	IBM_SAN384...	Switch	10ff	Al

Selected Router

Switch Name	IP	WWN
IBM_SAN384B_27	10.18.228.27	10:00:00:05

Selected Edge Fabric / EX_Port Parameters

Fabric ID: 1   R_A_TOV: 10000   E_D_TOV: 2000   PID Format: Extended Edge

Figure 9-24 Connect Edge Fabric, selecting Backbone and FID

4. Select a valid fabric ID (1 - 128) from the Fabric ID list. If the fabric is already configured to the FC router, the fabric ID is automatically selected. You can choose any unique fabric ID if it is consistent for all EX_Ports that connect to the same edge fabric.

> **Note:** The selected FID is the FID for the link as described in the `portcfgexport` command. Refer to 9.3.3, “Configuring inter-fabric link (IFL)” on page 157.

5. Click **OK** on the Router Configuration in the Connect Edge Fabric dialog box.

   The Element Manager starts automatically and opens the Port Configuration Wizard (Figure 9-25).

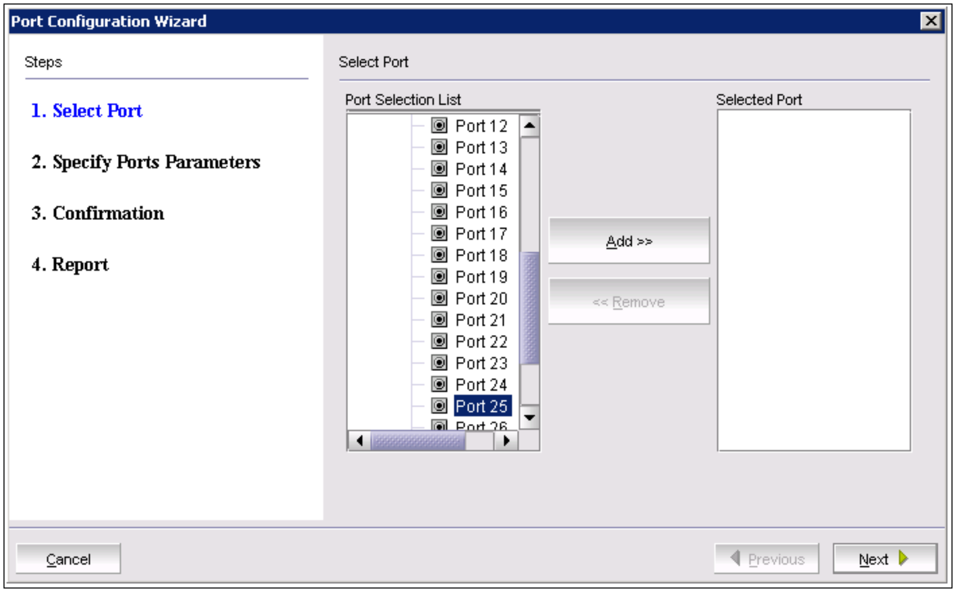


Figure 9-25 Element manager (Web Tools) Port Configuration wizard

6. Follow the same procedures with the element manger as described in 9.5.2, “Configuring inter-fabric link” on page 175 to have the fabrics configured with IFL.

9.6.1 Creating LSAN zones

Create the LSAN zones. An LSAN zone must be defined and enabled in each fabric that will be sharing a particular device:

- Backbone
- Edge

> **Note:** Create the LSAN zone with the prefix LSAN, using the tool you normally use for creating zones (CLI, Web Tools, DCFM).
>
> LSAN zone members must be identified by their PWWN.

For LSAN zone creation examples, refer to 9.3.4, “Creating LSAN zones” on page 162

9.6.2 Configuring routing domain IDs

Logical (phantom) domains are created to enable routed fabrics:

- A logical domain, called a front domain, is created in edge fabrics for every IFL.
- A logical domain, called a translate (xlate) domain, is created in routed fabrics that share devices.

> **Note:** Use Element Manager (Web Tools) or the CLI for EX_Ports creation. You might have to configure or change routing domain IDs by using DCFM.

To configure routing domain IDs, follow these steps:

1. Select the fabric for which you want to configure phantom domains. Select **Configure** → **Routing Domain IDs**. See Figure 9-26.

   Alternatively, you can right-click the edge fabric in the connectivity map or the Product List and select **Configure Routing Domain IDs**.

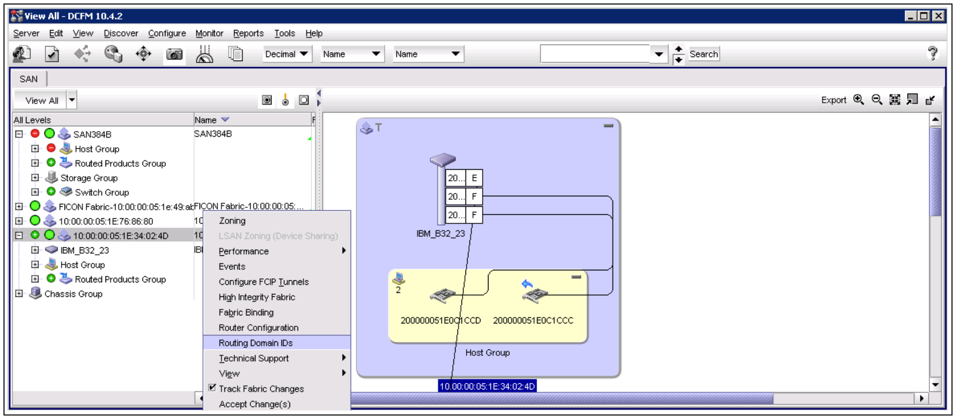
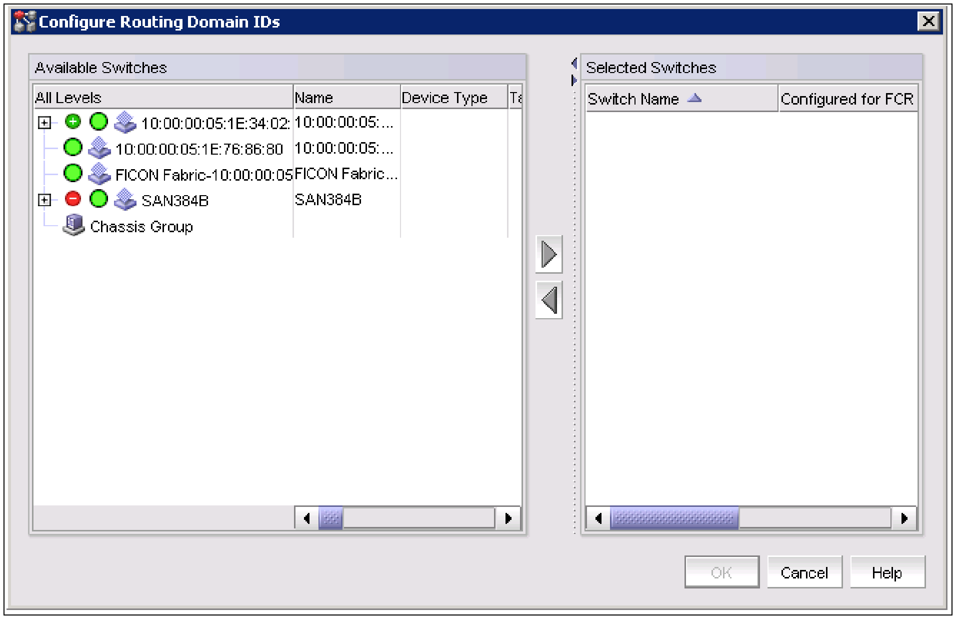


Figure 9-26 Routing Domain ID Menu

The Configure Routing Domain IDs dialog box (Figure 9-27) opens.

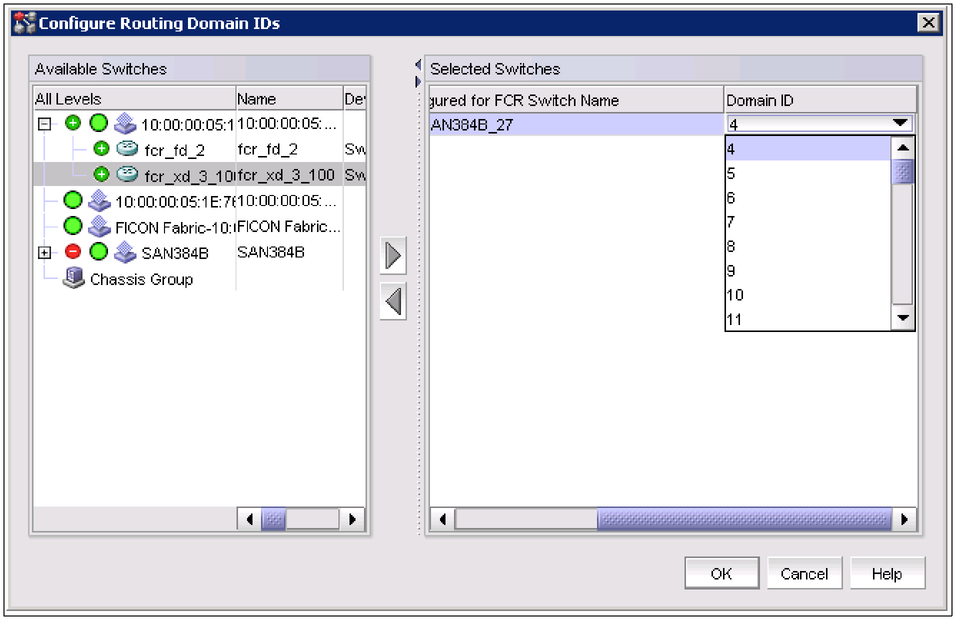


All Levels	Name	Device Type	Ta
⊞ ⊕ ● 10:00:00:05:1E:34:02:	10:00:00:05:...		
● 10:00:00:05:1E:76:86:80	10:00:00:05:...		
● FICON Fabric-10:00:00:05	FICON Fabric...		
⊞ ⊖ ● SAN384B	SAN384B		
Chassis Group			

Figure 9-27 Configure Routing Domain IDs

2. Right-click anywhere in the Available Switches table and select **Expand All** to expand the switch group for the fabric to display the FCR logical switches.

3. Select a logical switch, and click the right arrow to move the switch to the Selected Switches table. See Figure 9-28.



All Levels	Name	De
10:00:00:05:1	10:00:00:05:...	
fcr_fd_2	fcr_fd_2	Sw
fcr_xd_3_10	fcr_xd_3_100	Sw
10:00:00:05:1E:7	10:00:00:05:...	
FICON Fabric-10:	FICON Fabric...	
SAN384B	SAN384B	
Chassis Group		

gured for FCR Switch Name	Domain ID
AN384B_27	4

4
5
6
7
8
9
10
11

Figure 9-28 Configure Routing Domain ID - Selecting Logical switch

4. Select an unused domain ID number from the Domain ID list.

   You might have to scroll right or expand the size of the dialog box further to see the Domain ID column.

5. Click **OK**. Routing Domain ID is now set.

9.6.3 Showing FC-FC routing in DCFM

Figure 9-29 shows the FC-FC routing view in DCFM.

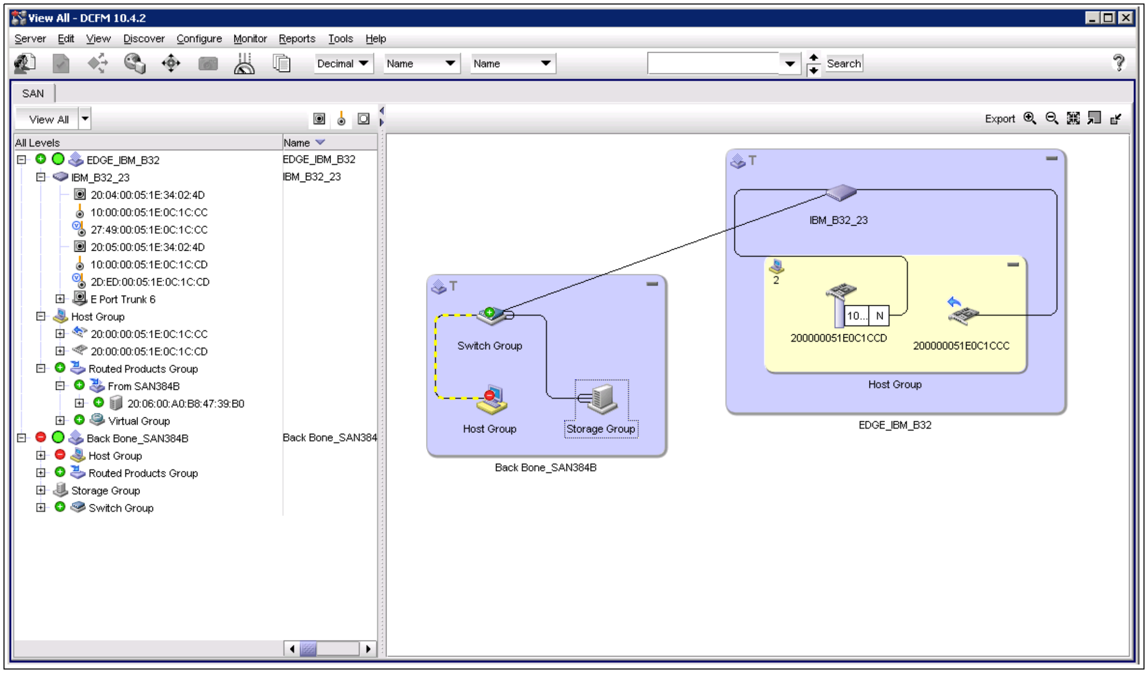


Figure 9-29 FC-FC routing in DCFM

FC-FC Routing is now implemented.

10

FCIP implementation

In this chapter, we describe how to extend our SAN fabric by using FCIP links, to establish connections between devices in different fabrics. We perform this using Web Tools, Data Center Fabric Manager (DCFM), and the command-line interface (CLI), and we give examples of how to make this work.

10.1 Recent changes in the FCIP implementation

Since the last edition of this book, two releases of FabricOS have been released. In this section, we discuss the changes in versions 6.3.1 and 6.4.0. In terms of the CLI the implementation is the same, but we introduce the changes here so they are clear, and we document all the new features or differences with previous versions.

We first review some important terms related to FCIP that you should be familiar with:

- Circuit

  A circuit is a communication that is established between a source IP address to destination IP address.

- Tunnel

  A tunnel is a collection of one or more circuits between two switches. Note that in the case of two or more circuits in the tunnel, the tunnel is trunked.

- VE ort

  A VE port is a Virtual_E port that is behind one or more physical ports on each side of the tunnel.

Figure 10-1 shows a graphical representation of these terms.

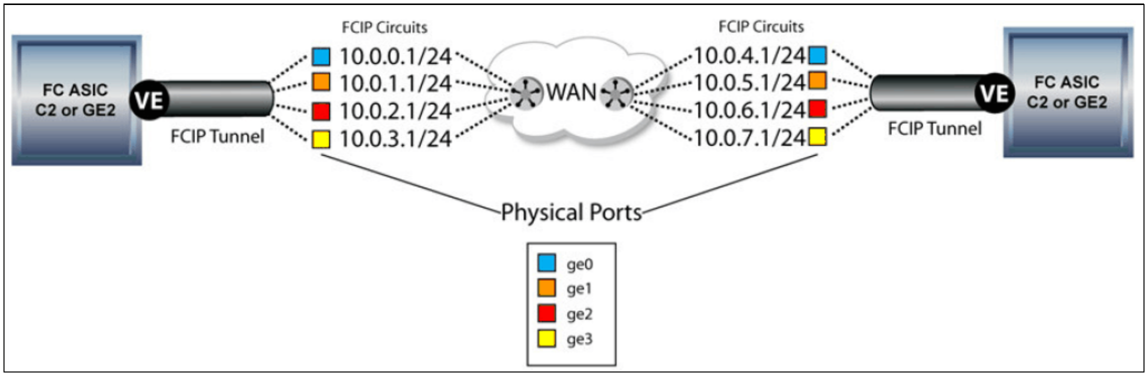


Figure 10-1 FCIP terms explanation

The next sections describe the main changes in the two latest releases of the firmware that concerns FCIP implementation. These changes do not affect the commands and the way to proceed or execute one FCIP configuration, but can have an impact on how to plan your infrastructure and how to deploy it. These changes can also explain why some features will work after you update the firmware, but you cannot modify them afterwards, because the FabricOS will require compliance with some values. If this is the case in the latest release, we explain it.

> **Note:** This book is not intended to provide a comprehensive list of all changes and differences between releases. For more information, refer to the administrator's guide, the `readme.txt` files, and/or the FabricOS manuals.

Changes in FabricOS version 6.3.1

In this version of FabricOS, we have four major changes:

- 10 GbE to 1GbE FCIP tunnel/circuit connectivity
- VLAN tagging/802.1p
- IPSec (only for the IBM System Storage SAN06B-R)
- DCFM v10.4 support for all the features above

Changes in FabricOS version 6.4.0

This version of FabricOS has the following changes:

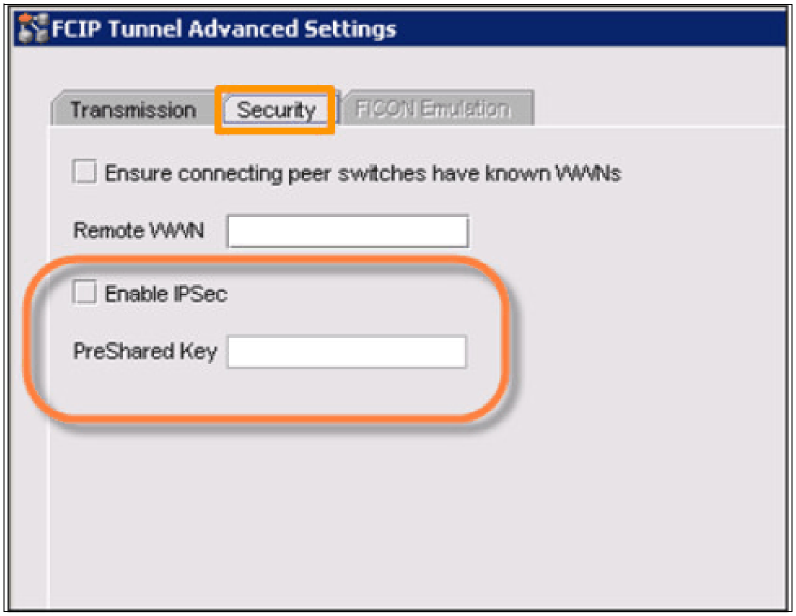
- IPv6 (IPv6 support for IPSec is not supported)
- IPSec (for FCoE 10GbE blade, already supported on SAN06B-R)
- Virtual EX_port (for FCoE 10GbE blade, already supported on SAN06B-R)
- Software compression for maximum compression ratio (for FCoE 10GbE blade, already supported on SAN06B-R)
- DSCP
- Scalability increase (4 blades per chassis, for FCoE 10GbE blade)
- Lossless DLS on FC ports
- TPerf enhancements
- Supports up to 100ms with 0.1% packet loss for FCIP tunnels with one or both ends on 10GbE
- DCFM v10.4 support for all the features above

These changes are explained in detail in Chapter 2, "Multiprotocol routing terminology and concepts" on page 19.

DCFM screenshots of the previously listed enhancements

In the following set of screen captures you will see the enhancements in the DCFM software. This section is intended to show how it looks in the DCFM interface to have a clear overview of the changes.

As you can see in Figure 10-2, DCFM now supports the configuration of FCIP tunnel advanced settings. You can reach this menu when creating or editing a tunnel, under the **Advanced Settings** button.



☐ Ensure connecting peer switches have known WWNs

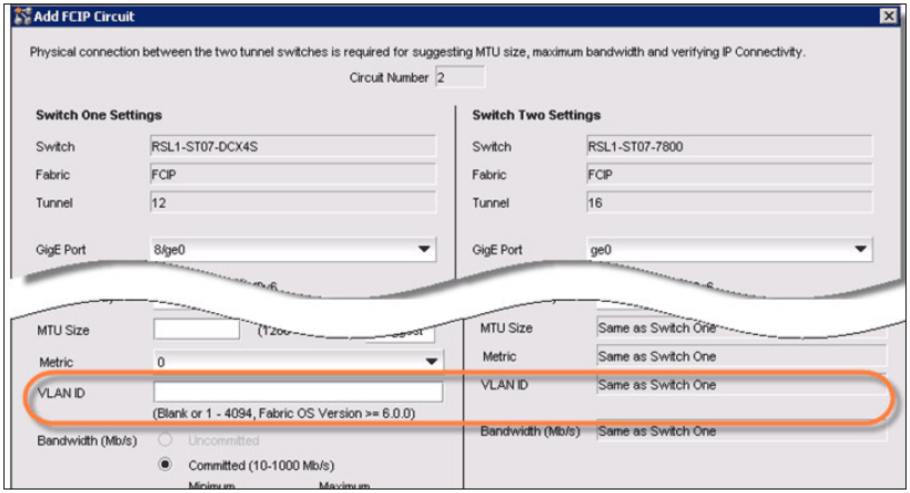
Remote WWN

☐ Enable IPSec

PreShared Key

Figure 10-2 TCIP tunnel configuration on DCFM

In Figure 10-3, see how DCFM is able to help configure the VLAN tagging options for FCIP, and DCFM will be able to discover both fabrics for the VLAN.



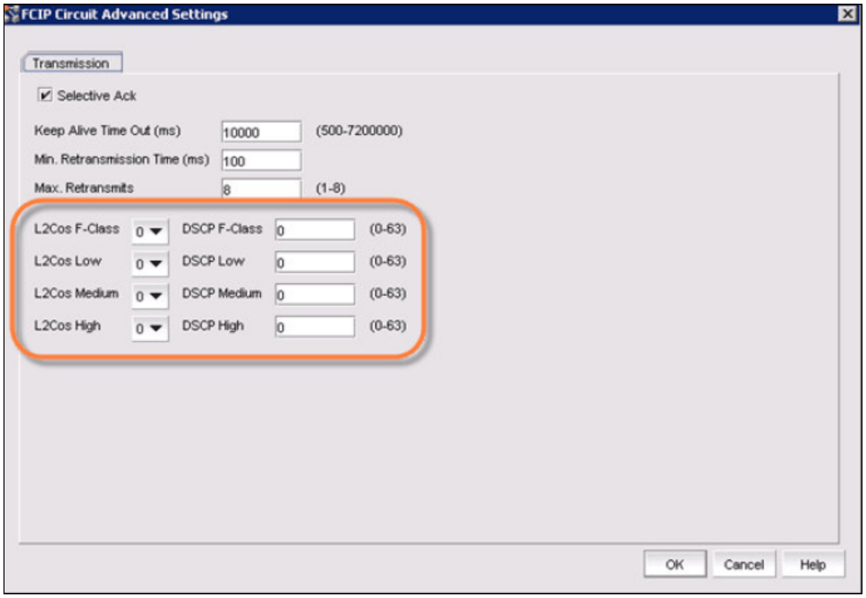
Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number 2

Switch One Settings		Switch Two Settings	
Switch	RSL1-ST07-DCX4S	Switch	RSL1-ST07-7800
Fabric	FCIP	Fabric	FCIP
Tunnel	12	Tunnel	16
GigE Port	8/ge0	GigE Port	ge0
MTU Size		MTU Size	Same as Switch One
Metric	0	Metric	Same as Switch One
VLAN ID	(Blank or 1 - 4094, Fabric OS Version >= 6.0.0)	VLAN ID	Same as Switch One
Bandwidth (Mb/s)	○ Uncommitted ● Committed (10-1000 Mb/s)	Bandwidth (Mb/s)	Same as Switch One

Figure 10-3 VLAN tagging configuration on DCFM

Figure 10-4 shows how to configure DSCP and L2CoS using DCFM, in the “FCIP circuit Advanced Settings” page for the circuit.



FCIP Circuit Advanced Settings

Transmission

☑ Selective Ack

Keep Alive Time Out (ms) 10000 (500-7200000)

Min. Retransmission Time (ms) 100

Max. Retransmits 8 (1-8)

L2Cos F-Class 0 DSCP F-Class 0 (0-63)

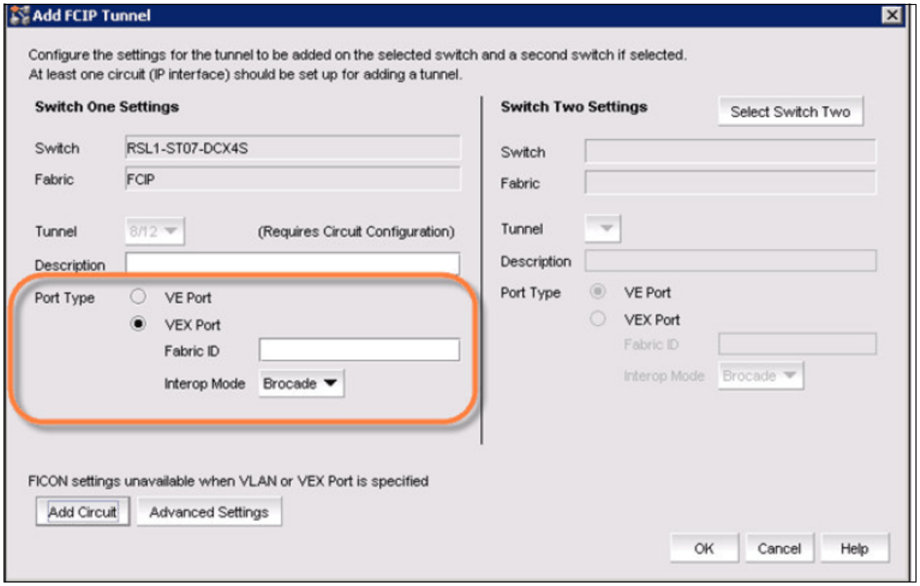
L2Cos Low 0 DSCP Low 0 (0-63)

L2Cos Medium 0 DSCP Medium 0 (0-63)

L2Cos High 0 DSCP High 0 (0-63)

Figure 10-4 DSCP and L2CoS options

Figure 10-5 is the configuration screen for the VEX_Port options, using DCFM.



Add FCIP Tunnel

Configure the settings for the tunnel to be added on the selected switch and a second switch if selected.
At least one circuit (IP interface) should be set up for adding a tunnel.

Switch One Settings

Switch RSL1-ST07-DCX4S

Fabric FCIP

Tunnel 8/12 (Requires Circuit Configuration)

Description

Port Type ○ VE Port ● VEX Port

Fabric ID

Interop Mode Brocade

Switch Two Settings

Select Switch Two

Switch

Fabric

Tunnel

Description

Port Type ● VE Port ○ VEX Port

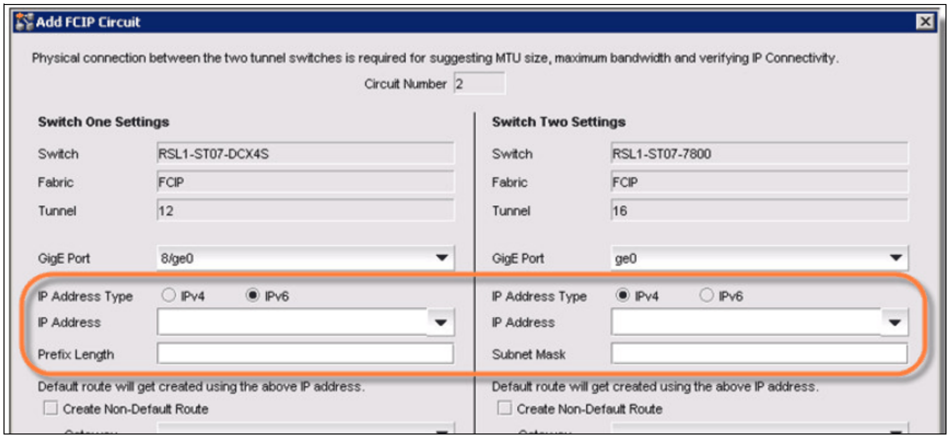
Fabric ID

Interop Mode Brocade

FICON settings unavailable when VLAN or VEX Port is specified

Figure 10-5 VEX_Port configuration screen

IPv6 support will be added in the configuration screens, when available, as shown in Figure 10-6.


Add FCIP Circuit

Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number 2

Switch One Settings

Switch: RSL1-ST07-DCX4S
Fabric: FCIP
Tunnel: 12
GigE Port: 8/ge0
IP Address Type: ○ IPv4 ● IPv6
IP Address:
Prefix Length:

Default route will get created using the above IP address.

□ Create Non-Default Route

Switch Two Settings

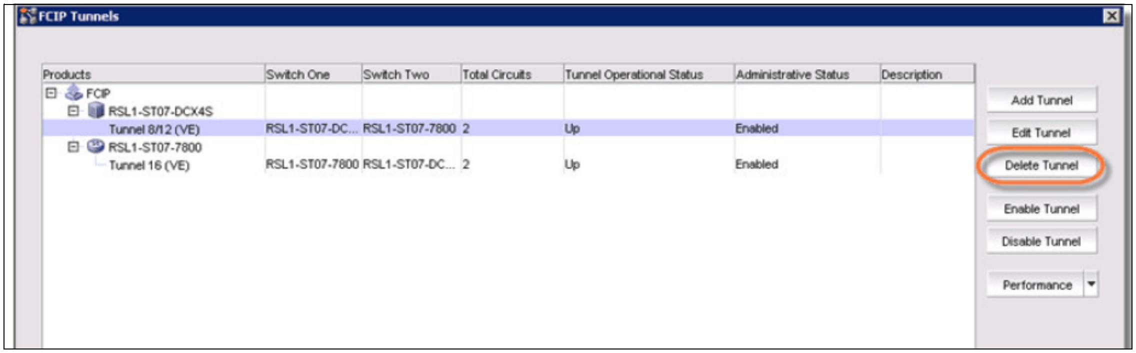
Switch: RSL1-ST07-7800
Fabric: FCIP
Tunnel: 16
GigE Port: ge0
IP Address Type: ● IPv4 ○ IPv6
IP Address:
Subnet Mask:

Default route will get created using the above IP address.

□ Create Non-Default Route

Figure 10-6 IPv6 support

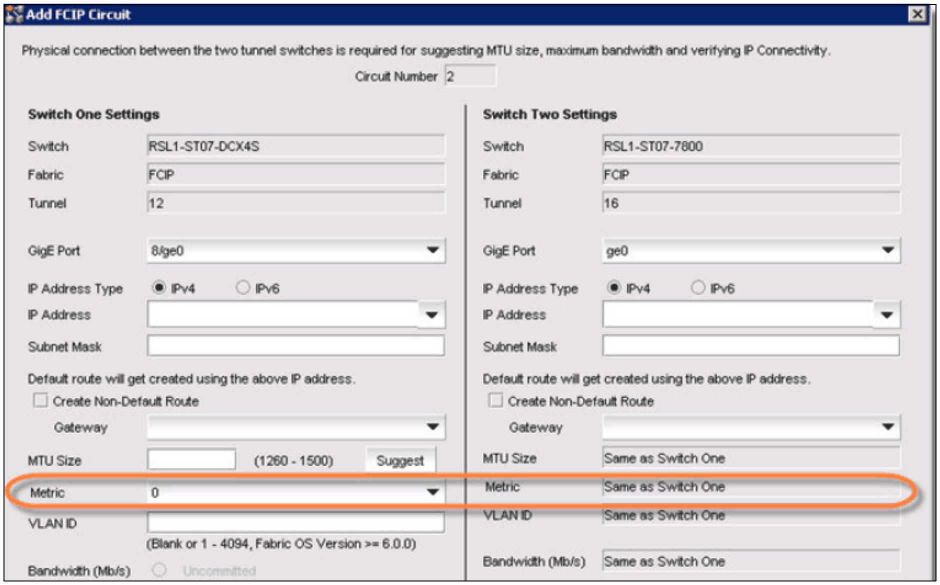
There is a new **Delete** button in the FCIP tunnel configuration screen that lets you delete a tunnel from DCFM. This is shown in Figure 10-7.


FCIP Tunnels

Products	Switch One	Switch Two	Total Circuits	Tunnel Operational Status	Administrative Status	Description
FCIP						
RSL1-ST07-DCX4S						
Tunnel 8/12 (VE)	RSL1-ST07-DC...	RSL1-ST07-7800	2	Up	Enabled	
RSL1-ST07-7800						
Tunnel 16 (VE)	RSL1-ST07-7800	RSL1-ST07-DC...	2	Up	Enabled	

Figure 10-7 Delete button for FCIP tunnel on DCFM

There is a new “metric” field in DCFM that can be configured when adding a new FCIP circuit from the GUI. This is shown in Figure 10-8.



Add FCIP Circuit

Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number 2

Switch One Settings

Switch RSL1-ST07-DCX4S
Fabric FCIP
Tunnel 12
GigE Port 8/ge0
IP Address Type ● IPv4 ○ IPv6
IP Address
Subnet Mask
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway
MTU Size (1260 - 1500) Suggest
Metric 0
VLAN ID
(Blank or 1 - 4094, Fabric OS Version >= 6.0.0)
Bandwidth (Mb/s) ○ Uncommitted

Switch Two Settings

Switch RSL1-ST07-7800
Fabric FCIP
Tunnel 16
GigE Port ge0
IP Address Type ● IPv4 ○ IPv6
IP Address
Subnet Mask
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway
MTU Size Same as Switch One
Metric Same as Switch One
VLAN ID Same as Switch One
Bandwidth (Mb/s) Same as Switch One

Figure 10-8 Metric field when adding an FCIP circuit on DCFM

10.1.1 Configuration guidelines

To configure FCIP using the latest FabricOS version there are guidelines recommended by the manufacturer. In this section we address the main ones. These guidelines help you using the new features and serve as a reminder when you update your firmware. As described in the beginning of this chapter, some updates are possible with no constraints, but some others are limited by some hardcoded values that you need to know. These limits are explained in the sections that follow.

Committed rate

An FCIP configuration must have the same committed rate configuration on each end of a circuit, starting with FabricOS 6.4.0. In previous releases you could have different committed rates on each side. This committed rate is enforced at circuit initialization, and if the committed rates do not match, an error is shown in the CLI or log.

Figure 10-9 illustrates this configuration.

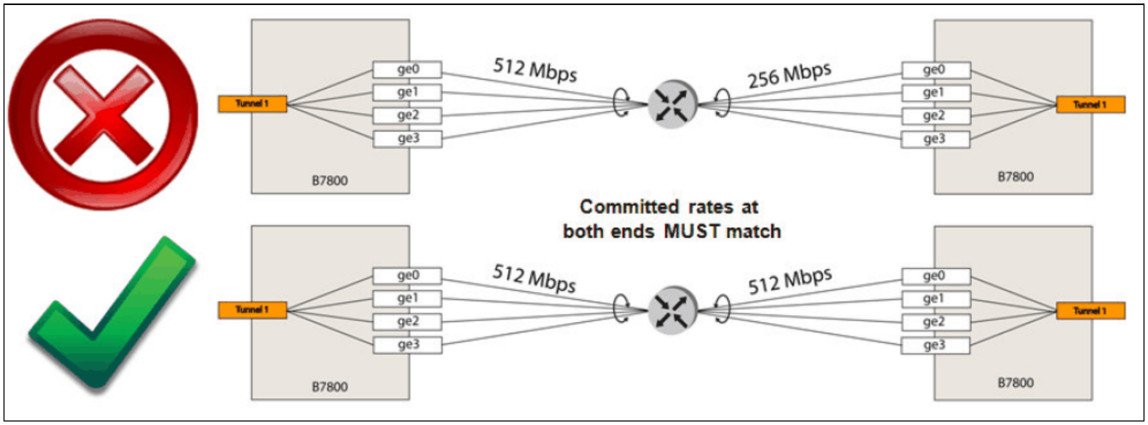


Figure 10-9 Committed rates recommendations.

This includes tunnels that exist already and are upgraded to FabricOS 6.4.0. After upgrade, the tunnel cannot go online, and an error is generated.

Note: Remember to validate the committed rates in your configuration, especially in the case of a FabricOS update.

Adaptive Rate Limiting (ARL)

When using ARL, consider the following caveats:

- The maximum committed rate cannot be larger than five times the minimum committed rate. For example:
  - A minimum of 100 Mbps and a maximum of 500 Mbps is allowed
  - A minimum of 10 Mbps and a maximum of 500 Mbps will not be allowed
- The CLI produces an error if the configuration request does not meet the guidelines above.

Figure 10-10 shows an example of this ARL guideline.

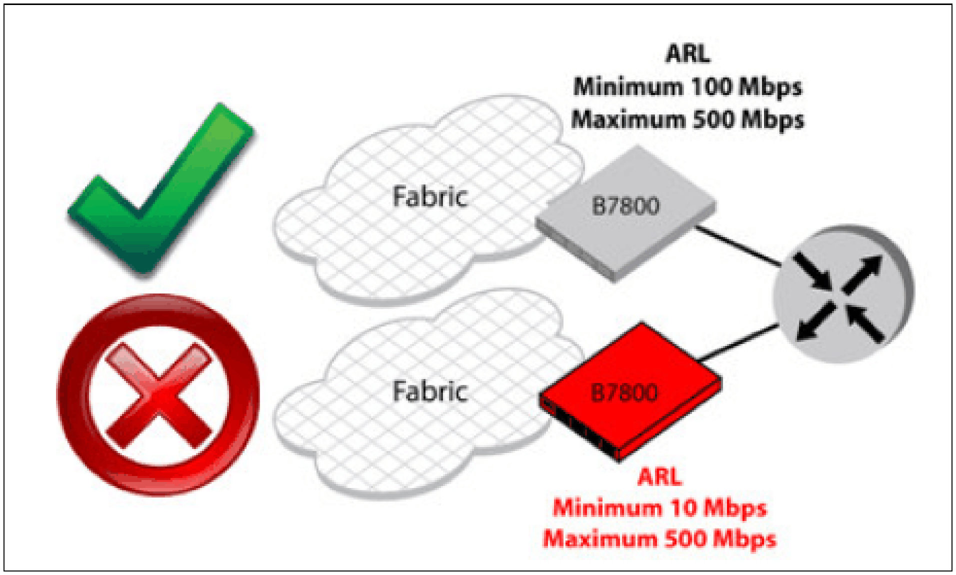


Figure 10-10 ARL limits

When updating an existing tunnel, the tunnel continues to function using an invalid configuration. The administrator cannot make additional changes to the tunnel configuration until the ARL delta is compliant. Remember this when updating and later validating your configuration to avoid compliance issues.

Trunking across multiple FCIP circuits

When trunking across multiple FCIP circuits the delta bandwidth between the circuits should be no greater than a factor of four. For example:

- Trunking between a circuit running on an OC3 (155.52 Mbps) and another running on an OC12 (622.08 Mbps) is allowed.
- Trunking between a 10 Mbps circuit and a 500 Mbps circuit is **not** recommended.

This is not enforced with the CLI, but it is not supported, so consider it when defining your trunking. If the factor is greater than four, the tunnel cannot fully use all the bandwidth available for the circuits, and you will not be using the optimal configuration.

This restriction only includes circuits with the same metric values (standby circuits, metric 1, are not included in this calculation).

In general, the minimum committed rate of a circuit will be 10 Mbps, and is enforced by the CLI. A configuration attempt lower than this will fail.

Note: On the previous FabricOS 6.3 the minimum committed rate was 1.544 Mbps.

When upgrading an existing tunnel, the tunnel continues to function using an invalid configuration. The administrator cannot make additional changes in the tunnel configuration until the minimum commit rate is compliant. Remember that some configurations are not supported, even if they do work.

Supported packet loss and delay

In some cases the tunnel might have some tolerance to packet loss and support a certain delay. This is well documented. Table 10-1 shows the supported values for the latest two releases of FabricOS.

Table 10-1 shows the supported packet loss and delay in the two latest (at the time of writing) releases of FabricOS.

Table 10-1 Supported packet loss and delay

Tunnels	FabricOS 6.3	FabricOS 6.4.0
Both ends 1GbE	200 ms latency 1% packet loss	200 ms latency 1% packet loss
One or both ends 10GbE	50 ms latency 0.1% packet loss	100 ms latency 0.1% packet loss

Scalability considerations

When planning your network, scalability should be considered. It is common to start with a small to medium configuration, and plan to upgrade in the future. In the FabricOS release 6.4.0, there is support for up to four FCoE 10GbE blades in a chassis.

Note: Downgrading to FabricOS 6.3 will fail if there are more than two FCoE 10 GbE blades in the chassis.

As stated at the beginning, the changes that we have explained are not always related to new features, but more a set of new enhancements of existing features, and the corresponding guidelines. Consider those when implementing as the CLI or Web Tools can enforce some values or specific configurations. If this is the case, you will notice it with an error or a message from the system.

10.2 Configuring FCIP and LSAN

In this section, we discuss the steps to establish a connection between two fabrics to enable a server at site A to access storage at site B. This process is done by using SAN routers with an FCIP link between them. We also demonstrate how to create LSAN zones using devices from both fabrics, which enables the attached devices to use the FCIP tunnel.

You can configure the FCIP connection by using CLI or DCFM. Web Tools configuration of FCIP tunnels is not possible in Fabric OS version 6.2. To accomplish our configuration we demonstrate how to use DCFM and CLI in the following sections.

To configure FCIP tunnels, perform the following steps:

1. Check whether the FCIP license is applied.
2. Enable persistently disabled ports.
3. Configure the virtual GigE ports.
4. Define an IP interface on each virtual GigE port.
5. Define IP routes on GigE ports.
6. Verify IP connectivity.
7. Configure the FCIP tunnel.
8. Verify the FCIP tunnel setup.
9. Create LSAN-zones.
10. Verify performance on the GigE connections.

Lab configuration

This section describes the lab configuration that is used to set up the FCIP and LSAN environment.

In our scenario, we have a Windows 2003 Server R2(A) at one site connected to a SAN64B-4 switch through a Brocade 8 Gbps HBA. This server needs to access DS4700 storage (B) at another site. The DS4700 is connected to a SAN256B backbone director switch with FC-connections. The two sites are placed at significant distances, and traffic has to be routed over an IP-network, as FC connectivity between the sites does not exist. The two sites represent different SANs and merging the SANs is not allowed, that is, we have to establish a connection between the two SANs, which will allow traffic between the two devices (storage and server), but will not merge the fabrics.

The devices we use to interconnect the two fabrics are an FR4-18i routing blade in the SAN256B director switch at the storage site, and a SAN18B-R router connected to the SAN64B-4 at the server site.

In our lab, the IP network is a direct connection between the LAN ports of the two SAN routers.

In a real life environment, because the SAN18B-R routers use a standard optical 4 Gbps Fibre Channel SFP for the two 1 Gbps LAN connections, the IP network must be able to support such connections. Examples of such switches are the IBM c-series or IBM g-series of Ethernet Switches.

Figure 10-11 shows our lab configuration.

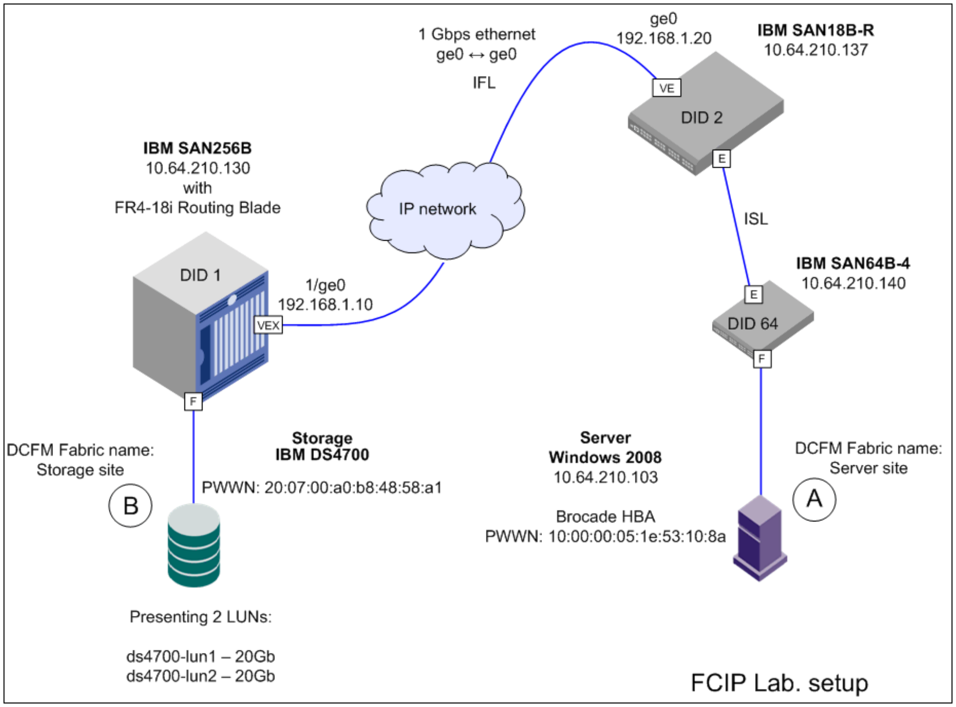


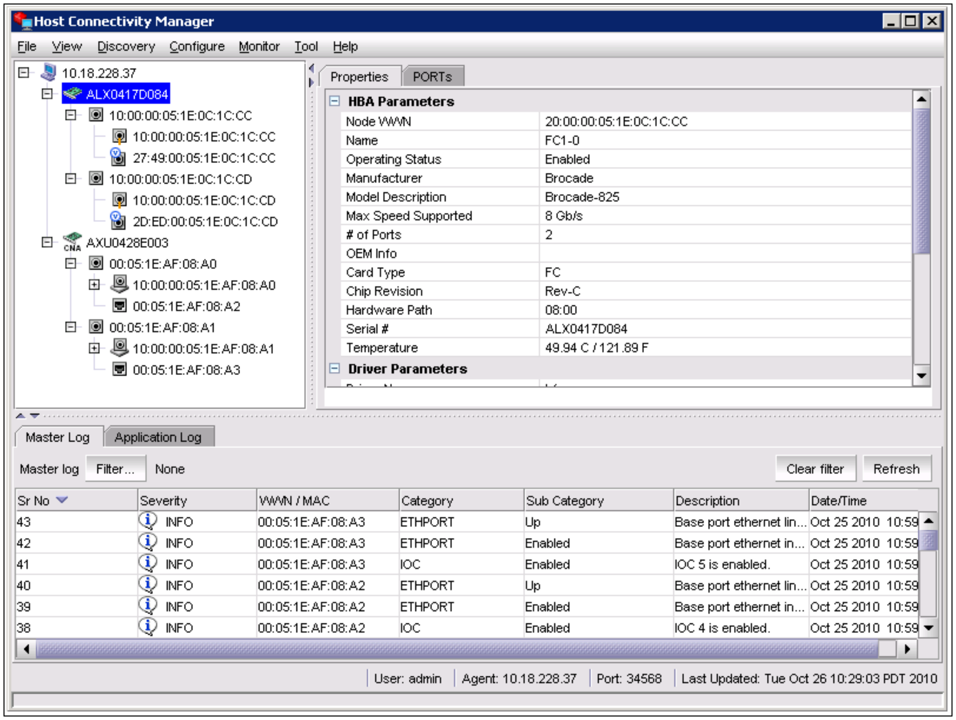
Figure 10-11 Our lab setup: an FCIP routed network

10.3 Initial tasks

In this section, we show the initial tasks that must be performed.

10.3.1 Identifying HBA WWNs

Before we can configure storage LUNs on the DS4700, we must identify which worldwide names (WWN) our server HBAs have. Our server uses two Brocade 8 Gbps HBAs, and we use the Brocade Host Connectivity Manager (HCM) version 2.0 to check the WWNs. Figure 10-12 shows the HBA WWNs using HCM version 2.0.



```
⊟ 10.18.228.37
  ⊟ ALX0417D084
    ⊟ 10:00:00:05:1E:0C:1C:CC
        10:00:00:05:1E:0C:1C:CC
        27:49:00:05:1E:0C:1C:CC
    ⊟ 10:00:00:05:1E:0C:1C:CD
        10:00:00:05:1E:0C:1C:CD
        2D:ED:00:05:1E:0C:1C:CD
  ⊟ AXU0428E003
    ⊟ 00:05:1E:AF:08:A0
      ⊞ 10:00:00:05:1E:AF:08:A0
        00:05:1E:AF:08:A2
    ⊟ 00:05:1E:AF:08:A1
      ⊞ 10:00:00:05:1E:AF:08:A1
        00:05:1E:AF:08:A3
```

⊟ HBA Parameters

Node WWN	20:00:00:05:1E:0C:1C:CC
Name	FC1-0
Operating Status	Enabled
Manufacturer	Brocade
Model Description	Brocade-825
Max Speed Supported	8 Gb/s
# of Ports	2
OEM Info	
Card Type	FC
Chip Revision	Rev-C
Hardware Path	08:00
Serial #	ALX0417D084
Temperature	49.94 C / 121.89 F

⊟ Driver Parameters

Sr No	Severity	WWN / MAC	Category	Sub Category	Description	Date/Time
43	INFO	00:05:1E:AF:08:A3	ETHPORT	Up	Base port ethernet lin...	Oct 25 2010 10:59
42	INFO	00:05:1E:AF:08:A3	ETHPORT	Enabled	Base port ethernet in...	Oct 25 2010 10:59
41	INFO	00:05:1E:AF:08:A3	IOC	Enabled	IOC 5 is enabled.	Oct 25 2010 10:59
40	INFO	00:05:1E:AF:08:A2	ETHPORT	Up	Base port ethernet lin...	Oct 25 2010 10:59
39	INFO	00:05:1E:AF:08:A2	ETHPORT	Enabled	Base port ethernet in...	Oct 25 2010 10:59
38	INFO	00:05:1E:AF:08:A2	IOC	Enabled	IOC 4 is enabled.	Oct 25 2010 10:59

User: admin | Agent: 10.18.228.37 | Port: 34568 | Last Updated: Tue Oct 26 10:29:03 PDT 2010

Figure 10-12 Brocade Host Connectivity Manager

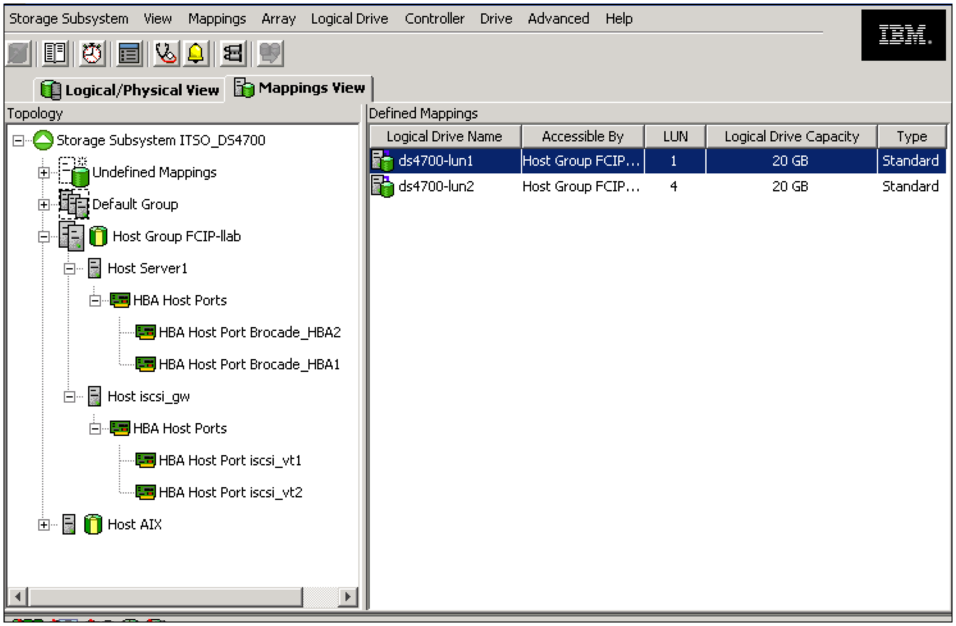
What we need is the worldwide port name (WWPN) of the HBA port we are using for the DS4000 Storage manager. Our server has two single port HBAs, but in our lab we only use one, representing a single fabric.

If we were configuring two fabrics, which would be the case in an optimal scenario, then we would need the WWPN from both HBA ports. In this example, we only configure a single fabric. The WWPN we use is: `10:00:00:05:1e:53:10:8a` We continue by configuring our storage LUNs.

10.3.2 Configuring storage

In our example, we use an IBM DS4700 representing two LUNs, each 20 GB large per Windows 2008 server. By opening the DS4000 Storage Manager, we are now able to create, initialize, and map our three LUNs to the server. We will not go in detail with these steps, but refer to IBM Redbooks publication *IBM System Storage DS4000 and Storage Manager V10.30*, SG24-7010 for more information about configuring DS4000.

Figure 10-13 shows the DS4000 Storage Manager where we have configured and mapped the two 20 GB LUNs to the server with the two Brocade HBAs.



Logical Drive Name	Accessible By	LUN	Logical Drive Capacity	Type
ds4700-lun1	Host Group FCIP...	1	20 GB	Standard
ds4700-lun2	Host Group FCIP...	4	20 GB	Standard

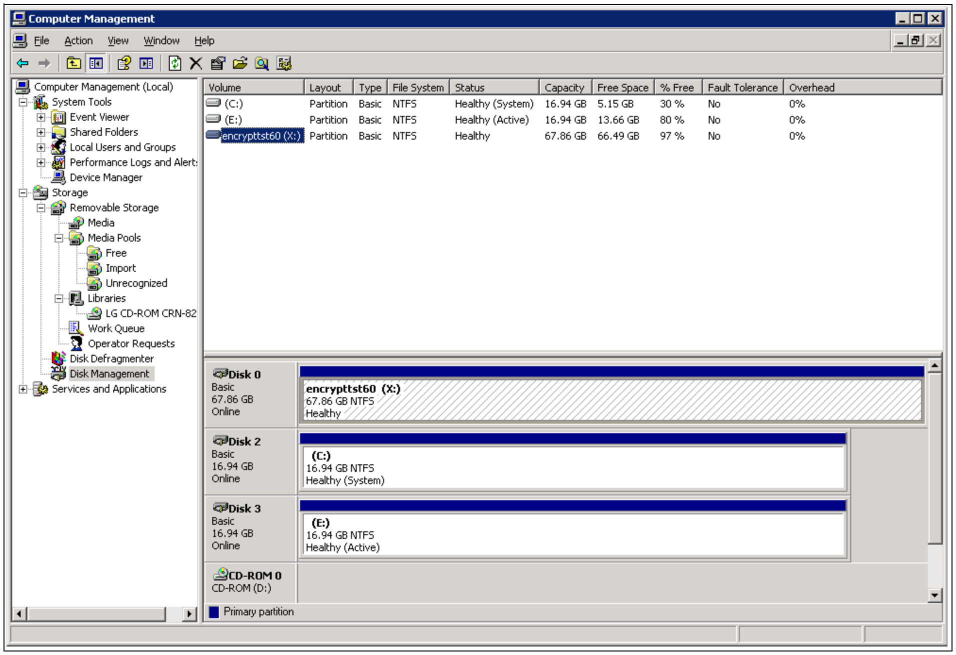
Figure 10-13 DS4000 Storage manager

We are now ready to check our server.

10.3.3 Checking the server

In our example, we use a Windows 2003 Server R2 connected to our SAN by using two single-ported Brocade HBAs. In addition, we have a CNA adapter from Brocade that has two 10 Gbps ports. In the previous steps, we configured storage LUNs and mapped them to the server. However, remember that you need to configure your SAN route and create zoning to see any disk LUNs in disk management.

Figure 10-14 shows the disk management on the server. In our case, three volumes are available, and one of them is an encrypted disk we have created. Without the correct routes setup and zoning, you will not see these volumes.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	16.94 GB	5.15 GB	30 %	No	0%
(E:)	Partition	Basic	NTFS	Healthy (Active)	16.94 GB	13.66 GB	80 %	No	0%
encrypttst60 (X:)	Partition	Basic	NTFS	Healthy	67.86 GB	66.49 GB	97 %	No	0%

Disk 0 Basic 67.86 GB Online	**encrypttst60 (X:)** 67.86 GB NTFS Healthy
Disk 2 Basic 16.94 GB Online	**(C:)** 16.94 GB NTFS Healthy (System)
Disk 3 Basic 16.94 GB Online	**(E:)** 16.94 GB NTFS Healthy (Active)
CD-ROM 0 CD-ROM (D:)	

Figure 10-14 Disk management on the server

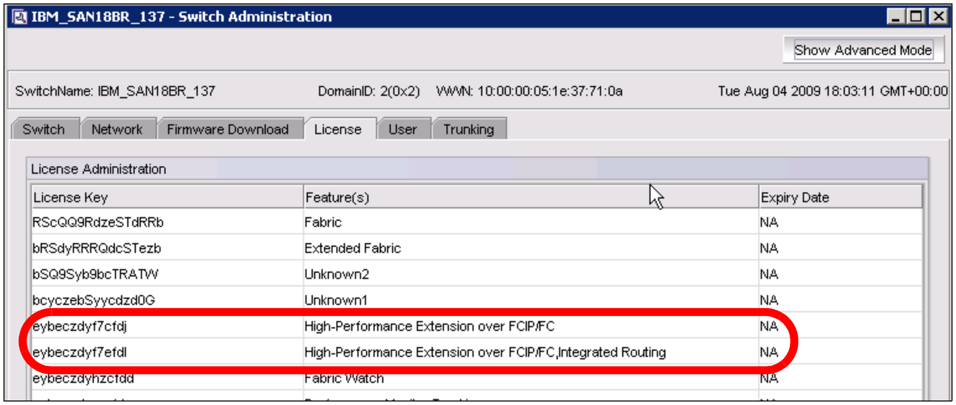
10.3.4 Checking the FCIP license

In this section, we show how to check whether the appropriate license for enabling FCIP. An FC-IP Services or High Performance Extension over FCIP/FC license is required on both sides of the tunnel.

The license can be checked from Web Tools or CLI. We show both in our example. As mentioned previously, licenses have to be installed on both sides of the tunnel. The side we check in our example is the IBM SAN18B-R router with Domain ID 2 (DID 2).

Using Web Tools

Figure 10-15 uses Web Tools to show the installed licenses.



IBM_SAN18BR_137 - Switch Administration

SwitchName: IBM_SAN18BR_137 DomainID: 2(0x2) WWN: 10:00:00:05:1e:37:71:0a Tue Aug 04 2009 18:03:11 GMT+00:00

License Administration

License Key	Feature(s)	Expiry Date
RScQQ9RdzeSTdRRb	Fabric	NA
bRSdyRRRQdcSTezb	Extended Fabric	NA
bSQ9Syb9bcTRATW	Unknown2	NA
bcyczebSyycdzd0G	Unknown1	NA
eybeczdyf7cfdj	High-Performance Extension over FCIP/FC	NA
eybeczdyf7efdl	High-Performance Extension over FCIP/FC,Integrated Routing	NA
eybeczdyhzcfdd	Fabric Watch	NA

Figure 10-15 Licenses are listed on the License page

Using the command-line interface

We now use the command-line interface (CLI) to list the licenses installed on our switches as shown in Example 10-1.

Example 10-1 Showing licenses using CLI

```
IBM_SAN18BR_137:admin> licenseshow
bSQ9Syb9bcTRATW:
    Unknown2 license
RScQQ9RdzeSTdRRb:
    Fabric license
bRSdyRRRQdcSTezb:
    Extended Fabric license
eybeczdyhzcfdd:
    Fabric Watch license
eybeczdyf7cfdj:
    High-Performance Extension over FCIP/FC license
eybeczdyf7efdl:
    High-Performance Extension over FCIP/FC license
    Integrated Routing license
eybeczdyrzcfdn:
    Performance Monitor license
    Trunking license
bcyczebSyycdzd0G:
    Unknown1 license

IBM_SAN18BR_137:admin>
```

The Fibre Channel routing licenses are installed on our switches.

If they were not present on the switch, you would have to go through the following steps to install them:

1. Acquire FCIP activation license (name and type depending on the product to be installed on) from your authorized IBM dealer.
2. Register the license on the following IBM SAN switch feature activation web site, where the switch WWN and the transaction key from the license paper, is needed:

   http://www-912.ibm.com/LicenseRequestClient/

3. Install the license on the switch using CLI or Web Tools. See Example 10-2.

Example 10-2 Example of installing a FCIP license

```
IBM_SAN18BR_137:admin> licenseadd "RScQQ9RdzeSbfZRl"
adding license-key [RScQQ9RdzeSbfZRl]
For license to take effect, Please reboot the switch now...

IBM_SAN18BR_137:admin>
```

We are now ready to enable the FCR routing service.

10.3.5 Enabling the FCR routing service

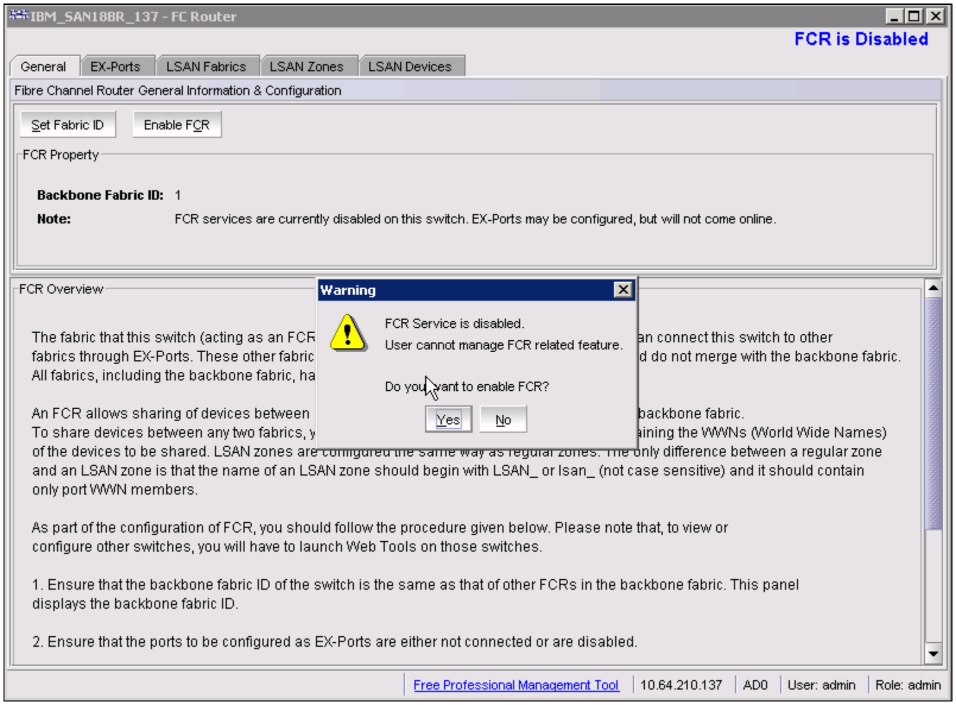
Before we can configure routing, we must enable the FCR routing service. We show how to do this using Web Tools and CLI in the following sections.

Using Web Tools

From the Web Tools main window, click **FCR**, which opens the “FCR General Information & Configuration” window. Click **Enable FCR**.

In the “FCR Property” window, click **Set Fabric ID**. The Backbone Fabric ID must be the same for all other routers connected to the fabric. In our case we leave the Backbone Fabric ID to the default **1**.

Figure 10-16 shows how to enable the FCR service from Web Tools.



Fibre Channel Router General Information & Configuration

FCR Property

Backbone Fabric ID: 1

Note: FCR services are currently disabled on this switch. EX-Ports may be configured, but will not come online.

FCR Overview

The fabric that this switch (acting as an FCR ... an connect this switch to other
fabrics through EX-Ports. These other fabric ... d do not merge with the backbone fabric.
All fabrics, including the backbone fabric, ha

An FCR allows sharing of devices between ... backbone fabric.
To share devices between any two fabrics, y ... ining the WWNs (World Wide Names)
of the devices to be shared. LSAN zones are configured the same way as regular zones. The only difference between a regular zone and an LSAN zone is that the name of an LSAN zone should begin with LSAN_ or lsan_ (not case sensitive) and it should contain only port WWN members.

As part of the configuration of FCR, you should follow the procedure given below. Please note that, to view or configure other switches, you will have to launch Web Tools on those switches.

1. Ensure that the backbone fabric ID of the switch is the same as that of other FCRs in the backbone fabric. This panel displays the backbone fabric ID.

2. Ensure that the ports to be configured as EX-Ports are either not connected or are disabled.

FCR Service is disabled.
User cannot manage FCR related feature.

Do you want to enable FCR?

Free Professional Management Tool | 10.64.210.137 | AD0 | User: admin | Role: admin

Figure 10-16 Enabling FCR from Web Tools

Using the CLI

The same results can be accomplished using CLI, as shown in Example 10-3.

Example 10-3 enabling FCR service from CLI

```
IBM_SAN18BR_137:admin> fosconfig --enable fcr
FC Routing service is enabled

IBM_SAN18BR_137:admin>
```

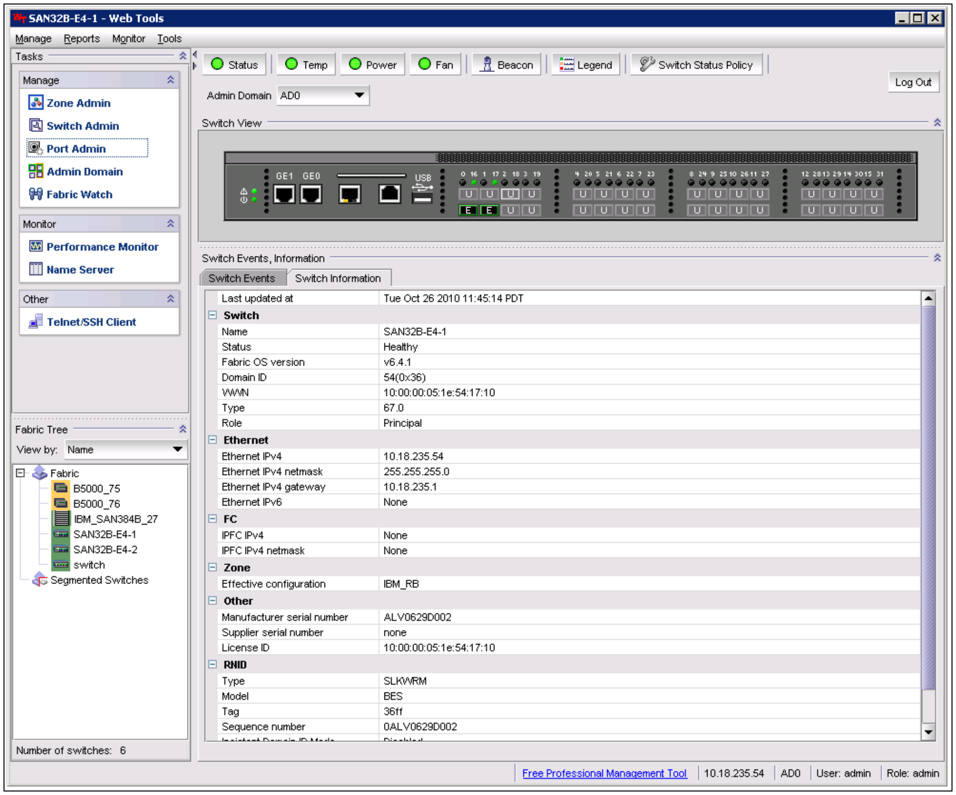
We are ready to enable the GigE ports.

10.3.6 Enabling ports

When a SAN switch port is persistently disabled, it remains disabled even after a switch-reboot. Disabling the ports without doing so persistently will re-enable the port after disabling or rebooting the switch. We now persistently enable our GigE ports. Again, we use Web Tools and CLI.

Using Web Tools

Figure 10-17 shows the Web Tools main window from where we get to the Port Administration (Port Admin) window.

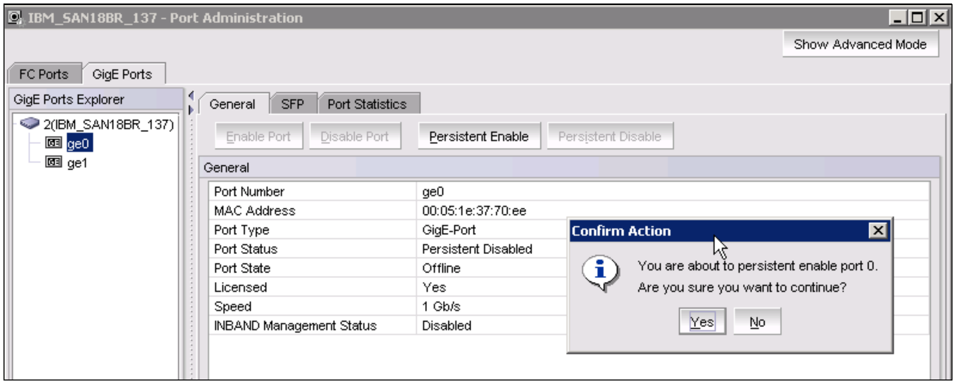


Last updated at	Tue Oct 26 2010 11:45:14 PDT
Switch	
Name	SAN32B-E4-1
Status	Healthy
Fabric OS version	v6.4.1
Domain ID	54(0x36)
WWN	10:00:00:05:1e:54:17:10
Type	67.0
Role	Principal
Ethernet	
Ethernet IPv4	10.18.235.54
Ethernet IPv4 netmask	255.255.255.0
Ethernet IPv4 gateway	10.18.235.1
Ethernet IPv6	None
FC	
IPFC IPv4	None
IPFC IPv4 netmask	None
Zone	
Effective configuration	IBM_RB
Other	
Manufacturer serial number	ALV0629D002
Supplier serial number	none
License ID	10:00:00:05:1e:54:17:10
RNID	
Type	SLKWRM
Model	BES
Tag	36ff
Sequence number	0ALV0629D002

Figure 10-17 Web Tools main window

Click any port listed in the main window.

The Port Admin window opens, shown in Figure 10-18. This shows how to persistently enable the GigE ports from the Port Admin window. Click **Persistent enable**, and it is configured. Confirm your operation through a confirmation window.



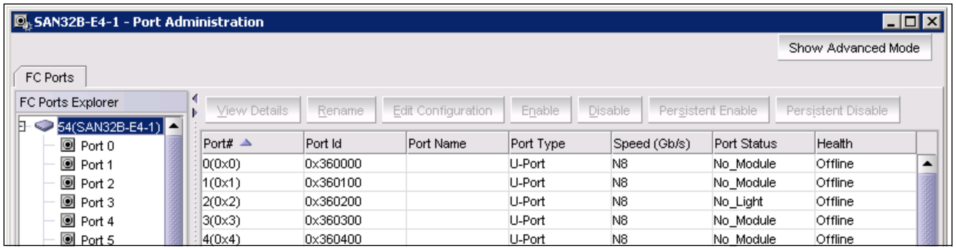
Port Number	ge0
MAC Address	00:05:1e:37:70:ee
Port Type	GigE-Port
Port Status	Persistent Disabled
Port State	Offline
Licensed	Yes
Speed	1 Gb/s
INBAND Management Status	Disabled

Confirm Action

You are about to persistent enable port 0.
Are you sure you want to continue?

Figure 10-18 Persistently enable the GigE ports

Figure 10-19 shows that the GigE ports are now persistently enabled. Port number ge0 is online, which means that a connection exists to another enabled port. Port number ge1 is offline, which means that there is either no connection, or the other end of the connection has a disabled port. However we are only using port ge0 in this exercise.



Port#	Port Id	Port Name	Port Type	Speed (Gb/s)	Port Status	Health
0(0x0)	0x360000		U-Port	N8	No_Module	Offline
1(0x1)	0x360100		U-Port	N8	No_Module	Offline
2(0x2)	0x360200		U-Port	N8	No_Light	Offline
3(0x3)	0x360300		U-Port	N8	No_Module	Offline
4(0x4)	0x360400		U-Port	N8	No_Module	Offline

Figure 10-19 GigE ports are now enabled persistently

Using the CLI

Port management is faster by using the CLI. Ports can be persistently enabled using the **`portcfgpersistentenable`** command, as shown in Example 10-4.

Example 10-4 Enable/disable ports from CLI

```
IBM_SAN18BR_137:admin> portcfgpersistentenable ge0

IBM_SAN18BR_137:admin>
```

To check the ports after managing them, use the **`switchshow`** command.

Because we are not using ge1 ports, we might want to persistently disable them. To disable them, use the **`portcfgpersistentdisable`** command.

We are now ready to configure our tunnel from server to storage.

10.4 Configuring FCIP using DCFM

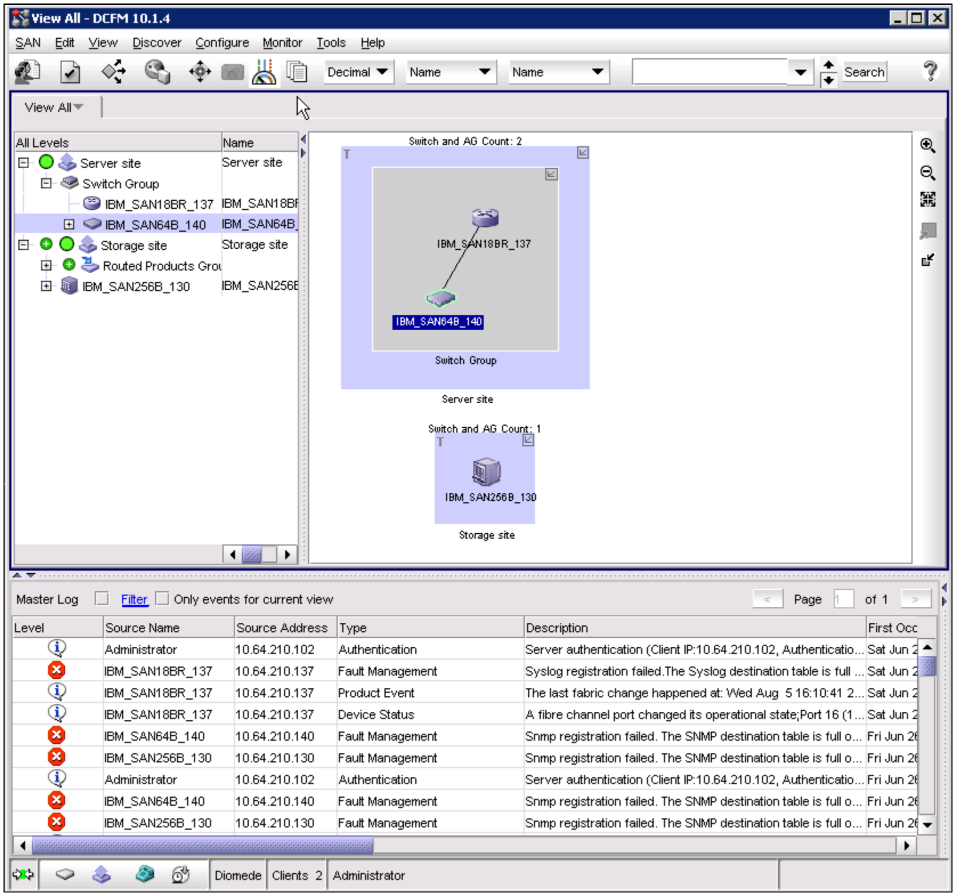
In Fabric OS 6.2, FCIP tunnels cannot be created and managed from Web Tools. In previous versions of Fabric OS, these tasks could be accomplished by opening the Port Administration window, and clicking **Advanced**. Then, by clicking the GigE ports, FCIP interfaces and tunnels could be managed. This functionality has been removed from Web Tools, so FCIP has to be managed from either the CLI or Data Center Fabric Manager (DCFM).

As mentioned in Chapter 7, “Multiprotocol routing basic implementation” on page 113, DCFM Enterprise must be purchased to perform comprehensive FCR (Fibre Channel Routing) and FCIP management. If DCFM Enterprise is not purchased, FCR can be managed only by using the CLI. This is, however, not entirely true. FC-FC connections (EX_ports) can still be created by using Web Tools.

10.4.1 Creating the FCIP tunnel

From the initial DCFM window, the first action is to discover the two SANs between which we are creating an FC route.

Figure 10-20 shows the DCFM main window after discovering our SANs.



Level	Source Name	Source Address	Type	Description	First Occ
ⓘ	Administrator	10.64.210.102	Authentication	Server authentication (Client IP:10.64.210.102, Authenticatio...	Sat Jun 2
✖	IBM_SAN18BR_137	10.64.210.137	Fault Management	Syslog registration failed.The Syslog destination table is full ...	Sat Jun 2
ⓘ	IBM_SAN18BR_137	10.64.210.137	Product Event	The last fabric change happened at: Wed Aug 5 16:10:41 2...	Sat Jun 2
ⓘ	IBM_SAN18BR_137	10.64.210.137	Device Status	A fibre channel port changed its operational state;Port 16 (1...	Sat Jun 2
✖	IBM_SAN64B_140	10.64.210.140	Fault Management	Snmp registration failed. The SNMP destination table is full o...	Fri Jun 26
✖	IBM_SAN256B_130	10.64.210.130	Fault Management	Snmp registration failed. The SNMP destination table is full o...	Fri Jun 26
ⓘ	Administrator	10.64.210.102	Authentication	Server authentication (Client IP:10.64.210.102, Authenticatio...	Fri Jun 26
✖	IBM_SAN64B_140	10.64.210.140	Fault Management	Snmp registration failed. The SNMP destination table is full o...	Fri Jun 26
✖	IBM_SAN256B_130	10.64.210.130	Fault Management	Snmp registration failed. The SNMP destination table is full o...	Fri Jun 26

Figure 10-20 DCFM main window

Perform the following steps to configure the FCIP tunnel:

1. From the Configure menu (Figure 10-21), select **FCIP tunnel**.

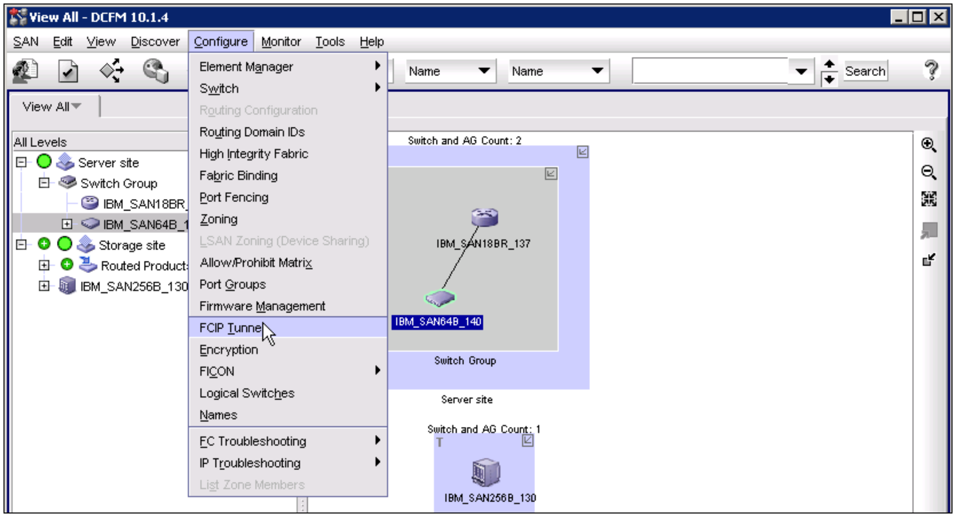
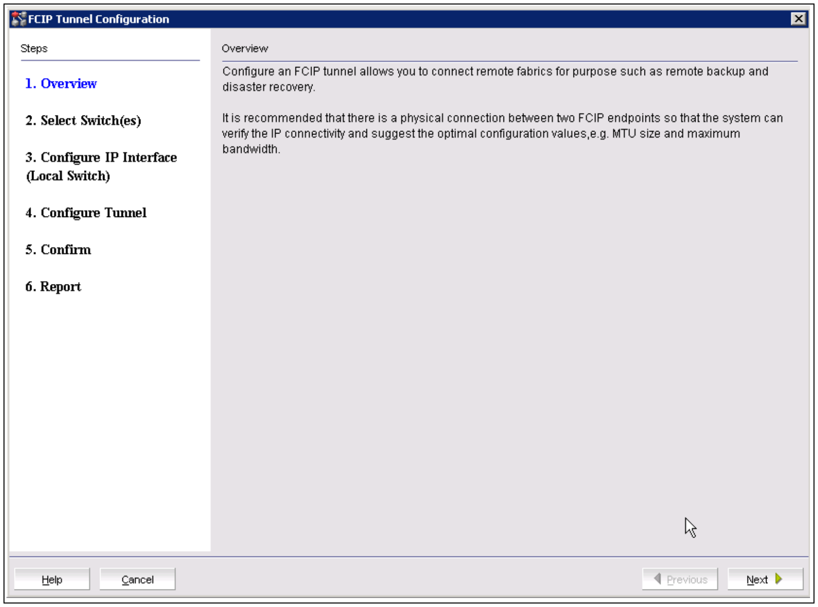


Figure 10-21 FCIP tunnel create option

The FCIP Tunnel Configuration wizard starts at the “Step 1: Overview” window (Figure 10-22). Click **Next**.


FCIP Tunnel Configuration

Steps

1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure Tunnel
5. Confirm
6. Report

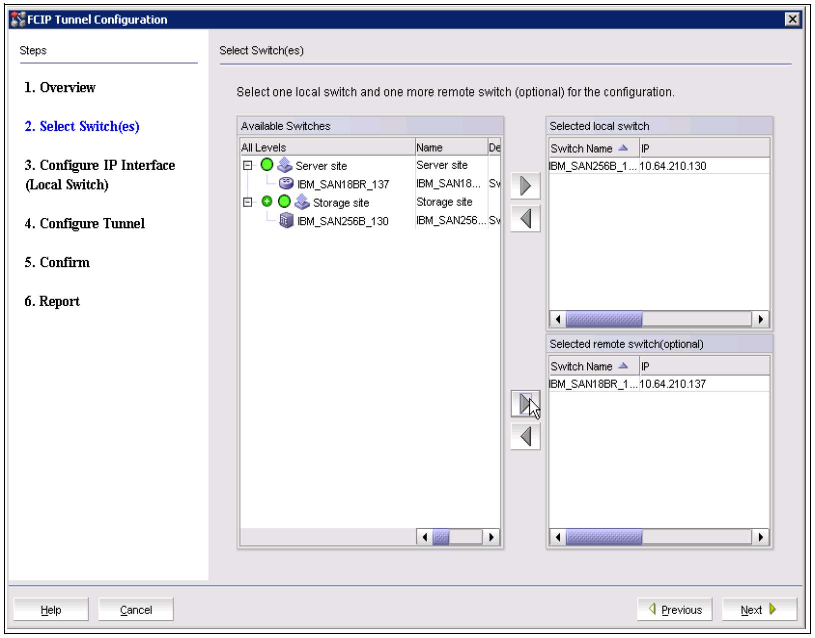
Overview

Configure an FCIP tunnel allows you to connect remote fabrics for purpose such as remote backup and disaster recovery.

It is recommended that there is a physical connection between two FCIP endpoints so that the system can verify the IP connectivity and suggest the optimal configuration values,e.g. MTU size and maximum bandwidth.

Figure 10-22 Step 1: Overview window

2. Select the participating switches (SAN routers) by moving them to the "Selected" panes in the "Step 2: Select Switch(es)" window (Figure 10-23). Our local switch is Storage site B with the SAN256B director switch, and the remote switch is the SAN18B-R switch at Server site A. Click **Next**.



FCIP Tunnel Configuration

Steps

1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure Tunnel
5. Confirm
6. Report

Select Switch(es)

Select one local switch and one more remote switch (optional) for the configuration.

Available Switches

All Levels	Name	De
Server site	Server site	
IBM_SAN18BR_137	IBM_SAN18...	Sv
Storage site	Storage site	
IBM_SAN256B_130	IBM_SAN256...	Sv

Selected local switch

Switch Name	IP
IBM_SAN256B_1...	10.64.210.130

Selected remote switch(optional)

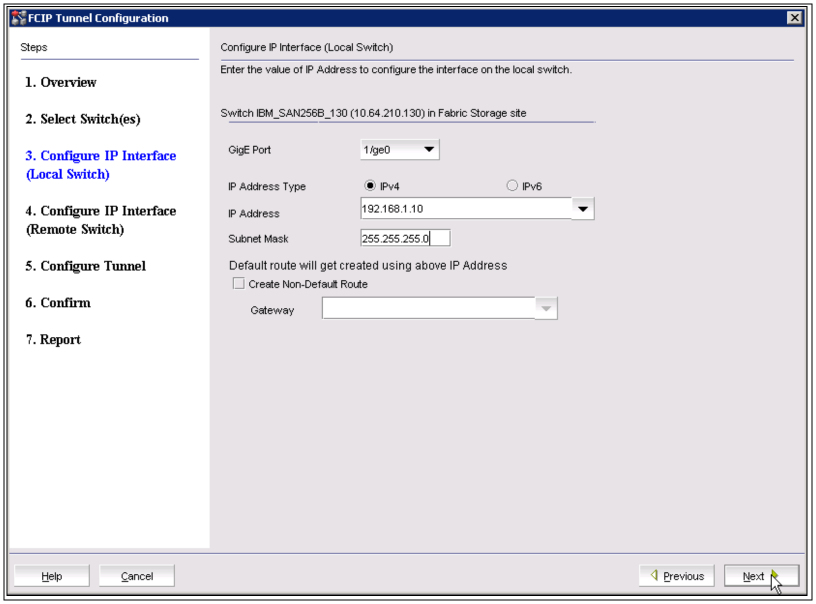
Switch Name	IP
IBM_SAN18BR_1...	10.64.210.137

Figure 10-23 Step 2: Select switch(es) window

3. Configure the IP address of the local GigE port in the “Step 3: Configure Local IP Interface” window (Figure 10-24). This is `192.168.1.10` for the GigE port ge0 on blade 1 of the SAN256B switch, which is indicated by the port name `1/ge0`.

   Because this is a direct connection, we do not configure the default gateway, which is selected automatically. In a real-life situation, a non-default gateway probably will have to be configured.

   Click **Next**.



FCIP Tunnel Configuration

Steps

1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure IP Interface (Remote Switch)
5. Configure Tunnel
6. Confirm
7. Report

Configure IP Interface (Local Switch)

Enter the value of IP Address to configure the interface on the local switch.

Switch IBM_SAN256B_130 (10.64.210.130) in Fabric Storage site

GigE Port: 1/ge0

IP Address Type: ● IPv4 ○ IPv6

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

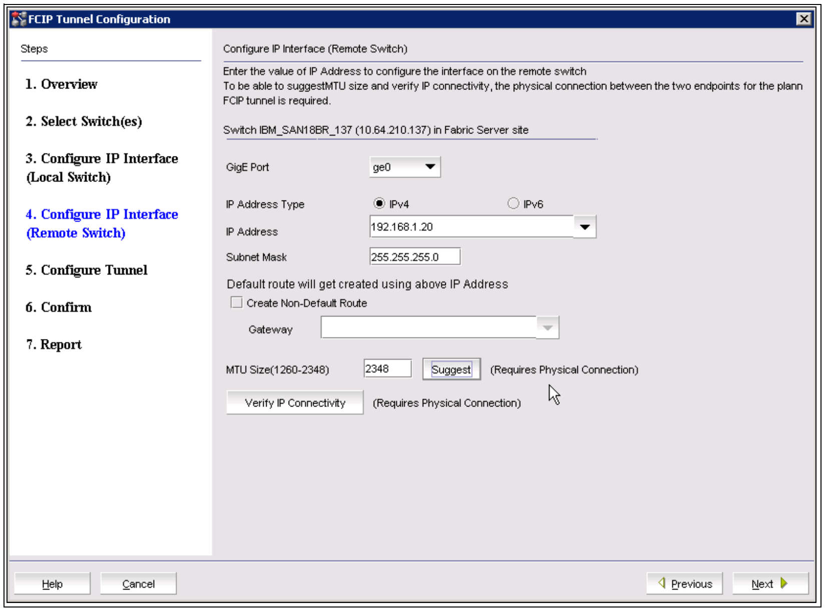
Default route will get created using above IP Address

□ Create Non-Default Route

Gateway:

Figure 10-24 Step 3: Configure the local IP Interface (Local Switch) window

4. Configure the IP address in the “Step 4: Configure IP Interface (Remote Switch) window (Figure 10-25). We use `192.168.1.20` in our setup.



FCIP Tunnel Configuration

Steps

1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure IP Interface (Remote Switch)
5. Configure Tunnel
6. Confirm
7. Report

Configure IP Interface (Remote Switch)

Enter the value of IP Address to configure the interface on the remote switch
To be able to suggestMTU size and verify IP connectivity, the physical connection between the two endpoints for the plann
FCIP tunnel is required.

Switch IBM_SAN18BR_137 (10.64.210.137) in Fabric Server site

GigE Port: ge0

IP Address Type: ● IPv4 ○ IPv6

IP Address: 192.168.1.20

Subnet Mask: 255.255.255.0

Default route will get created using above IP Address

□ Create Non-Default Route

Gateway:

MTU Size(1260-2348): 2348 Suggest (Requires Physical Connection)

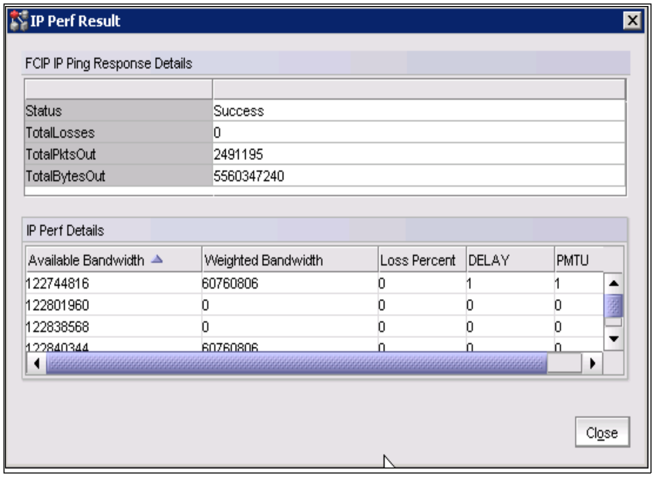
Verify IP Connectivity (Requires Physical Connection)

Figure 10-25 Step 4: Configure IP Interface (Remote Switch) window

At this point, we have two other options:

– Suggest MTU Size

  By clicking **Suggest**, the physical link can suggest an MTU size. The standard MTU size is 1500. Although a larger MTU size might improve performance, it requires that every part of the network supports jumbo frames. Figure 10-26 shows the IP Perf Result window.



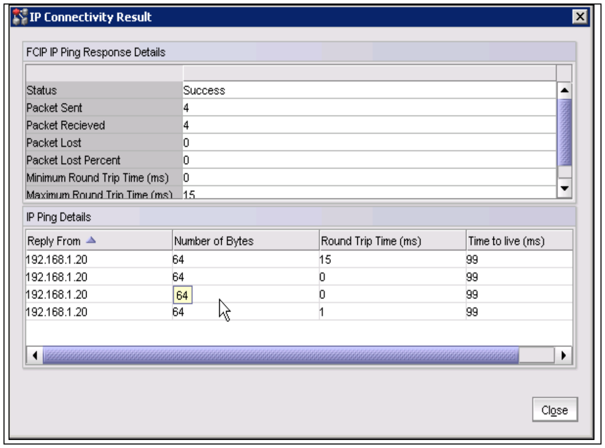
Status	Success
TotalLosses	0
TotalPktsOut	2491195
TotalBytesOut	5560347240

Available Bandwidth	Weighted Bandwidth	Loss Percent	DELAY	PMTU
122744816	60760806	0	1	1
122801960	0	0	0	0
122838568	0	0	0	0
122840344	60760806	0	0	0

Figure 10-26 Suggest MTU size result IP Perf Result window

– Verify IP Connectivity

  By clicking **Verify IP Connectivity**, the physical link is checked by configuring IP addresses on the interfaces and executing a **`ping`** command. After the test, the interfaces are deconfigured and the test result is displayed. Figure 10-27 shows the IP Connectivity Result window.

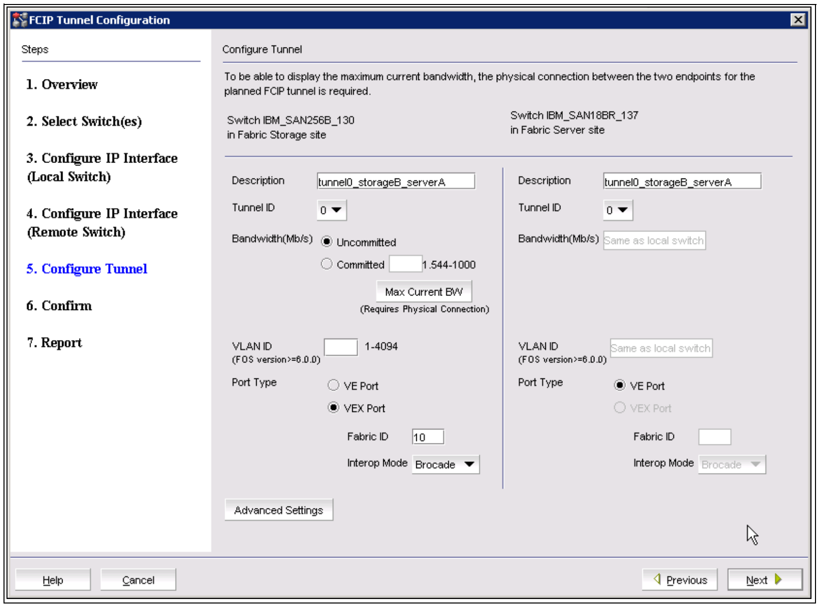


Status	Success
Packet Sent	4
Packet Recieved	4
Packet Lost	0
Packet Lost Percent	0
Minimum Round Trip Time (ms)	0
Maximum Round Trip Time (ms)	15

Reply From	Number of Bytes	Round Trip Time (ms)	Time to live (ms)
192.168.1.20	64	15	99
192.168.1.20	64	0	99
192.168.1.20	64	0	99
192.168.1.20	64	1	99

Figure 10-27 Verify IP Connectivity result window

5. Configure a description of the tunnel and a tunnel ID, on each of the participating switches in the “Step 5: Configure Tunnel” window (Figure 10-28). At this step we also configure whether the local port will be a VE port or a VEX port.



FCIP Tunnel Configuration

Steps

1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure IP Interface (Remote Switch)
5. Configure Tunnel
6. Confirm
7. Report

Configure Tunnel

To be able to display the maximum current bandwidth, the physical connection between the two endpoints for the planned FCIP tunnel is required.

Switch IBM_SAN256B_130
in Fabric Storage site

Description: tunnel0_storageB_serverA
Tunnel ID: 0
Bandwidth(Mb/s): ● Uncommitted
○ Committed 1.544-1000
Max Current BW
(Requires Physical Connection)
VLAN ID (FOS version>=6.0.0): 1-4094
Port Type: ○ VE Port
● VEX Port
Fabric ID: 10
Interop Mode: Brocade

Switch IBM_SAN18BR_137
in Fabric Server site

Description: tunnel0_storageB_serverA
Tunnel ID: 0
Bandwidth(Mb/s): Same as local switch
VLAN ID (FOS version>=6.0.0): Same as local switch
Port Type: ● VE Port
○ VEX Port
Fabric ID:
Interop Mode: Brocade

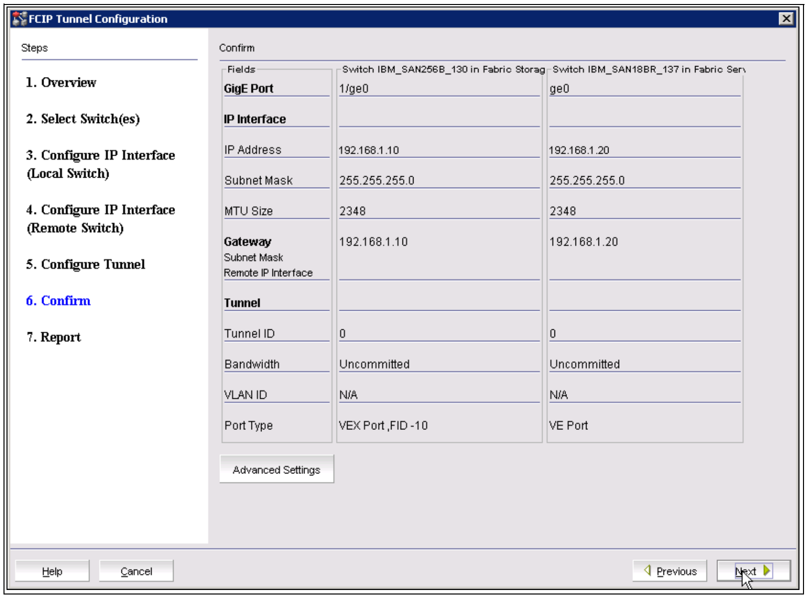
Figure 10-28 Step 5: Configure Tunnel window

Creating two VE ports causes the two SANs to merge into a single fabric. This approach might not be preferred over an IP link, and in our scenario, merging fabrics is not allowed, so we choose VEX port. Our choice prevents the fabrics from merging. When **VEX port** is selected, we must configure Interop mode (**Brocade**) and define a fabric ID. We assign **10** to our fabric ID.

The tunnel ID defines which virtual port we are using on the switch. This parameter is not important to know when you are using DCFM to configure the FCIP tunnel, but as explained later, this parameter is important to understand when we use CLI to configure the FCIP tunnel.

Click **Next**.

6. Choices made in previous steps are shown in the “Step 6: Confirm” window (Figure 10-29). Confirm these before the tunnel is created.



FCIP Tunnel Configuration

Steps

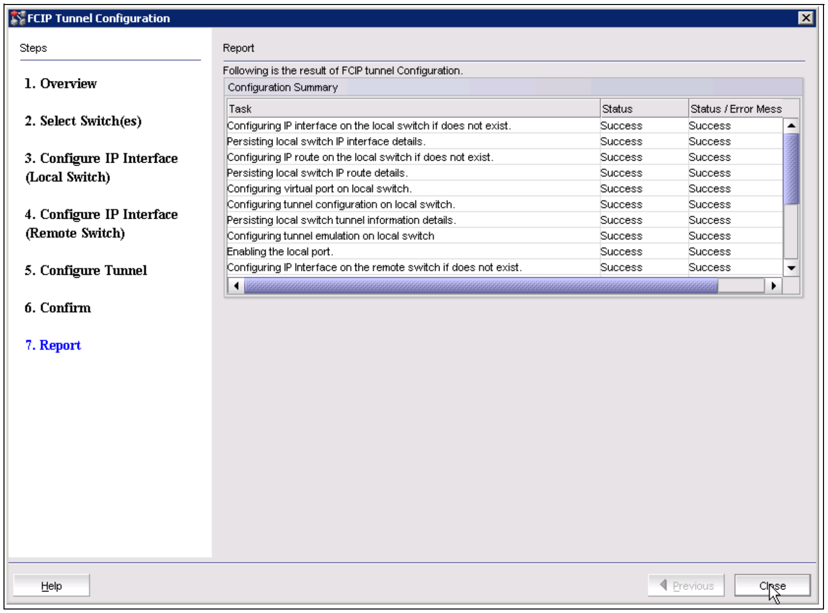
1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure IP Interface (Remote Switch)
5. Configure Tunnel
6. Confirm
7. Report

Confirm

Fields	Switch IBM_SAN256B_130 in Fabric Storag	Switch IBM_SAN18BR_137 in Fabric Serv
GigE Port	1/ge0	ge0
IP Interface		
IP Address	192.168.1.10	192.168.1.20
Subnet Mask	255.255.255.0	255.255.255.0
MTU Size	2348	2348
Gateway Subnet Mask Remote IP Interface	192.168.1.10	192.168.1.20
Tunnel		
Tunnel ID	0	0
Bandwidth	Uncommitted	Uncommitted
VLAN ID	N/A	N/A
Port Type	VEX Port ,FID -10	VE Port

Figure 10-29   Step 6: Confirm window

DCFM creates the tunnel and the result of the process is listed in the Report window (Figure 10-30).



FCIP Tunnel Configuration
Steps
1. Overview
2. Select Switch(es)
3. Configure IP Interface (Local Switch)
4. Configure IP Interface (Remote Switch)
5. Configure Tunnel
6. Confirm
7. Report
Help
Previous
Close

Report

Following is the result of FCIP tunnel Configuration.

Configuration Summary

Task	Status	Status / Error Mess
Configuring IP interface on the local switch if does not exist.	Success	Success
Persisting local switch IP interface details.	Success	Success
Configuring IP route on the local switch if does not exist.	Success	Success
Persisting local switch IP route details.	Success	Success
Configuring virtual port on local switch.	Success	Success
Configuring tunnel configuration on local switch.	Success	Success
Persisting local switch tunnel information details.	Success	Success
Configuring tunnel emulation on local switch	Success	Success
Enabling the local port.	Success	Success
Configuring IP Interface on the remote switch if does not exist.	Success	Success

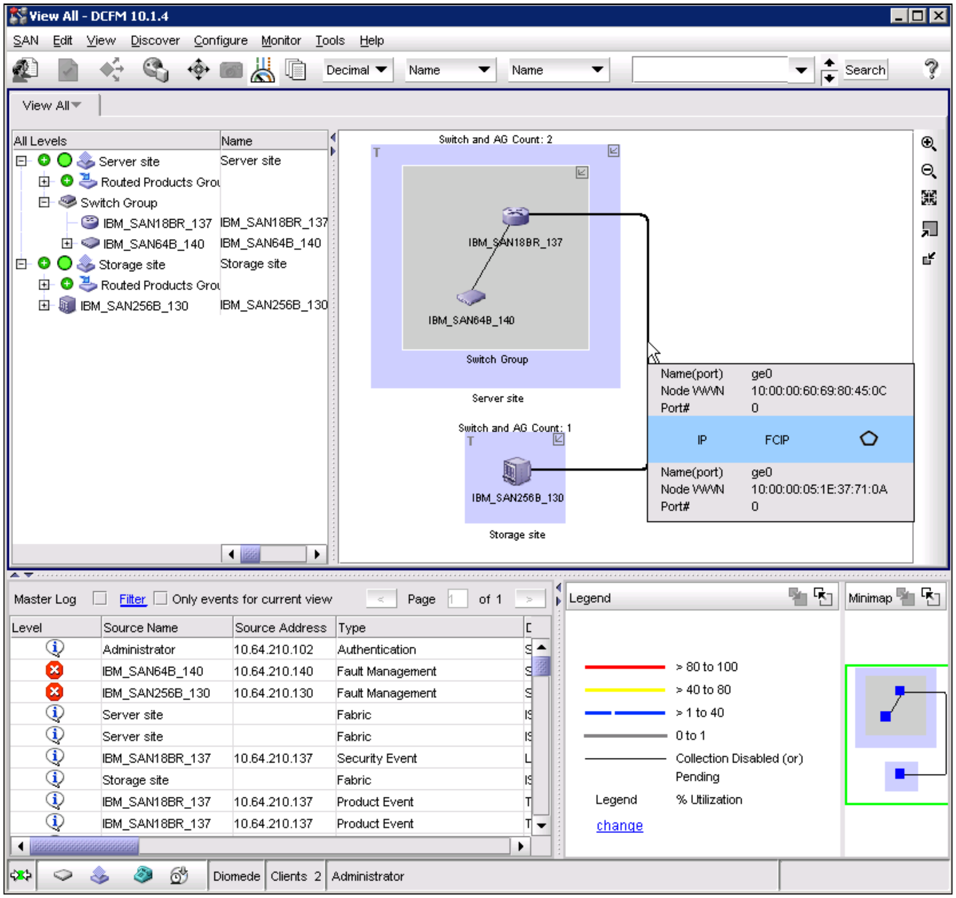
Figure 10-30 the Report window, step 7

Our FCIP tunnel between server A and storage B is now created and ready for use by the LSAN zones.

10.4.2 Checking the FCIP tunnel

The main window of DCFM now shows a link between the routers in our storage site and the server site.

Figure 10-31 now shows a line between the two switches where we have configured a route.



All Levels	Name
Server site	Server site
Routed Products Grou	
Switch Group	
IBM_SAN18BR_137	IBM_SAN18BR_137
IBM_SAN64B_140	IBM_SAN64B_140
Storage site	Storage site
Routed Products Grou	
IBM_SAN256B_130	IBM_SAN256B_130

Name(port)	ge0	
Node WWN	10:00:00:60:69:80:45:0C	
Port#	0	
IP	FCIP	⬠
Name(port)	ge0	
Node WWN	10:00:00:05:1E:37:71:0A	
Port#	0	

□ Only events for current view Page 1 of 1

Level	Source Name	Source Address	Type	D
ⓘ	Administrator	10.64.210.102	Authentication	S
✖	IBM_SAN64B_140	10.64.210.140	Fault Management	S
✖	IBM_SAN256B_130	10.64.210.130	Fault Management	S
ⓘ	Server site		Fabric	IS
ⓘ	Server site		Fabric	IS
ⓘ	IBM_SAN18BR_137	10.64.210.137	Security Event	L
ⓘ	Storage site		Fabric	IS
ⓘ	IBM_SAN18BR_137	10.64.210.137	Product Event	T
ⓘ	IBM_SAN18BR_137	10.64.210.137	Product Event	T

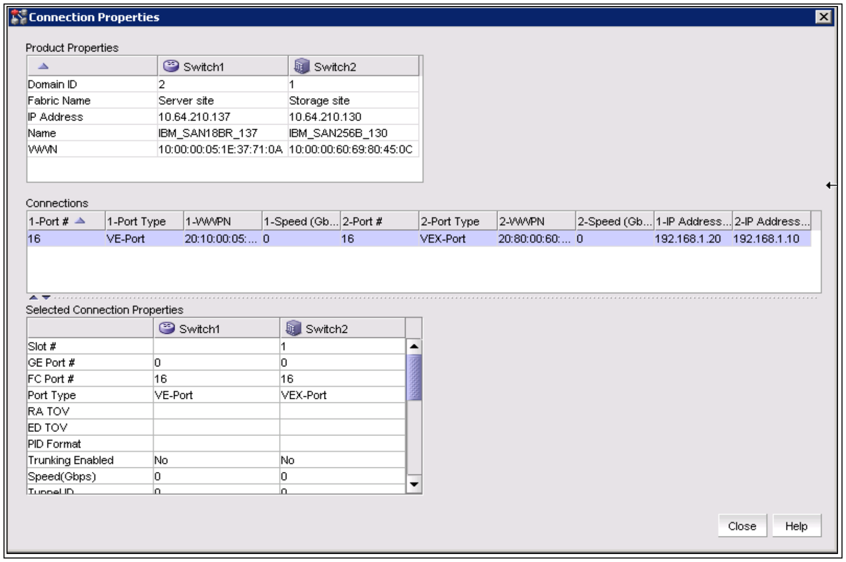
Legend	% Utilization
🟥	> 80 to 100
🟨	> 40 to 80
🟦	> 1 to 40
⬜	0 to 1
—	Collection Disabled (or) Pending

change

Figure 10-31 DCFM main window shows a link between routed switches

By hovering our cursor over the FCIP link, DCFM shows properties for this connection.

Figure 10-32 shows properties for our FCIP connection when we double-click the connection.



Product Properties

	Switch1	Switch2
Domain ID	2	1
Fabric Name	Server site	Storage site
IP Address	10.64.210.137	10.64.210.130
Name	IBM_SAN18BR_137	IBM_SAN256B_130
WWN	10:00:00:05:1E:37:71:0A	10:00:00:60:69:80:45:0C

Connections

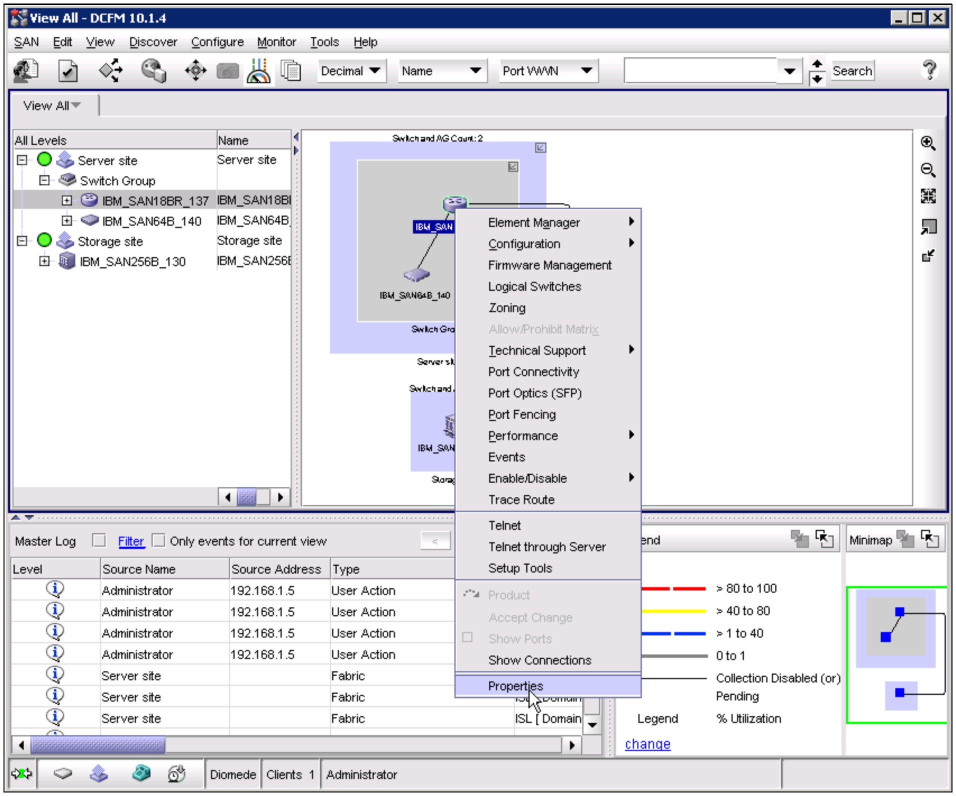
1-Port #	1-Port Type	1-WWPN	1-Speed (Gb...	2-Port #	2-Port Type	2-WWPN	2-Speed (Gb...	1-IP Address...	2-IP Address...
16	VE-Port	20:10:00:05:...	0	16	VEX-Port	20:80:00:60:...	0	192.168.1.20	192.168.1.10

Selected Connection Properties

	Switch1	Switch2
Slot #		1
GE Port #	0	0
FC Port #	16	16
Port Type	VE-Port	VEX-Port
RA TOV		
ED TOV		
PID Format		
Trunking Enabled	No	No
Speed(Gbps)	0	0
Tunnel ID	0	0

Figure 10-32 FCIP connection properties

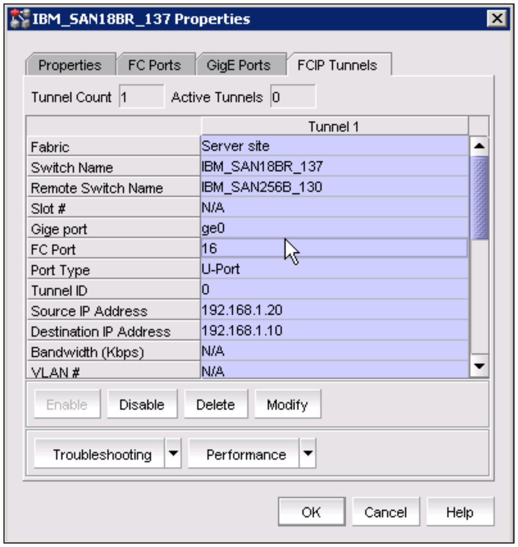
Figure 10-33 shows how to access properties for FCIP tunnels and GigE ports. Right-click the switch where you want to manage the ports and tunnels, and click **Properties**.



Level	Source Name	Source Address	Type
ⓘ	Administrator	192.168.1.5	User Action
ⓘ	Administrator	192.168.1.5	User Action
ⓘ	Administrator	192.168.1.5	User Action
ⓘ	Administrator	192.168.1.5	User Action
ⓘ	Server site		Fabric
ⓘ	Server site		Fabric
ⓘ	Server site		Fabric

Figure 10-33 Accessing properties for our FCIP tunnel and GigE ports

Figure 10-34 shows the properties for our FCIP tunnel. From here, the tunnel can be disabled, deleted, or modified.



Tunnel Count 1 Active Tunnels 0

	Tunnel 1
Fabric	Server site
Switch Name	IBM_SAN18BR_137
Remote Switch Name	IBM_SAN256B_130
Slot #	N/A
Gige port	ge0
FC Port	16
Port Type	U-Port
Tunnel ID	0
Source IP Address	192.168.1.20
Destination IP Address	192.168.1.10
Bandwidth (Kbps)	N/A
VLAN #	N/A

Figure 10-34 Properties for our FCIP tunnel

Our FCIP tunnel appears functional, so we are now ready to continue with creating our LSAN zones.

10.4.3 Creating LSAN zones

An LSAN zone consists of zones in two or more edge or backbone fabrics that contain the same devices. LSAN zones essentially provide device connectivity between fabrics without forcing you to merge those fabrics.

Although an LSAN zone is managed using the same tools as any other zone, two behaviors distinguish an LSAN zone from a conventional zone:

- A required naming convention. The name of an LSAN zone begins with the `LSAN_` prefix. The LSAN zone name is case-insensitive, so the LSAN zone name can start with either lsan_, LSAN_, Lsan_, and so on.
- Members must be identified by their port worldwide name (WWN) because port IDs are not necessarily unique across fabrics.

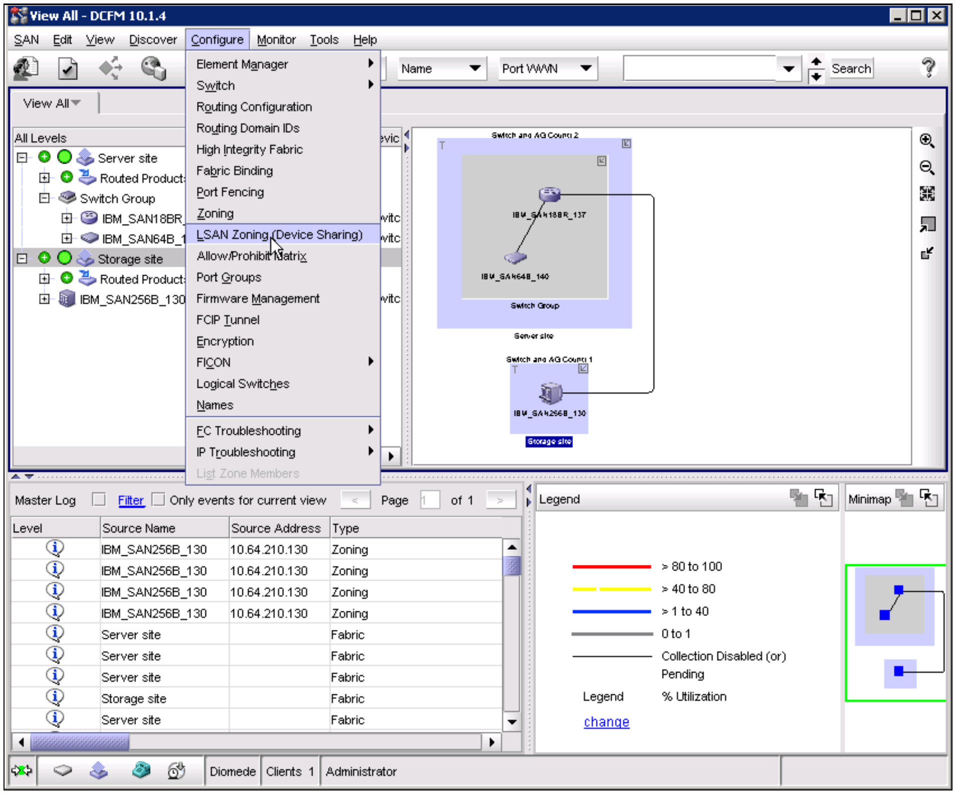
Because we are creating two identical zone configurations on each side of our tunnel, and because these must contain only WWNs, traditional Web Tools zoning cannot pick the WWNs from two unmerged fabrics. Therefore, we must manually type in the WWNs; if we are using traditional Web Tools to create our LSAN zones, this process might be slow.

DCFM provides a tool for creating the LSAN zones, where the WWNs of unmerged fabrics can be picked and added to an LSAN zone. This tool is also able to apply this zone to both the participating fabrics. This process makes DCFM a convenient tool for creating LSAN zones.

Perform the following steps to create an LSAN zone”

1. Highlight the local switch where we created the VEX port, and then we select **LSAN Zoning (Device Sharing)** from the Configure menu.

   Figure 10-35 shows the DCFM main window where we start the LSAN zoning tool.



Level	Source Name	Source Address	Type
ⓘ	IBM_SAN256B_130	10.64.210.130	Zoning
ⓘ	IBM_SAN256B_130	10.64.210.130	Zoning
ⓘ	IBM_SAN256B_130	10.64.210.130	Zoning
ⓘ	IBM_SAN256B_130	10.64.210.130	Zoning
ⓘ	Server site		Fabric
ⓘ	Server site		Fabric
ⓘ	Server site		Fabric
ⓘ	Storage site		Fabric
ⓘ	Server site		Fabric

Figure 10-35 DCFM main window

The Zoning window opens, shown in Figure 10-36.

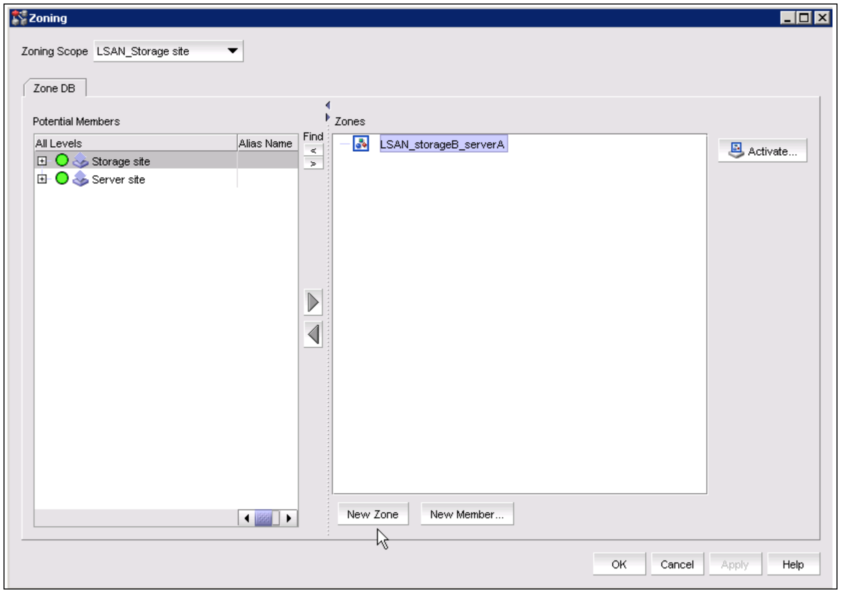


Figure 10-36 LSAN zoning window

2. From the Zoning Scope menu, we select **LSAN_Storage site**.
3. As shown in Figure 10-37, right-click the fabric and select **Show Connected End Devices** to expand the fabrics and make DCFM show WWNs.

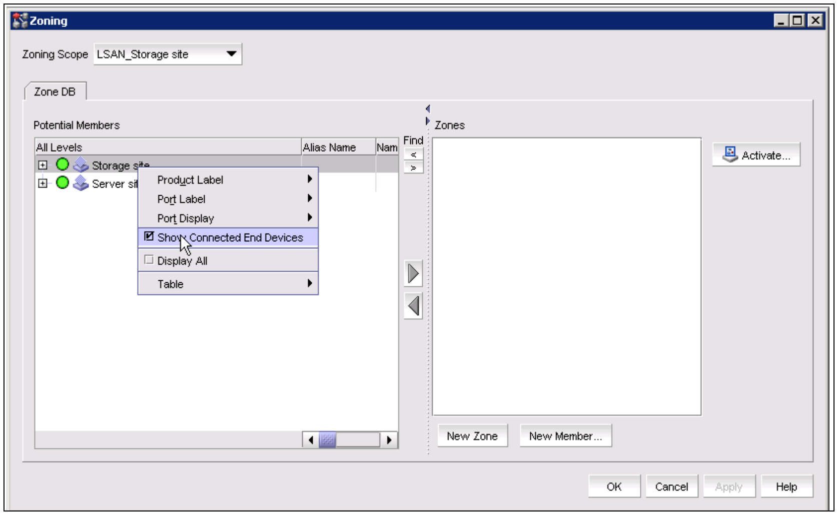
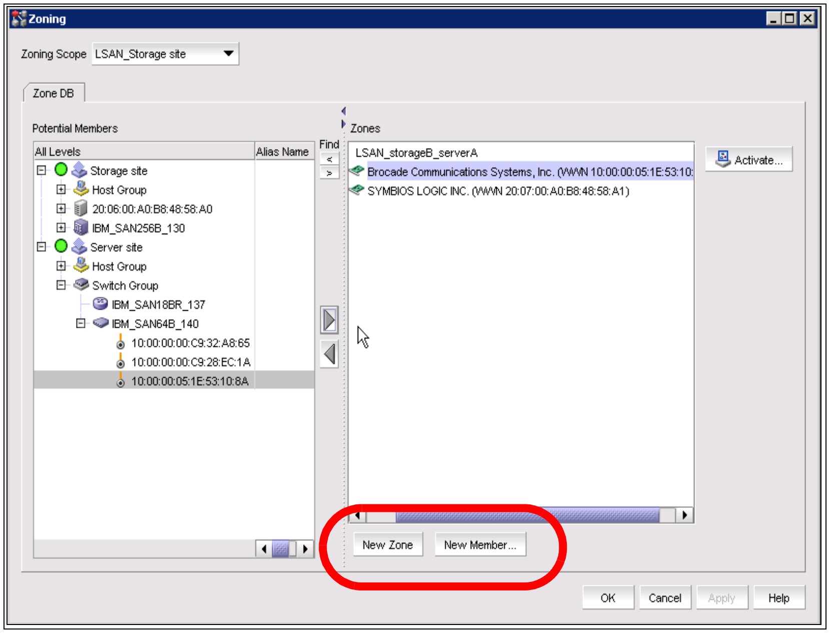


Figure 10-37 Making DCFM show WWNs

Figure 10-38 show how to create a new LSAN zone.



Zoning Scope LSAN_Storage site

LSAN_storageB_serverA
Brocade Communications Systems, Inc. (WWN 10:00:00:05:1E:53:10:
SYMBIOS LOGIC INC. (WWN 20:07:00:A0:B8:48:58:A1)

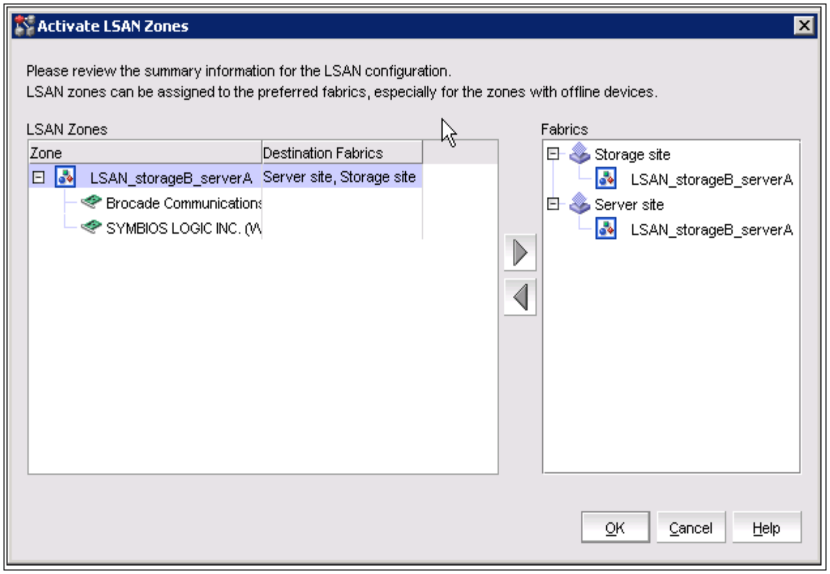
Figure 10-38 Create a new LSAN zone

4. In the Zones pane (on the right), click **New Zone**. Give the new zone the name `LSAN_storageB_serverA`.
5. From the left pane, select and add the two WWNs we need in our zone. They represent the WWN of the server HBA, and the WWN of the storage controller.

   Because DCFM can pick WWNs from two unmerged fabrics, avoid typing in WWNs manually. If for some reason we want to do that, we click **New Member**.

6. Click **Activate** to open the Activate LSAN Zones window.

   Figure 10-39 shows the Activate LSAN Zones window. From here, you can select which zones to activate on which fabrics, as shown in the Fabrics pane. The figure shows that our LSAN zone is to be activated at the Server site and the Storage site fabrics.



Activate LSAN Zones

Please review the summary information for the LSAN configuration.
LSAN zones can be assigned to the preferred fabrics, especially for the zones with offline devices.

LSAN Zones

Zone	Destination Fabrics
⊟ LSAN_storageB_serverA	Server site, Storage site
Brocade Communications	
SYMBIOS LOGIC INC. (W	

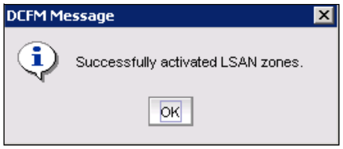
Fabrics

- ⊟ Storage site
  - LSAN_storageB_serverA
- ⊟ Server site
  - LSAN_storageB_serverA

Figure 10-39 LSAN zone activation

   Click **OK**.

   DCFM returns the message shown in Figure 10-40. Click **OK**.

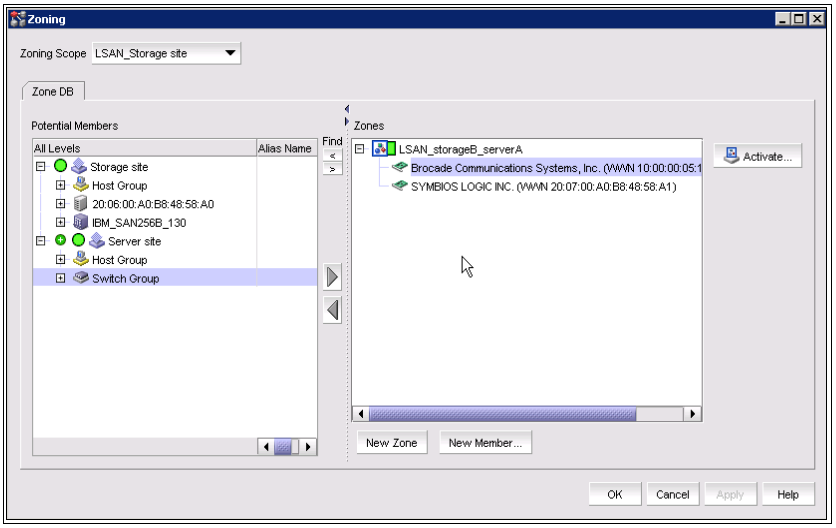


DCFM Message

Successfully activated LSAN zones.

Figure 10-40 DCFM message

Figure 10-41 shows that the LSAN zone is active; the color green indicating it is an active LSAN zone.



Zoning Scope: LSAN_Storage site

Potential Members:

- Storage site
  - Host Group
  - 20:06:00:A0:B8:48:58:A0
  - IBM_SAN256B_130
- Server site
  - Host Group
  - Switch Group

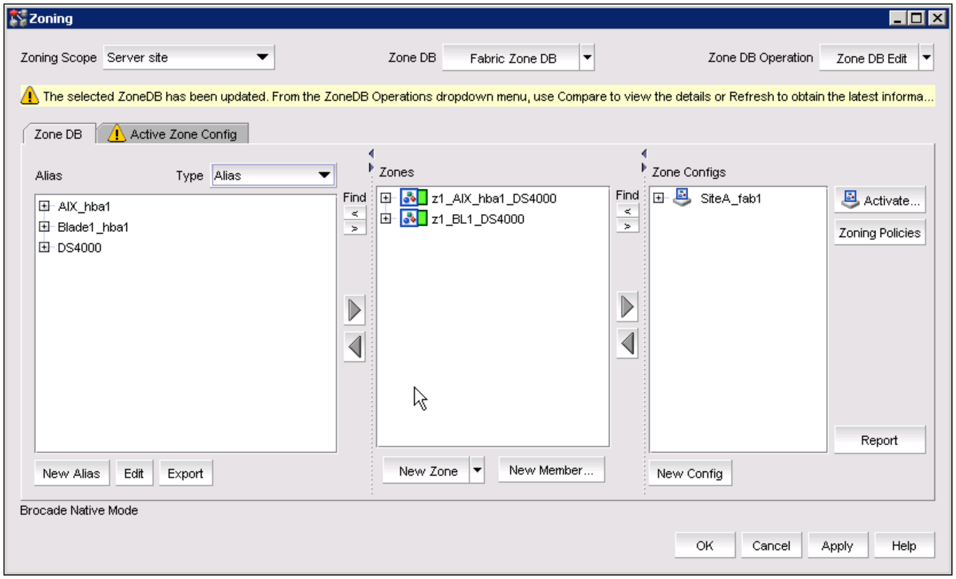
Zones:

- LSAN_storageB_serverA
  - Brocade Communications Systems, Inc. (WWN 10:00:00:05:1
  - SYMBIOS LOGIC INC. (WWN 20:07:00:A0:B8:48:58:A1)

Figure 10-41 Active LSAN zone

7. From the Zoning Scope menu, select either **Server site** or **Storage site**. The ordinary DCFM zoning window opens.

Figure 10-42 shows that zoning has changed.



Zoning Scope: Server site

Zone DB: Fabric Zone DB

Zone DB Operation: Zone DB Edit

The selected ZoneDB has been updated. From the ZoneDB Operations dropdown menu, use Compare to view the details or Refresh to obtain the latest informa...

Type: Alias

Alias:
- AIX_hba1
- Blade1_hba1
- DS4000

Zones:
- z1_AIX_hba1_DS4000
- z1_BL1_DS4000

Zone Configs:
- SiteA_fab1

Brocade Native Mode

Figure 10-42 Zoning has changed

Figure 10-43 shows the refreshed DCFM zoning window where the new LSAN zones are now included in the zoning configuration for both sides.

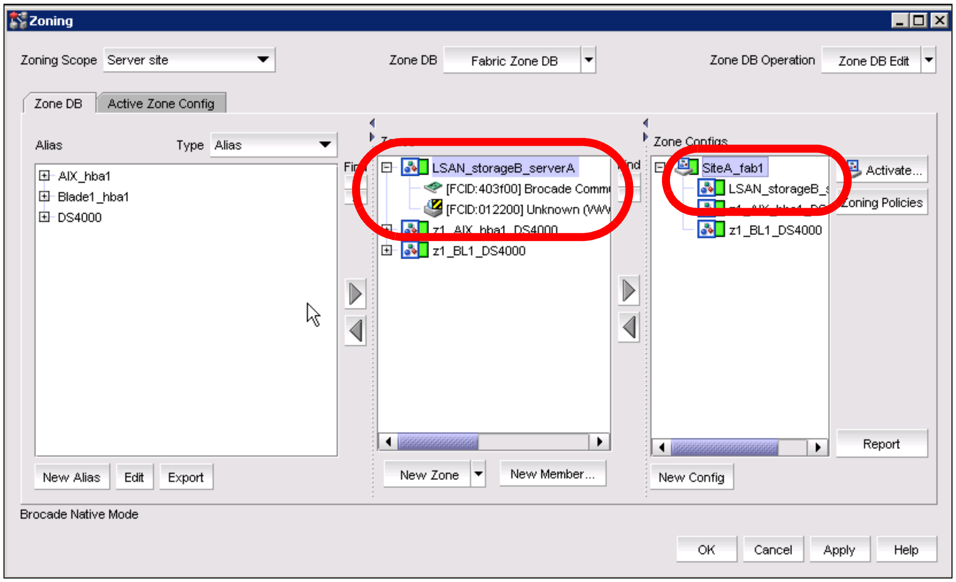


Figure 10-43 DCFM zoning window

Our LSAN zones are now active, and we are ready to check the server, which at this point we should be able to see our two DS4700 LUNs. Before checking the server, we demonstrate how to create the FCIP tunnel by using the CLI.

10.5 Configuring FCIP using the CLI

In this section, we show how to create FCIP tunnels and LSAN zones using CLI.

> **Note:** For further details on the FCIP-related commands and syntax, refer to the Brocade document, *Fabric OS Command Reference Manual Supporting Fabric OS 6.2.0*, which can be obtained from the Brocade Technical Resource Center.
>
> You cannot create FCIP tunnels using Web Tools because it is an element manager. Although viewing FCIP configurations is possible in Web Tools, creating FCIP must be done using DCFM or the CLI.

10.5.1 Configuring the FCIP tunnel

When working with the CLI, knowing which ports on the switch refer to the tunnels we create is important. For each GigE port, creating eight tunnels is possible. These eight tunnels are each represented on the switch by a virtual switch port. In our example, we use GigE port ge0 and we configure the tunnel ID to be 0 (zero), which means that 16 is the virtual port that we are configuring for.

Table 10-2 shows the port-to-tunnel ID relationship.

Table 10-2 Port-to-tunnel ID relationship

Port	ge0 tunnel ID	Port	ge1 tunnel ID
Port 16	0	Port 24	0
Port 17	1	Port 25	1
Port 18	2	Port 26	2
Port 19	3	Port 27	3
Port 20	4	Port 28	4
Port 21	5	Port 29	5
Port 22	6	Port 30	6
Port 23	7	Port 31	7

Configuring the storage side

First, logon to our SAN256B director and configure the storage side of the FCIP tunnel. Begin with the VEX port side to make sure no accidental fabric-merge takes place. That could happen if we were to configure both sides as VE ports.

In Example 10-5 on page 237, we are configuring the virtual tunnel port 1/16 as being a VEX port. This represents tunnel ID 0, on the ge0 interface, on blade 1, in the SAN256B director switch.

Example 10-5 Creating the VEX port

```
IBM_SAN256B_130:admin> portdisable 1/16
IBM_SAN256B_130:admin> portcfgvexport 1/16 -a 1 -f 10 -d 1
IBM_SAN256B_130:admin> portenable 1/16
IBM_SAN256B_130:admin> portshow 1/16
portName:
portHealth: OFFLINE

Authentication: None

EX_Port Mode:   Enabled
Fabric ID:      10
Front Phantom:  state = Not OK  Pref Dom ID: 1
Fabric params:  R_A_TOV: 0      E_D_TOV: 0      PID fmt: auto

Authentication Type: None
Hash Algorithm: N/A
DH Group: N/A
Edge fabric's primary wwn: N/A
Edge fabric's version stamp: N/A

portDisableReason: None
portCFlags: 0x1
portFlags: 0x4001        PRESENT VIRTUAL U_PORT EX_PORT LED
portType:  12.0
portState: 2    Offline
portPhys:  6    In_Sync
portScn:   2    Offline
port generation number:    46
portId:    018000
portIfId:    43120029
portWwn:   20:80:00:60:69:80:45:0c
portWwn of device(s) connected:

Distance:  normal
Port part of other ADs: No

IBM_SAN256B_130:admin>
```

The port must be disabled prior to setting VEX_Port attributes. The port must be enabled before the port can become active following VEX_Port parameter changes. Use the **portDisable** or **portEnable** command to disable or enable the port.

Currently, our port is an EX_PORT, and it is offline because we did not configure the other side of the FCIP tunnel.

Our **`portcfgvexport`** command uses the following arguments:

`portcfgvexport` *`1/16 -a 1 -f 10 -d 1`*

Where:

1/16	The virtual port for tunnel 0, port ge0
-a 1	Enables the port as a VEX port
-f 10	Uses 10 as the fabric ID
-d 1	Uses 1 as domain ID

The fabric ID and domain ID should not be confused with the FIDs for virtual fabrics or the switch domain ID for a switch. From a routing perspective, each route must be configured with a fabric ID and a domain ID. The fabric ID must be the same for every router port that is connected to the same edge fabric, and different for every edge fabric.

Configure and enable the virtual tunnel port 1/16. In a real-life scenario, you might want to wait before doing that until the final configuration steps of both sides of the tunnel. Waiting enables you to review the configuration before bringing the configuration online, which could prevent undesired behavior, such as an accidental merging of fabrics.

> **Note:** To avoid undesired behavior, disable the GigE ports and virtual ports, until you want the newly created FCIP tunnel to become active.

Create an IP address on the GigE port on blade 1 port ge0 as shown in Example 10-6.

Example 10-6 creating the IP interface

```
IBM_SAN256B_130:admin> portcfg ipif 1/ge0 create 192.168.1.10
255.255.255.0 2348
WARNING: You are trying to configure MTU size greater than 1500.
       Please make sure that all devices in your IP
       network can support Max Ethernet Size frames
       You can also use cli "portcmd --ipperf" to
       find out the actual PMTU.
Operation Succeeded

IBM_SAN256B_130:admin> portshow ipif 1/ge0

Slot: 1 Port: ge0
Interface IP Address      NetMask         MTU
----------------------------------------------
    0     192.168.1.10    255.255.255.0   2348

IBM_SAN256B_130:admin>
```

Our **portcfg** command uses the following arguments:

portcfg ipif *1/ge0* **create** *192.168.1.10 255.255.255.0 2348*

Where:

ipif	Configures an IP Interface
1/ge0	The port we are configuring
create	Creates an IP Interface
192.168.1.10	The IP address
255.255.255.0	The subnet mask
2348	MTU size (for IP network is 1500)

The allowed MTU range is 1260 - 2348. Set the value to 1500, which is the normal value in an Ethernet network. Some networks support jumbo frames (packets larger than 1500). If the network you are using supports jumbo frames, a value in the range of 1500 - 2348 can improve performance.

Note: All parts of the Ethernet network must be able to support jumbo frames if you are enabling an MTU size larger than 1500. Again, an MTU size larger than 1500 can improve performance.

In Example 10-7 we create the FCIP tunnel.

Example 10-7 Creating the FCIP tunnel

```
IBM_SAN256B_130:admin> portcfg fciptunnel 1/ge0 create 0 192.168.1.20
192.168.1.10 0 -d tunnel0_storageB_serverA
Operation Succeeded

IBM_SAN256B_130:admin> portshow fciptunnel 1/ge0 all

Slot: 1 Port: ge0
-------------------------------------------
        Tunnel ID 0
        Tunnel Description "tunnel0_storageB_serverA"
        Remote IP Addr 192.168.1.20
        Local IP Addr 192.168.1.10
        Remote WWN Not Configured
        Local WWN 10:00:00:60:69:80:45:0c
        Compression off
        Fastwrite off
        Tape Pipelining off
        Uncommitted bandwidth, minimum of 1000 Kbps (0.001000 Gbps)
        SACK on
        Min Retransmit Time 100
        Keepalive Timeout 10
        Max Retransmissions 8
        VC QoS Mapping off
        DSCP Marking (Control): 0, DSCP Marking (Data): 0
        VLAN Tagging Not Configured
        TCP Byte Streaming off
        Status : Inactive
        Connected Count: 10

IBM_SAN256B_130:admin>
```

While configuring the FCIP tunnel, we have the option of specifying the remote WWN with the `-n` option. If we do so only the switch with the specified WWN will be able to use the tunnel, which is a security measure. The switch WWN can be retrieved by using the **`switchshow`** command or the **`wwn`** command.

Our **portcfg** command uses the following arguments:

portcfg fciptunnel *1/ge0* **create** *0 192.168.1.20 192.168.1.10 0*
-d tunnel0_storageB_serverA

Where:

fciptunnel	Configures an FCIP tunnel
1/ge0	The port we are configuring
create	Creates an FCIP tunnel
0	The tunnel ID (range of 0 - 7 is possible)
192.168.1.20	The remote IP address (SAN18B-R port ge0)
192.168.1.10	The local IP address (SAN256B port 1/ge0)
0	The committed traffic rate: A value of 0 is an uncommitted tunnel.
-d tunnel0_storageB_serverA	A descriptive name of our tunnel

In Example 10-8, we create an IP route for our FCIP tunnel.

Example 10-8 Creating the IP route

```
IBM_SAN256B_130:admin> portcfg iproute 1/ge0 create 192.168.1.20
255.255.255.0 192.168.1.1 1
Route prefix address does not match netmask, host bits are set

IBM_SAN256B_130:admin> portshow iproute 1/ge0

Slot: 1 Port: ge0
IP Address      Mask           Gateway       Metric
----------------------------------------------------
192.168.1.0     255.255.255.0  192.168.1.10     0
----------------------------------------------------

COMMAND OUTPUT REMOVED FOR CLARITY

IBM_SAN256B_130:admin>
```

Our **portcfg** command uses the following arguments:

portcfg iproute *1/ge0* **create** *192.168.1.20 255.255.255.0 192.168.1.1 1*

Where:

iproute	Configures an IP route
1/ge0	The port we are configuring
create	Creates an IP Interface
192.168.1.20	The remote IP address (SAN18B-R port ge0)
255.255.255.0	The subnet mask
192.168.1.1	The default gateway
1	Metric: a low value encourages the use of the route

At this time, the **switchshow** command still shows port 1/16 as `Offline` because we have not yet configured the other side of the route. When the route becomes active, we expect port 1/16 to be a VEX port.

Configuring the server side

Next, we log on to our SAN18B-R router and configure the server side of our FCIP tunnel.

Look at the output from **switchshow** command, as in Example 10-9.

Example 10-9 Output from switchshow command

```
IBM_SAN18BR_137:admin> switchshow
switchName:     IBM_SAN18BR_137
.
.
 15  15   --    N4   No_Module
 16  16   --    --   Offline
 17  17   --    --   Offline         Disabled (Persistent)
.
.
 31  31   --    --   Offline         Disabled (Persistent)
     ge0  id    1G   Online    FCIP
     ge1  --    1G   No_Module FCIP  Disabled (Persistent)

COMMAND OUTPUT REMOVED FOR CLARITY

IBM_SAN18BR_137:admin>
```

Port 16 is the port that represents virtual tunnel 0. Port 16 is currently offline because no tunnel is active.

The server side is configured in a similar way as the storage side, and we will skip the details about each command. In Example 10-10, we create the IP interface.

Example 10-10 Creating the IP interface

```
IBM_SAN18BR_137:admin> portcfg ipif ge0 create 192.168.1.20
255.255.255.0 2348
WARNING: You are trying to configure MTU size greater than 1500.
       Please make sure that all devices in your IP
       network can support Max Ethernet Size frames
       You can also use cli "portcmd --ipperf" to
       find out the actual PMTU.
Operation Succeeded
IBM_SAN18BR_137:admin> portshow ipif ge0

Port: ge0
Interface IP Address      NetMask         MTU
----------------------------------------------
    0     192.168.1.20    255.255.255.0   2348

IBM_SAN18BR_137:admin>
```

In Example 10-11, we create the FCIP tunnel.

Example 10-11 Creating the FCIP tunnel

```
IBM_SAN18BR_137:admin> portcfg fciptunnel ge0 create 0 192.168.1.10
192.168.1.20 0 -d tunnel0_storageB_serverA
Operation Succeeded

IBM_SAN18BR_137:admin> portshow fciptunnel ge0 all

Port: ge0
-------------------------------------------
        Tunnel ID 0
        Tunnel Description "tunnel0_storageB_serverA"
        Remote IP Addr 192.168.1.10
        Local IP Addr 192.168.1.20
        Remote WWN Not Configured
        Local WWN 10:00:00:05:1e:37:71:0a
        Compression off
        Fastwrite off
        Tape Pipelining off
        Uncommitted bandwidth, minimum of 1000 Kbps (0.001000 Gbps)
        SACK on
        Min Retransmit Time 100
        Keepalive Timeout 10
        Max Retransmissions 8
        VC QoS Mapping off
        DSCP Marking (Control): 0, DSCP Marking (Data): 0
        VLAN Tagging Not Configured
        TCP Byte Streaming off
        Status : Inactive
        Connected Count: 10

IBM_SAN18BR_137:admin>
```

In Example 10-12, we create the IP route.

Example 10-12 creating the IP route

```
IBM_SAN18BR_137:admin> portshow iproute ge0

Port: ge0
IP Address      Mask            Gateway        Metric
-----------------------------------------------------
192.168.1.0     255.255.255.0   192.168.1.20     0
-----------------------------------------------------

COMMAND OUTPUT REMOVED FOR CLARITY

IBM_SAN18BR_137:admin>
```

We have now finished creating the FCIP tunnel. If the tunnel does not go online immediately after creating the route, try disabling the ge0 ports and then enabling them. Do not enable the virtual ports, or the GigE ports, before the configuration is finished and has been reviewed for accuracy.

Now, enable our FCIP tunnel, as shown in Example 10-13.

Example 10-13 Enabling the tunnel

```
IBM_SAN18BR_137:admin> portdisable ge0
IBM_SAN18BR_137:admin> portenable ge0
IBM_SAN18BR_137:admin> switchshow
switchName:     IBM_SAN18BR_137
.
.
 15  15   --    N4   No_Module
 16  16   --    --   Online          VE-Port  50:06:06:98:04:50:ce:0a ""
(downstream)

COMMAND OUTPUT REMOVED FOR CLARITY

IBM_SAN18BR_137:admin>
```

We check again, by using the **switchshow** command on the storage side as in Example 10-14.

Example 10-14 switchshow

```
IBM_SAN256B_130:admin> switchshow
switchName:     IBM_SAN256B_130
.
.
15    1   15   010f00   --    N4   No_Module Disabled (Persistent)
128    1   16   018000   --    --   Online          VEX-Port
10:00:00:05:1e:37:71:0a "IBM_SAN18BR_137" (fabric id = 10 )
VE-Port  50:00:51:e3:70:a4:5f:11 "fcr_xd_2_10"

COMMAND OUTPUT REMOVED FOR CLARITY

IBM_SAN256B_130:admin>
```

Our FCIP tunnel is now online and functional. The storage side has a VEX port and the server side has a VE port configured into the FCIP tunnel.

We can now create the LSAN zones needed to establish the connection from server to storage.

10.5.2 Creating LSAN zones

We described the concept of LSAN zones in 10.4.3, “Creating LSAN zones” on page 228. In this section, we create similar LSAN zones on each side (fabric) of the tunnel, each containing the WWN of the DS4700 storage controller and the WWN of the server HBA. In Example 10-15, we create the LSAN zone.

Example 10-15 Creating the LSAN zone

```
IBM_SAN18BR_137:admin> zonecreate lsan_storageB_serverA,
"10:00:00:05:1e:53:10:8a; 20:07:00:a0:b8:48:58:a1"

IBM_SAN18BR_137:admin> cfgadd SiteA_fab1, lsan_storageB_serverA

IBM_SAN18BR_137:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no, n): [no] y
Updating flash ...

IBM_SAN18BR_137:admin> cfgenable SiteA_fab1
```

```
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'SiteA_fab1' configuration  (yes, y, no, n): [no] y
zone config "SiteA_fab1" is in effect
Updating flash ...

IBM_SAN18BR_137:admin>
```

Either the **cfgshow** command or the **lsanzoneshow** command tells us how the LSAN zone is configured. The **-s** variable on the **lsanzoneshow** command tells us whether the WWN is currently present or is configured as in Example 10-16.

Example 10-16 cfgshow on SAN18B-R

```
IBM_SAN18BR_137:admin> cfgshow
Defined configuration:
 cfg:   SiteA_fab1
                z1_BL1_DS4000; z1_AIX_hba1_DS4000; lsan_storageB_serverA
 zone:  lsan_storageB_serverA
                10:00:00:05:1e:53:10:8a; 20:07:00:a0:b8:48:58:a1
 zone:  z1_AIX_hba1_DS4000
                64,20; 64,22
 zone:  z1_BL1_DS4000
                64,21; 64,22
 alias: AIX_hba1
                64,20
 alias: Blade1_hba1
                64,21
 alias: DS4000  64,22

Effective configuration:
 cfg:   SiteA_fab1
 zone:  lsan_storageB_serverA
                10:00:00:05:1e:53:10:8a
                20:07:00:a0:b8:48:58:a1
 zone:  z1_AIX_hba1_DS4000
                64,20
                64,22
 zone:  z1_BL1_DS4000
                64,21
                64,22

IBM_SAN18BR_137:admin>
```

In Example 10-17 we issue the **lsanzoneshow** command on the SAN256B.

Example 10-17 lsanzoneshow on SAN256B

```
IBM_SAN256B_130:admin> lsanzoneshow -s
Fabric ID: 1 Zone Name: lsan_storageB_serverA
        10:00:00:05:1e:53:10:8a  Imported
        20:07:00:a0:b8:48:58:a1  EXIST
Fabric ID: 10 Zone Name: lsan_storageB_serverA
        10:00:00:05:1e:53:10:8a  EXIST
        20:07:00:a0:b8:48:58:a1  Imported

IBM_SAN256B_130:admin>
```

In Example 10-18, we issue the **lsanzoneshow** command on the SAN18B-R.

Example 10-18 lsanzoneshow on SAN18B-R

```
IBM_SAN18BR_137:admin> lsanzoneshow -s
Fabric ID: 1 Zone Name: lsan_storageB_serverA
        10:00:00:05:1e:53:10:8a  EXIST
        20:07:00:a0:b8:48:58:a1  Configured

IBM_SAN18BR_137:admin>
```

Note: For further details about the zone command syntax, refer to the Brocade document, *Fabric OS Command Reference Manual Supporting Fabric OS 6.2.0*, which can be obtained from the Brocade Technical Resource Center.

We have now created our LSAN zones, and are ready to determine whether the server can see its DS4700 LUNs.

10.6 Finalizing the configuration

In this section, we show the steps we performed to finalize our configuration.

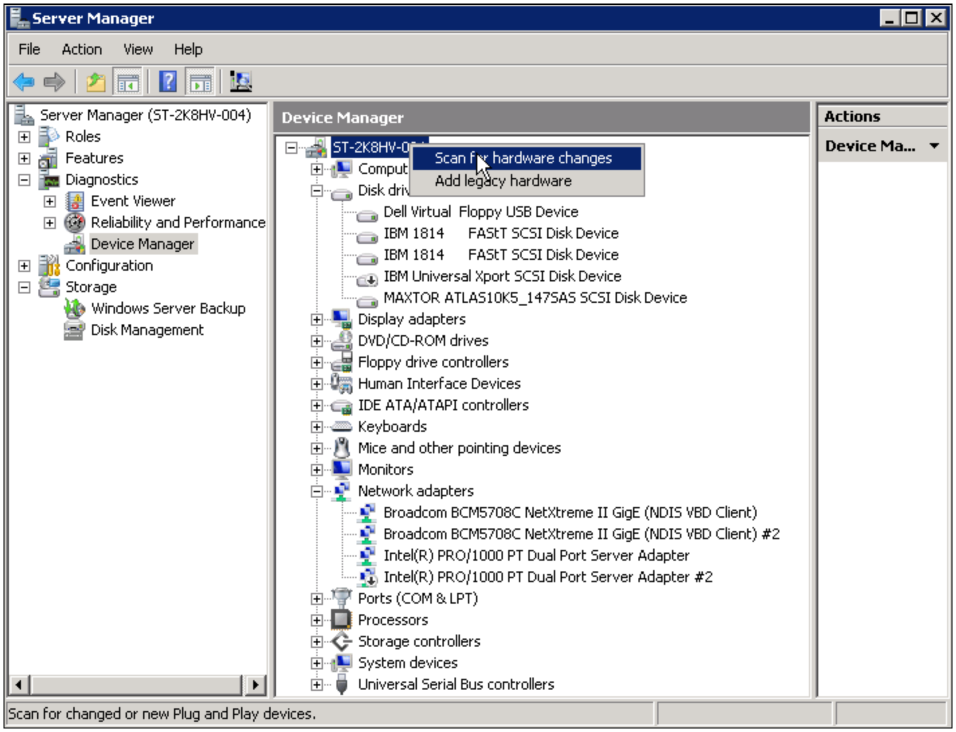
10.6.1 Checking the server for new disks

In the previous steps, we configured an FCIP tunnel and LSAN zones for a server in site A to access storage in site B. We demonstrated this procedure by using DCFM and the CLI.

Now, we check whether the server can see the disks presented from the DS4700. This is all done in Server Manager.

Perform the following steps to check the server for new disks:

1. Figure 10-44 shows the Microsoft Windows Server 2008 Device Manager where we scan for hardware changes by right-clicking the server name and selecting **Scan for hardware changes**.


Server Manager
File
Action
View
Help
Server Manager (ST-2K8HV-004)
Roles
Features
Diagnostics
Event Viewer
Reliability and Performance
Device Manager
Configuration
Storage
Windows Server Backup
Disk Management
Device Manager
ST-2K8HV-0
Comput
Disk driv
Scan for hardware changes
Add legacy hardware
Dell Virtual Floppy USB Device
IBM 1814 FAStT SCSI Disk Device
IBM 1814 FAStT SCSI Disk Device
IBM Universal Xport SCSI Disk Device
MAXTOR ATLAS10K5_147SAS SCSI Disk Device
Display adapters
DVD/CD-ROM drives
Floppy drive controllers
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client)
Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client) #2
Intel(R) PRO/1000 PT Dual Port Server Adapter
Intel(R) PRO/1000 PT Dual Port Server Adapter #2
Ports (COM & LPT)
Processors
Storage controllers
System devices
Universal Serial Bus controllers
Actions
Device Ma...

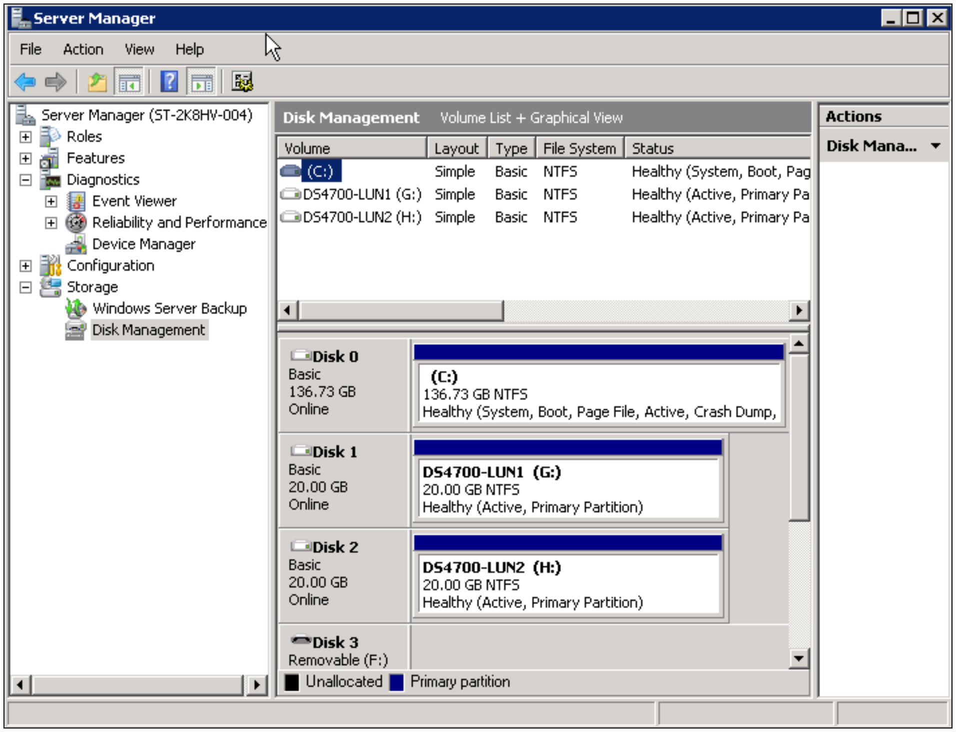
Scan for changed or new Plug and Play devices.

Figure 10-44 Scan for hardware changes

We see that the IBM 1814 LUNs are recognized.

2. Select **Disk Management**. In the Disk Management panel, shown in Figure 10-45, we can select **Action** → **Rescan Disks**. When the disks appear in the disks pane, the signature can be written to them, and they can be formatted following the standard Microsoft Windows procedure for this task.

   Figure 10-45 shows two IBM DS4700 LUNs formatted, with a drive letter ready to use.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (System, Boot, Pag
DS4700-LUN1 (G:)	Simple	Basic	NTFS	Healthy (Active, Primary Pa
DS4700-LUN2 (H:)	Simple	Basic	NTFS	Healthy (Active, Primary Pa

Disk 0
Basic
136.73 GB
Online

(C:)
136.73 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump,

Disk 1
Basic
20.00 GB
Online

DS4700-LUN1 (G:)
20.00 GB NTFS
Healthy (Active, Primary Partition)

Disk 2
Basic
20.00 GB
Online

DS4700-LUN2 (H:)
20.00 GB NTFS
Healthy (Active, Primary Partition)

Disk 3
Removable (F:)

Figure 10-45 Disk Management

10.6.2 Checking performance of the FCIP tunnel

In our lab, the IP network consists of a direct connection from the ge0 ports, giving us a bidirectional link speed of 1 Gbps. In a real-life situation, a real IP network carries the traffic, and performance varies depending on the quality and speed of the WAN connection. For this reason, measuring how fast the connection is can be important; IBM/Brocade provides a useful tool built into the SAN routers to perform this test.

Test the connectivity to see whether any connection exists at all, as shown in Example 10-19.

Example 10-19 Testing connectivity

```
IBM_SAN256B_130:admin> portcmd --ping 1/ge0 -s 192.168.1.10 -d
192.168.1.20
Pinging 192.168.1.20 from ip interface 192.168.1.10 on 1/ge0 with 64
bytes of data
Reply from 192.168.1.20: bytes=64 rtt=0ms ttl=99
Reply from 192.168.1.20: bytes=64 rtt=0ms ttl=99
Reply from 192.168.1.20: bytes=64 rtt=0ms ttl=99
Reply from 192.168.1.20: bytes=64 rtt=0ms ttl=99

Ping Statistics for 192.168.1.20:
        Packets: Sent = 4, Received = 4, Loss = 0 ( 0 percent loss)
        Min  RTT = 0ms, Max RTT = 0ms Average = 0ms

IBM_SAN256B_130:admin>
```

We receive a reply from the destination so we can continue with the performance test.

The performance test has to be initiated from both ends of the FCIP tunnel. First the receiving end is initiated, so that it replies to the performance test from the sending end, as shown in Example 10-20.

Example 10-20 Measuring performance: initiating the receiver

```
IBM_SAN18BR_137:admin> portcmd --ipperf ge0 -s 192.168.1.20 -d
192.168.1.10 -R
ipperf to 192.168.1.10 from IP interface 192.168.1.20 on 0/0:3227
```

While we leave the receiving end in this state, we can now initiate the performance test from the sending end as shown in Example 10-21.

Example 10-21 Measuring performance: initiating the sender

```
IBM_SAN256B_130:admin> portcmd --ipperf 1/ge0 -s 192.168.1.10 -d
192.168.1.20 -S
ipperf to 192.168.1.20 from IP interface 192.168.1.10 on 1/0:3227
Sampling frequency(30s) Total time(30s) BW:117.84MBps WBW:57.95MBps
Loss(%):0.00 Delay(ms):0 PMTU:2348
Sampling frequency(30s) Total time(60s) BW:117.15MBps WBW:86.97MBps
Loss(%):0.00 Delay(ms):0 PMTU:2348
Sampling frequency(30s) Total time(90s) BW:117.43MBps WBW:101.48MBps
Loss(%):0.00 Delay(ms):1 PMTU:2348
```

The sender reports the results of the test every 30 seconds (the default) until it is stopped with CTRL+C keystrokes. In Example 10-21, we see a stable performance in the area of 117 MBps. This is what we can expect on a direct connection operating at 1 Gbps. In real life, the results might not be quite as good; results can also vary depending on the direction we are measuring.

This concludes the configuration of our FCIP tunnel.

11

iSCSI gateway implementation

This chapter shows how to implement the iSCSI gateway service available with the iSCSI blade for the IBM TotalStorage SAN256B (2109-M48) director.

11.1 Overview

This chapter describes the FC4-16IP blade iSCSI gateway service. The iSCSI gateway service is supported only on the SAN256B director running Fabric OS v5.2.0 or later with one or more iSCSI-enabled FC4-16IP blades.

The FC4-16IP iSCSI gateway service is an intermediate device in the network, allowing iSCSI initiators in an IP SAN to access and use storage in a Fibre Channel (FC) SAN, as shown in the Figure 11-1.

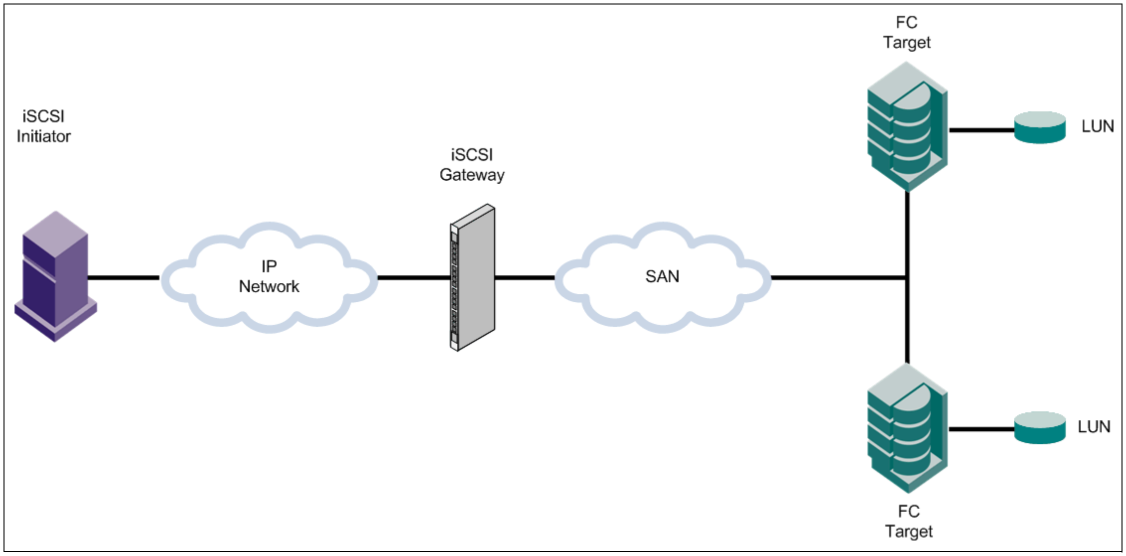


Figure 11-1 iSCSI Gateway

The iSCSI service allows non-FC-capable hosts to connect to an FC storage area network (SAN) infrastructure using IP and Ethernet connectivity. We start by completing the basic installation steps required for initial implementation. This is done using the iSCSI Launch Usability Wizard, which is accessible from the SAN256B Web Tools management GUI. We then demonstrate configuration tasks for use after the initial implementation.

iSCSI-enabled hosts connect to the iSCSI gateway service using iSCSI initiators, which can be implemented in both hardware and software. Through the iSCSI initiator the host operating system (OS) communicates with the iSCSI gateway service, from which iSCSI targets are accessible. Acting as an FC initiator, the iSCSI gateway then proxies the iSCSI connections onto the FC SAN, where the actual storage devices reside.

The iSCSI gateway service available with the iSCSI blade provides the following services to iSCSI initiators:

- Access to an IBM System Storage or TotalStorage based FC SAN using virtual FC devices (iSCSI targets)
- Support for target registration to an iSCSI name server (iSNS) for discovery
- Management of iSCSI initiator access control using discovery domains and discovery domain sets
- Session management features such as session tracking and performance monitoring
- Session authentication using Challenge Handshake Authentication Protocol (CHAP)
- Connection redirects to load balance across iSCSI ports and allow path failover

> **Note:** The iSCSI gateway service found on the iSCSI blade for the SAN256B director is not compatible with previous IBM TotalStorage b-type iSCSI platforms. This chapter assumes that Fabric OS v6.1.0 is installed on the SAN256B director and iSCSI blade.

iSCSI session translation

The iSCSI gateway enables applications on an IP network to use an iSCSI initiator to connect to FC targets. The iSCSI gateway translates iSCSI protocol to Fibre Channel Protocol (FCP), bridging the IP network and FC SAN. Figure 11-2 shows a basic implementation.

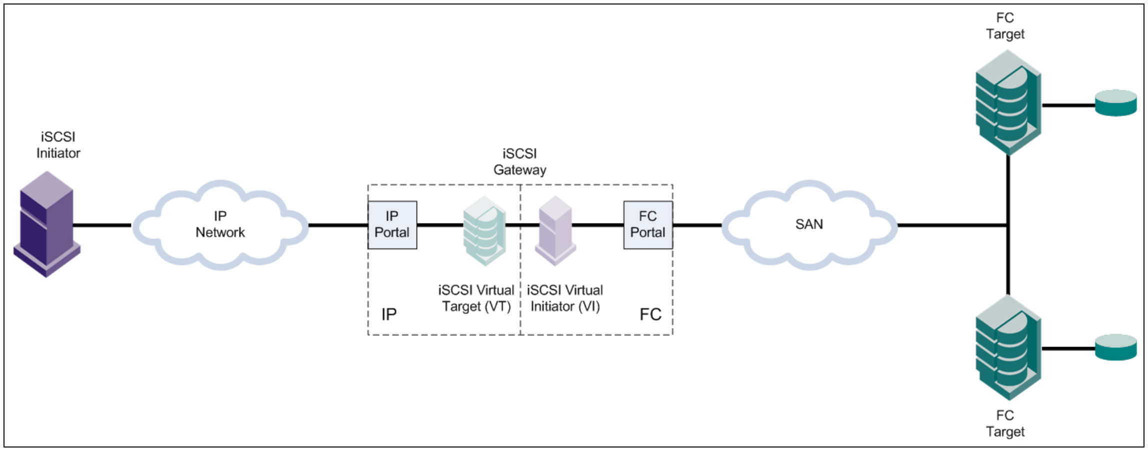


Figure 11-2 iSCSI gateway translation service

The IBM FC4-16IP blade acts as an iSCSI gateway between FC-attached targets and iSCSI initiators. On the iSCSI initiator, iSCSI is mapped between the SCSI driver and the TCP/IP stack. At the iSCSI gateway port, the incoming iSCSI data is converted to FCP (SCSI on FC) by the iSCSI virtual initiator, and then forwarded to the FC target. This approach allows low-cost servers to use an existing FC infrastructure.

To represent all iSCSI initiators and sessions, each iSCSI portal has one iSCSI virtual initiator (VI) to the FC fabric that appears as an N_Port device, with a special WWN format. Regardless of the number of iSCSI initiators or iSCSI sessions sharing the portal, Fabric OS uses one iSCSI VI per iSCSI portal.

Figure 11-3 shows the interaction of different layers from the iSCSI initiator stack to the FC target stack, including the iSCSI gateway service used during protocol translation.

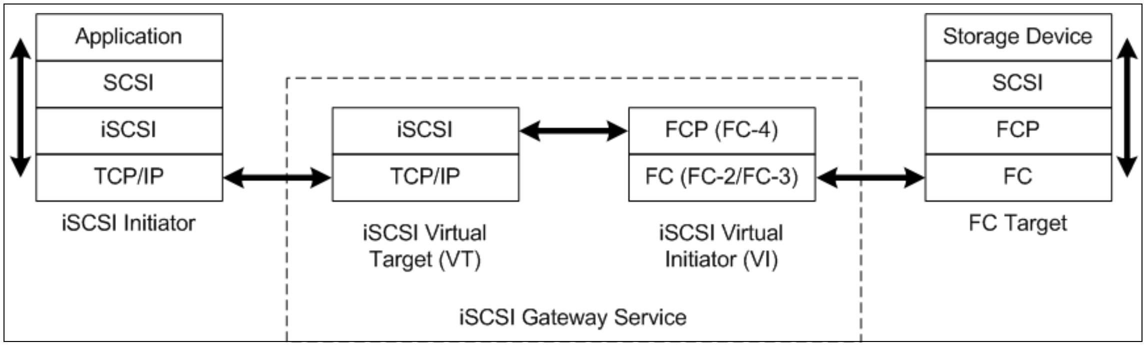


Figure 11-3 iSCSI-to-FC translation

FC4-16IP port numbering

The FC4-16IP blade has both GbE ports and FC ports (Figure 11-4). Ports are addressed using slot-number and port-number notation, for example, 2/7. FC ports are numbered in the range 0 - 7; GbE ports are numbered from ge0 through ge7.

Note: The FC4-16IP blade does not support FCIP functionality.

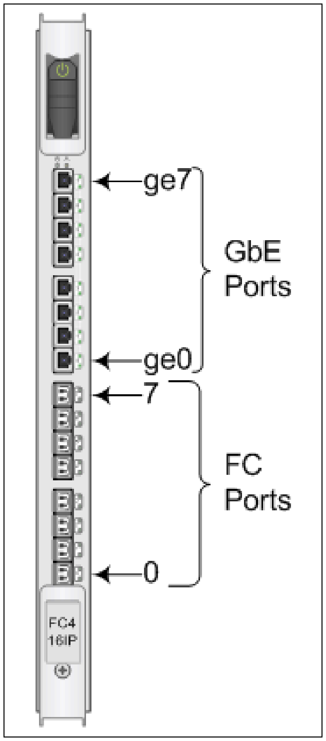


Figure 11-4 FC4-16IP ports

11.2 Initial implementation

After verifying that four power supplies are present in the SAN256B chassis, we insert and latch the iSCSI blade in slot 10 of the director. After a few minutes the blade is initialized and the iSCSI gateway service is available for configuration. The iSCSI feature does not require any additional licenses to be installed on the SAN256B director, the iSCSI blade, or elsewhere in the IBM SystemStorage SAN infrastructure.

To start using the iSCSI gateway service the following steps must be completed:

1. Ensure that an Ethernet infrastructure is in place and that FC storage is available for use with the iSCSI service.
2. Enable the iSCSI service on the SAN256B director.
3. Configure the iSCSI service using the Launch Usability Wizard.
4. Install and configure iSCSI initiators.

To demonstrate the iSCSI functionality, we use the basic lab setup shown in Figure 11-5 as our foundation.

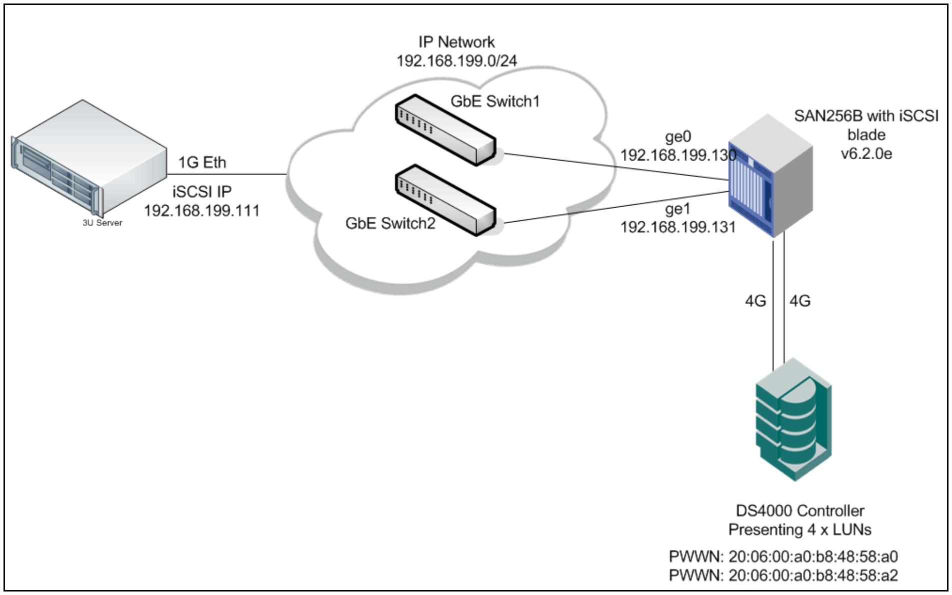


Figure 11-5 iSCSI setup diagram

Terms used in Figure 11-5:

DID	Switch domain ID
1G ETH	Gigabit Ethernet link
P *xx*	Port number on switch
***x*G**	FC link speed in Gbps
PWWN	Port world-wide name

The setup consists of a single rack mount server running Microsoft Windows Server 2003 standard edition with Service Pack 2 installed. The server with host name `st-2k8hv-004` has multiple IP/Ethernet connections, one being connected to a dedicated network for iSCSI using an IP address of 192.168.199.111 in the 192.168.199.0/24 IP subnet.

This dedicated iSCSI Ethernet network comprises two standard Gigabit Ethernet (GbE) switches. Only the server and the iSCSI blade are initially connected to this network, which does not implement any IP routers, firewalls, or virtual LANs (VLAN).

11.2.1 Setting up the basic lab

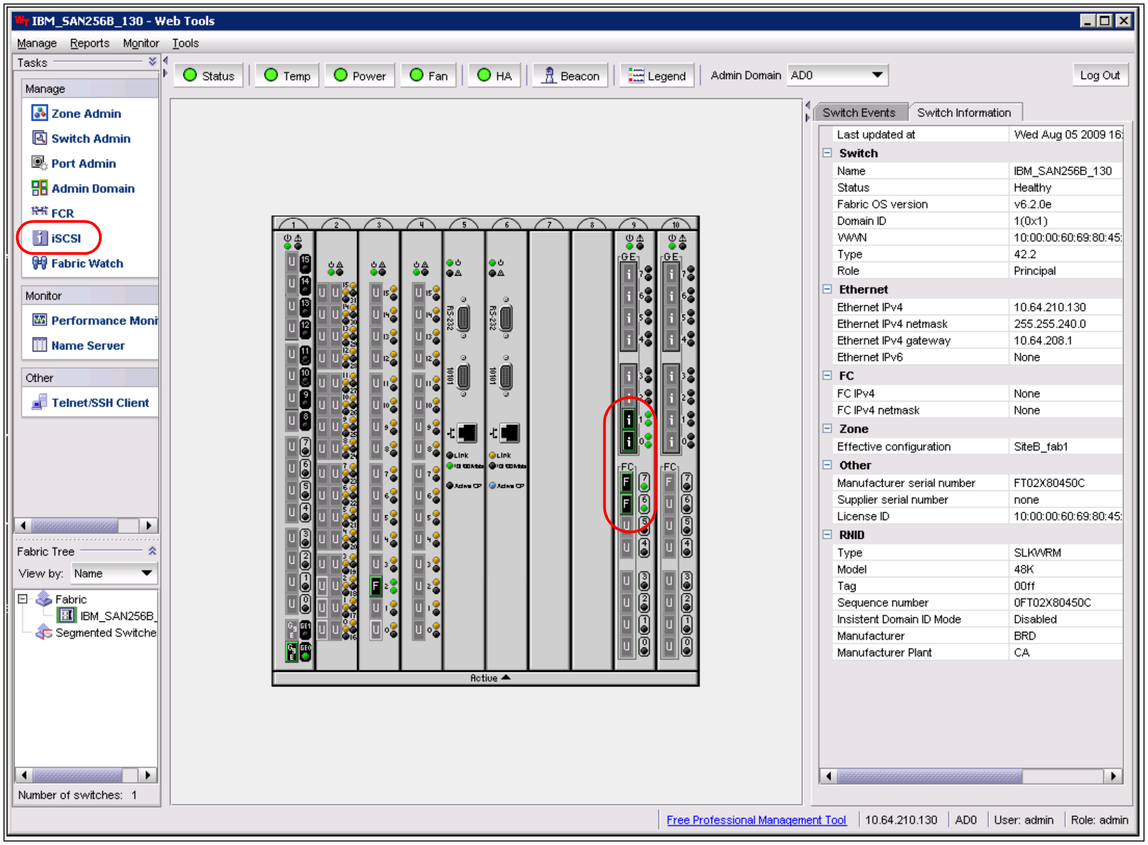
Perform the following steps to create the lab setup shown in Figure 11-5 on page 258.

1. Connect two of the GbE interfaces to the iSCSI blade (ge0 and ge1). A DS4000 with two LUNs configured is connected to two FC ports within the SAN256B director.

> **Note:** Worldwide name (WWN) information for both the SAN256B director and the iSCSI blades is needed to implement the access control on the disk storage subsystem. For more information, refer to 11.3.4, “LUN masking” on page 312.

2. With the physical setup in place, access the SAN256B's Web Tools management GUI, where you see two iSCSI blades in slot 9 and slot 10.

   Use the blade in slot 9. Figure 11-6 shows that the two GbE interfaces (depicted by an *i*) and the FC ports where the DS4000 is connected are green, indicating they are active.

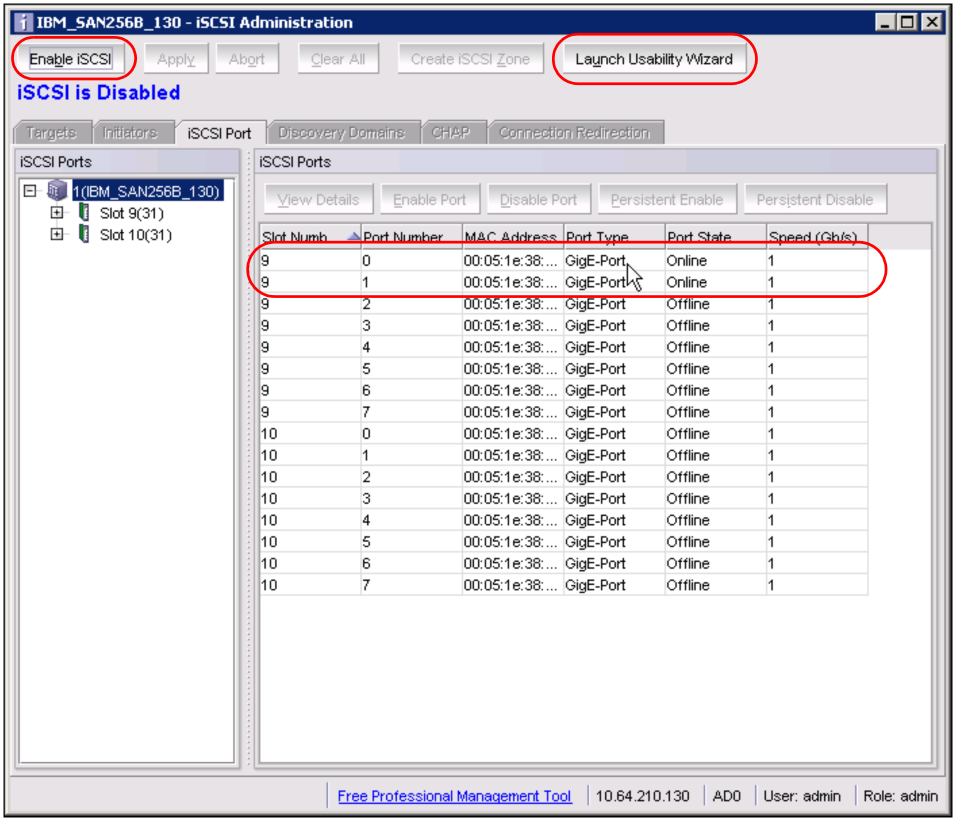


Last updated at	Wed Aug 05 2009 16:
Switch	
Name	IBM_SAN256B_130
Status	Healthy
Fabric OS version	v6.2.0e
Domain ID	1(0x1)
WWN	10:00:00:60:69:80:45:
Type	42.2
Role	Principal
Ethernet	
Ethernet IPv4	10.64.210.130
Ethernet IPv4 netmask	255.255.240.0
Ethernet IPv4 gateway	10.64.208.1
Ethernet IPv6	None
FC	
FC IPv4	None
FC IPv4 netmask	None
Zone	
Effective configuration	SiteB_fab1
Other	
Manufacturer serial number	FT02X80450C
Supplier serial number	none
License ID	10:00:00:60:69:80:45:
RNID	
Type	SLKWRM
Model	48K
Tag	00ff
Sequence number	0FT02X80450C
Insistent Domain ID Mode	Disabled
Manufacturer	BRD
Manufacturer Plant	CA

Figure 11-6 SAN256B Web Tools main view

3. The iSCSI service is administered by clicking the **iSCSI** link in the Manage panel on the left side of the window.

   A window opens (Figure 11-7) to show the iSCSI-capable GbE ports. Observe that ports 9/ge0 and 9/ge1 are online, indicating that the Ethernet media access control (MAC) function is active.



iSCSI is Disabled

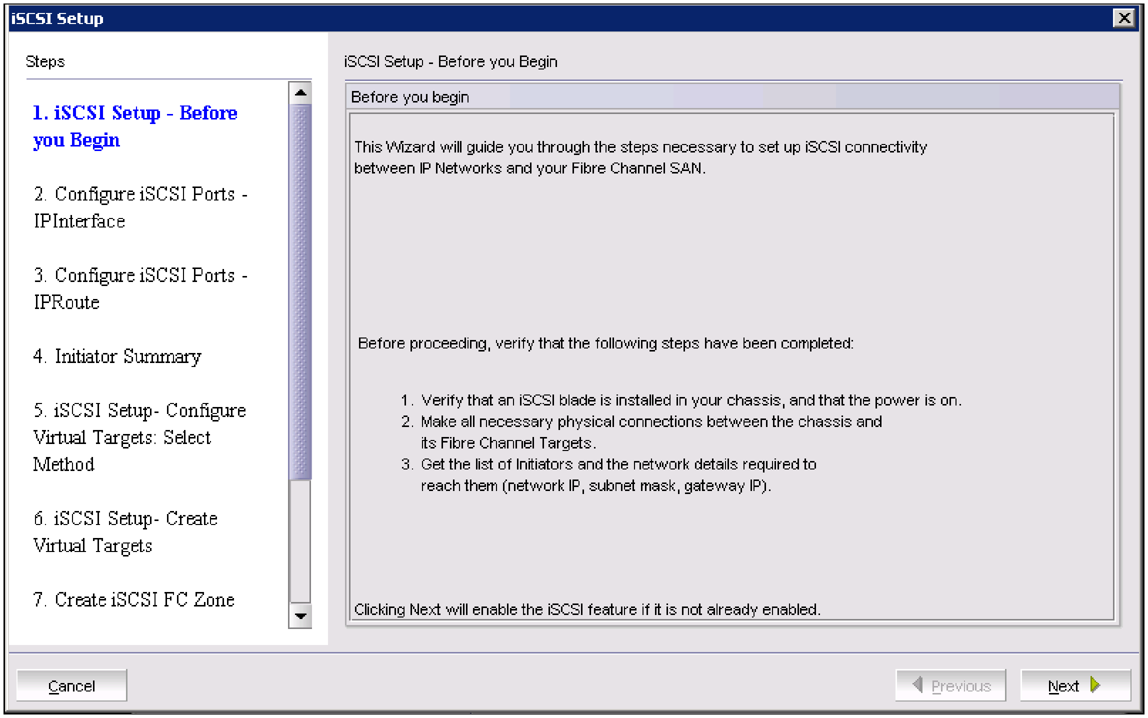
Slot Numb	Port Number	MAC Address	Port Type	Port State	Speed (Gb/s)
9	0	00:05:1e:38:...	GigE-Port	Online	1
9	1	00:05:1e:38:...	GigE-Port	Online	1
9	2	00:05:1e:38:...	GigE-Port	Offline	1
9	3	00:05:1e:38:...	GigE-Port	Offline	1
9	4	00:05:1e:38:...	GigE-Port	Offline	1
9	5	00:05:1e:38:...	GigE-Port	Offline	1
9	6	00:05:1e:38:...	GigE-Port	Offline	1
9	7	00:05:1e:38:...	GigE-Port	Offline	1
10	0	00:05:1e:38:...	GigE-Port	Offline	1
10	1	00:05:1e:38:...	GigE-Port	Offline	1
10	2	00:05:1e:38:...	GigE-Port	Offline	1
10	3	00:05:1e:38:...	GigE-Port	Offline	1
10	4	00:05:1e:38:...	GigE-Port	Offline	1
10	5	00:05:1e:38:...	GigE-Port	Offline	1
10	6	00:05:1e:38:...	GigE-Port	Offline	1
10	7	00:05:1e:38:...	GigE-Port	Offline	1

Figure 11-7 iSCSI administration main view

4. Notice that the iSCSI service is currently disabled. Enable it by clicking **Enable iSCSI**.

5. Click **Launch Usability Wizard** to start configuring the iSCSI service.

   You are presented with "iSCSI Setup - Before you Begin" window (Figure 11-8).



iSCSI Setup
Steps
1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets
7. Create iSCSI FC Zone
iSCSI Setup - Before you Begin
Before you begin
Cancel
Previous
Next

This Wizard will guide you through the steps necessary to set up iSCSI connectivity between IP Networks and your Fibre Channel SAN.

Before proceeding, verify that the following steps have been completed:

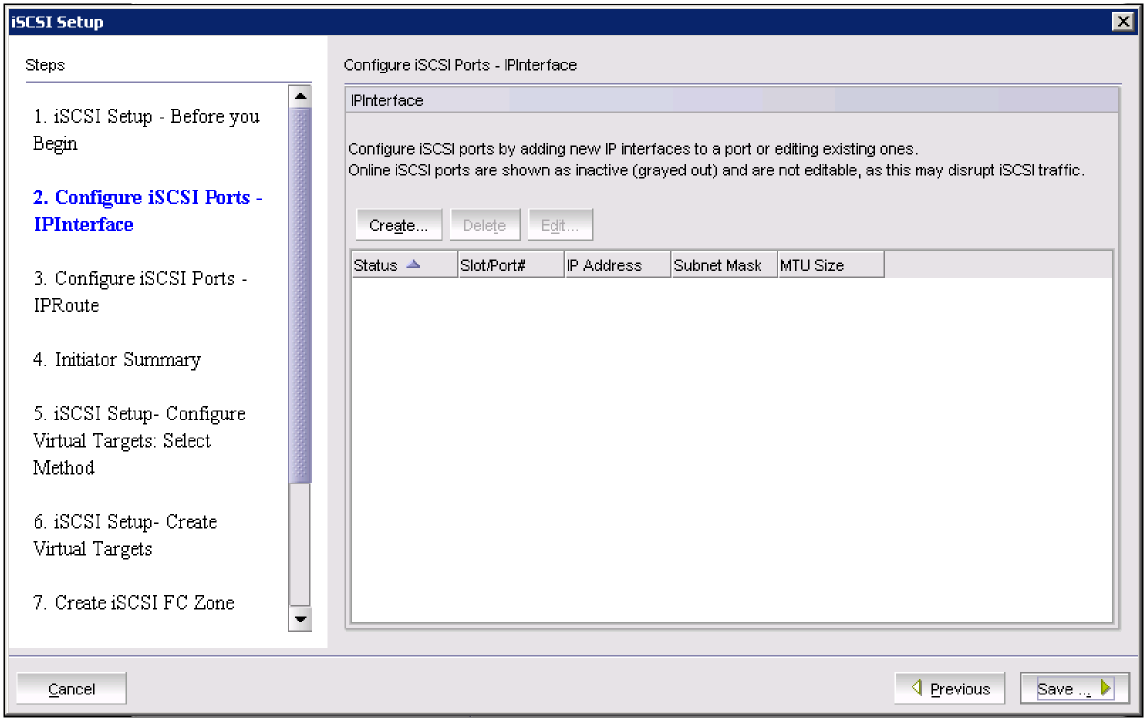
1. Verify that an iSCSI blade is installed in your chassis, and that the power is on.
2. Make all necessary physical connections between the chassis and its Fibre Channel Targets.
3. Get the list of Initiators and the network details required to reach them (network IP, subnet mask, gateway IP).

Clicking Next will enable the iSCSI feature if it is not already enabled.

Figure 11-8 iSCSI Launch Usability Wizard introduction window (iSCSI Setup)

Review the required steps and list of prerequisites, and click **Next**.

The “Configure iSCI Ports - IPInterface” window (Figure 11-9) opens.



1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets
7. Create iSCSI FC Zone

Configure iSCSI Ports - IPInterface

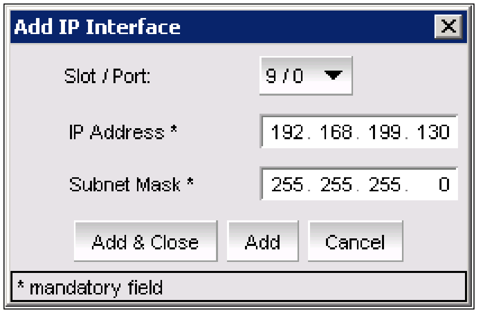
IPInterface

Configure iSCSI ports by adding new IP interfaces to a port or editing existing ones.
Online iSCSI ports are shown as inactive (grayed out) and are not editable, as this may disrupt iSCSI traffic.

Figure 11-9 Configure iSCSI Ports - IPInterface window

6. Configure IP interfaces for the two connected iSCSI GbE ports (the iSCSI portals).

   A maximum of one iSCSI portal (IP interface) can be configured for each GbE port. Start this process by clicking **Create**. The “Add IP Interface” dialog box (Figure 11-10) opens.



Slot / Port: 9 / 0

IP Address * 192 . 168 . 199 . 130

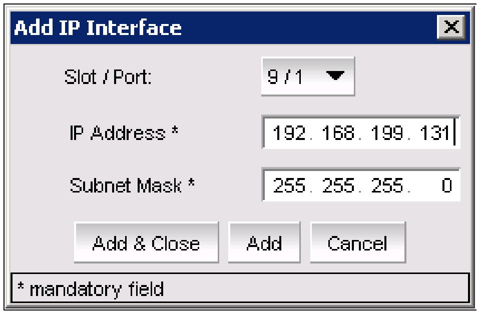
Subnet Mask * 255 . 255 . 255 . 0

* mandatory field

Figure 11-10 Entering IP configuration for first iSCSI GbE port

7. Select the GbE port to which to assign an IP address, and enter the IP configuration. Select **9/0**, and enter the IP information, which is the IP address 192.168.199.130 in the 192.168.199.0/24 IP subnet.

8. Click **Add** to keep the dialog box open for entering IP information for the second GbE port (**9/1**), shown in Figure 11-11. Assign the IP address 192.168.199.131, also in the 192.168.199.0/24 IP subnet, to this port.



Slot / Port: 9 / 1

IP Address * 192 . 168 . 199 . 131

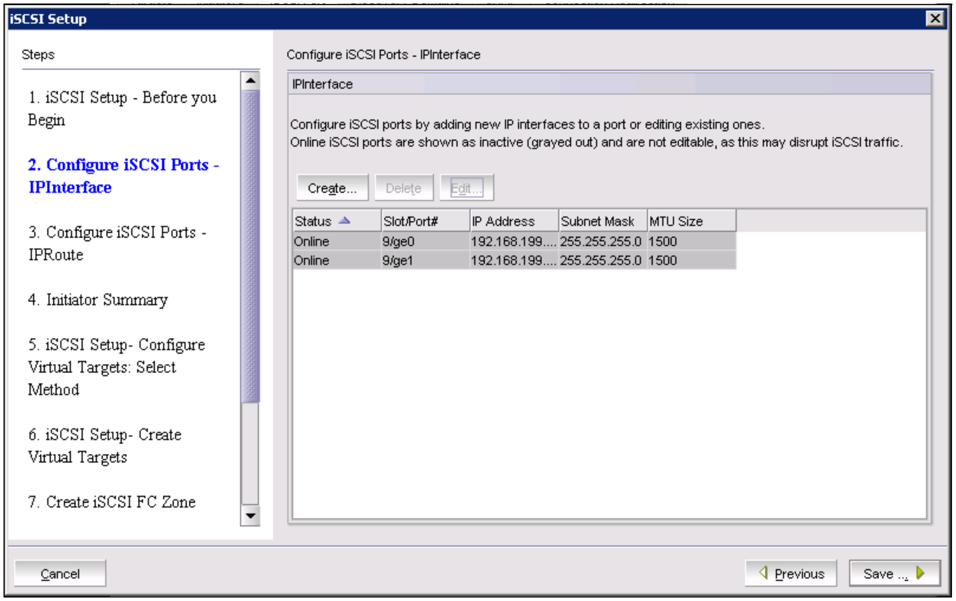
Subnet Mask * 255 . 255 . 255 . 0

* mandatory field

Figure 11-11 Entering IP configuration for second iSCSI GbE port.

9. Click **Add & Close** to exit the “Add IP Interface” dialog box.

10.Confirm the configuration and click **Save**. See Figure 11-12.

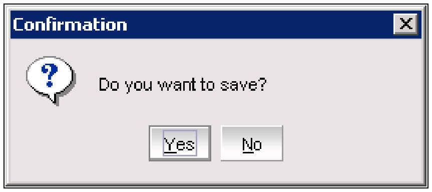

iSCSI Setup
Steps
1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets
7. Create iSCSI FC Zone
Configure iSCSI Ports - IPInterface
IPInterface

Configure iSCSI ports by adding new IP interfaces to a port or editing existing ones.
Online iSCSI ports are shown as inactive (grayed out) and are not editable, as this may disrupt iSCSI traffic.

Status	Slot/Port#	IP Address	Subnet Mask	MTU Size
Online	9/ge0	192.168.199....	255.255.255.0	1500
Online	9/ge1	192.168.199....	255.255.255.0	1500

Figure 11-12 IP configuration confirmation

A “Confirmation” dialog box (Figure 11-13) opens. Click **Yes** to save.

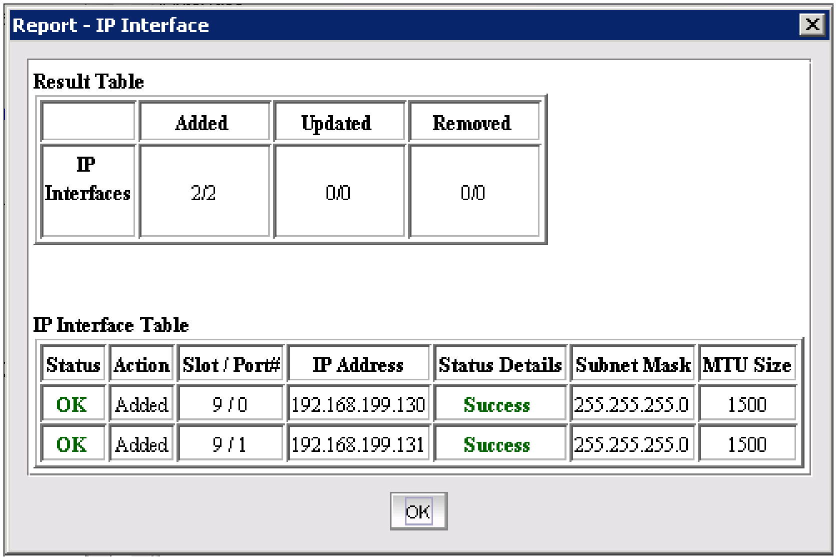


Confirmation

Do you want to save?

Figure 11-13 Save IP Confirmation dialog box

The “Report - IP Interface” window (Figure 11-14) opens. Confirm that the configuration has been applied successfully. Click **OK**.



Report - IP Interface

Result Table

	Added	Updated	Removed
IP Interfaces	2/2	0/0	0/0

IP Interface Table

Status	Action	Slot / Port#	IP Address	Status Details	Subnet Mask	MTU Size
OK	Added	9 / 0	192.168.199.130	Success	255.255.255.0	1500
OK	Added	9 / 1	192.168.199.131	Success	255.255.255.0	1500

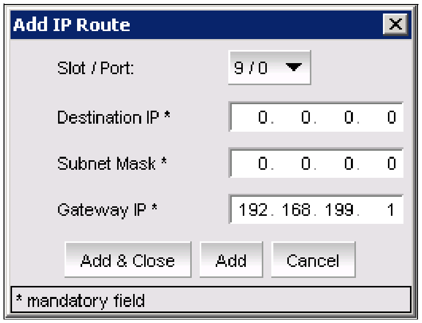
Figure 11-14 IP configuration success

11.2.2 Configuring IP routes for the iSCSI GbE ports

We now have the option to configure IP routes for the iSCSI GbE ports. This process specifies IP routes required for return traffic from the iSCSI blade to the initiator in a routed Ethernet network.

Perform the following steps to configure IP routes for the iSCSI GbE ports:

1. Add a route by clicking **Create** (Figure 11-12 on page 264).
2. In the “Add IP Route” window (Figure 11-15), enter information for a default gateway for any traffic not on the local subnet. Enter 0.0.0.0 for the Destination IP, 0.0.0.0 for the Subnet Mask, and 192.168.199.1 for the Gateway IP. Click **Add & Close**.



Add IP Route

Slot / Port: 9 / 0

Destination IP * 0. 0. 0. 0

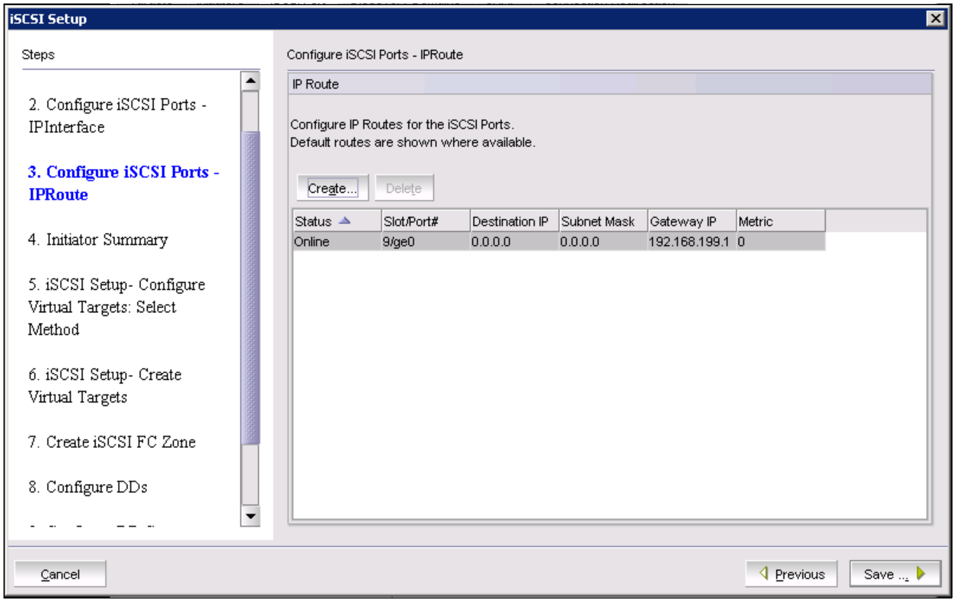
Subnet Mask * 0. 0. 0. 0

Gateway IP * 192. 168. 199. 1

* mandatory field

Figure 11-15 Default IP route example

3. Confirm the configuration and click **Save**, as shown in Figure 11-16.



iSCSI Setup

Steps

2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets
7. Create iSCSI FC Zone
8. Configure DDs

Configure iSCSI Ports - IPRoute

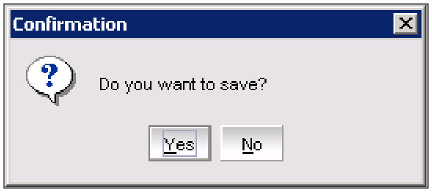
IP Route

Configure IP Routes for the iSCSI Ports.
Default routes are shown where available.

Status	Slot/Port#	Destination IP	Subnet Mask	Gateway IP	Metric
Online	9/ge0	0.0.0.0	0.0.0.0	192.168.199.1	0

Figure 11-16 Configuration confirmation

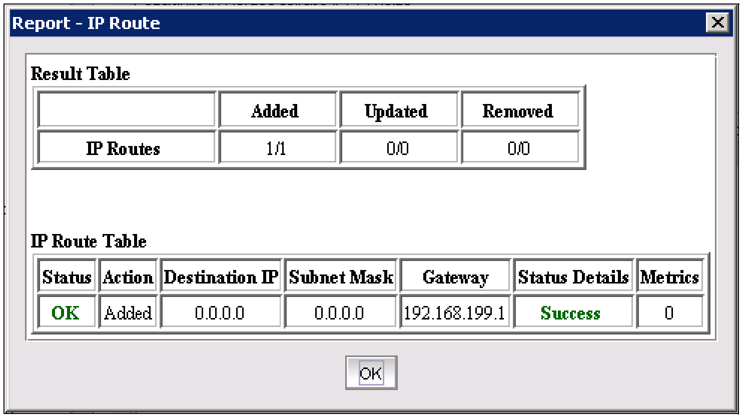
4. At the Confirmation dialog box (Figure 11-17), click **Yes** to save.


Confirmation

Do you want to save?

Figure 11-17 Save Route Confirmation dialog box

A report indicates that the IP route will be added (Figure 11-18). Click **OK**, and **Next**.


Report - IP Route

Result Table

	Added	Updated	Removed
IP Routes	1/1	0/0	0/0

IP Route Table

Status	Action	Destination IP	Subnet Mask	Gateway	Status Details	Metrics
OK	Added	0.0.0.0	0.0.0.0	192.168.199.1	Success	0

Figure 11-18 IP route report

An iSCSI initiator summary is displayed, as shown in Figure 11-19, showing any iSCSI initiators that have logged in on any of the iSCSI ports. We have not yet configured any iSCSI initiators, so the list is empty. Click **Next**.

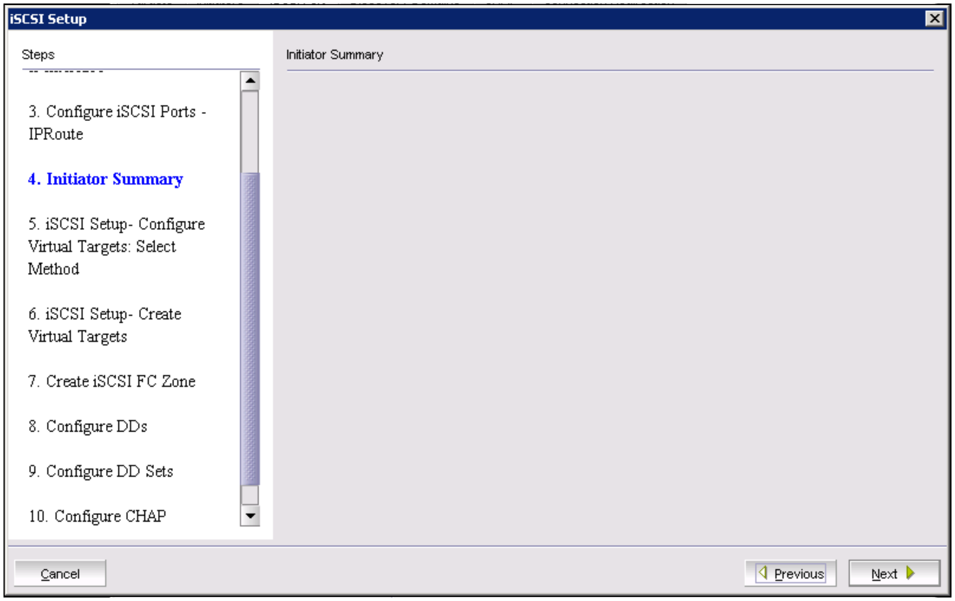
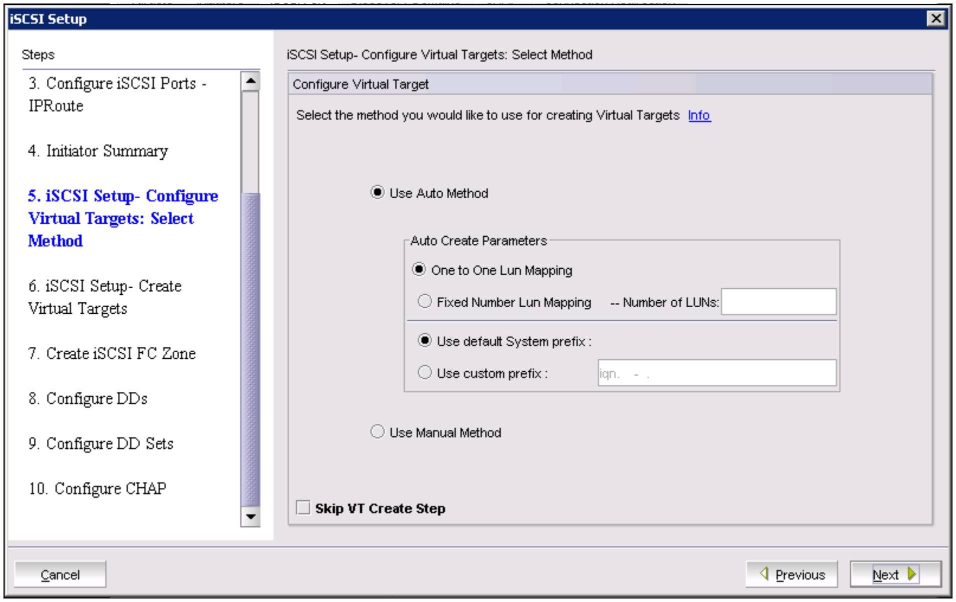


Figure 11-19 Empty iSCSI initiator summary

5. Choose how to configure iSCSI virtual targets (VT) in the “iSCSI Setup - Configure VIrtual Targets: Select Method” window (Figure 11-20). Select **Use Auto Method** and **One to One Lun Mapping**, which means that each FC logical unit number (LUN) will result in an iSCSI VT. To skip iSCSI VT creation, select the **Skip VT Create Step** check box.


iSCSI Setup

Steps

3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets
7. Create iSCSI FC Zone
8. Configure DDs
9. Configure DD Sets
10. Configure CHAP

iSCSI Setup- Configure Virtual Targets: Select Method

Configure Virtual Target

Select the method you would like to use for creating Virtual Targets Info

● Use Auto Method

Auto Create Parameters

● One to One Lun Mapping

○ Fixed Number Lun Mapping -- Number of LUNs:

● Use default System prefix :

○ Use custom prefix : iqn. - .

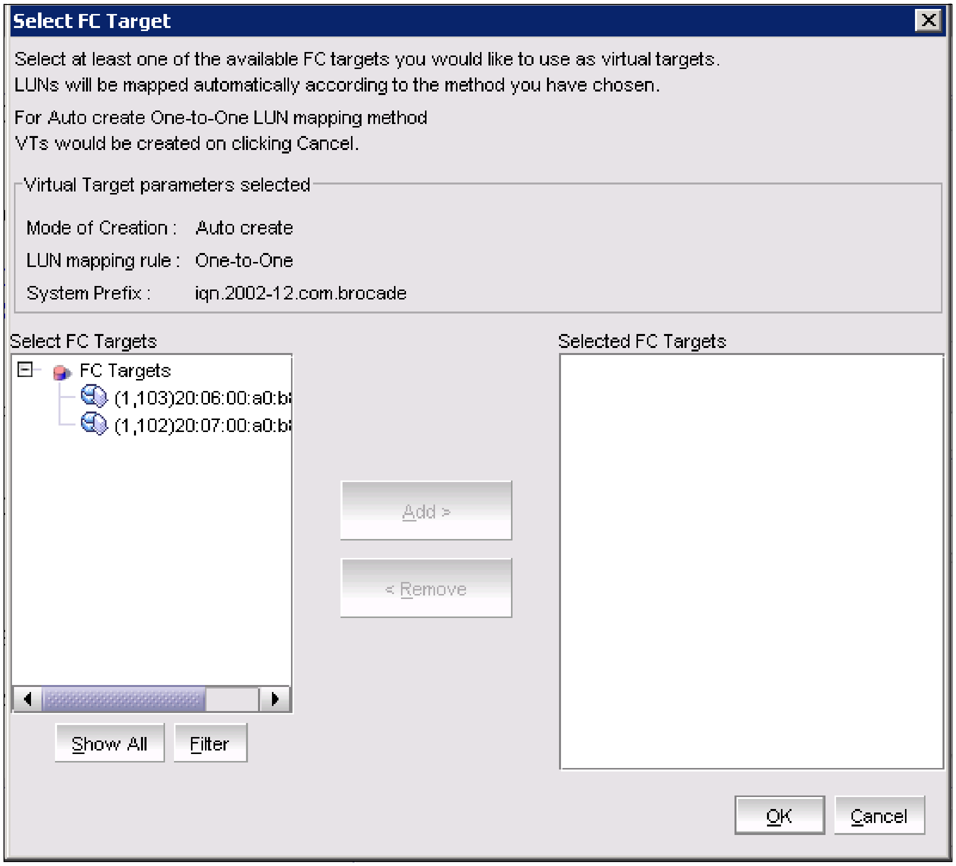
○ Use Manual Method

□ Skip VT Create Step

Figure 11-20 ISCSI virtual target creation method

Leave the iSCSI qualified name (IQN) prefix as standard, which means that all the iSCSI VTs will have a Brocade IQN name indicating that they reside on a SAN256B. Click **Next**.

6. The wizard presents the FC targets available in the FC SAN fabric (Figure 11-21). Select the FC targets to use with the iSCSI service. The two controllers from the DS4000 are visible and can be added.



Select FC Target

Select at least one of the available FC targets you would like to use as virtual targets.
LUNs will be mapped automatically according to the method you have chosen.

For Auto create One-to-One LUN mapping method
VTs would be created on clicking Cancel.

Virtual Target parameters selected

Mode of Creation : Auto create
LUN mapping rule : One-to-One
System Prefix : iqn.2002-12.com.brocade

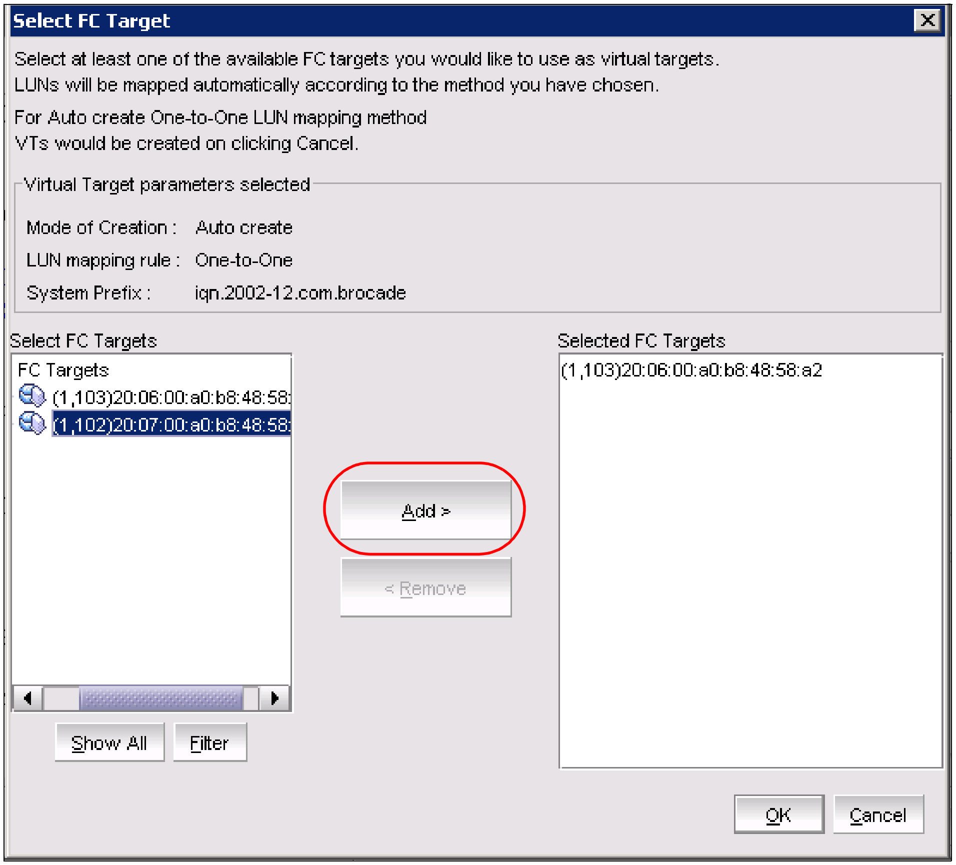
Select FC Targets

- FC Targets
  - (1,103)20:06:00:a0:b
  - (1,102)20:07:00:a0:b

Selected FC Targets

Figure 11-21 Select FC targets

One way to add is to select the individual target interfaces and add them to the Selected FC Targets list by clicking **Add**, as shown in Figure 11-22.



Select FC Target

Select at least one of the available FC targets you would like to use as virtual targets.
LUNs will be mapped automatically according to the method you have chosen.

For Auto create One-to-One LUN mapping method
VTs would be created on clicking Cancel.

Virtual Target parameters selected

Mode of Creation : Auto create
LUN mapping rule : One-to-One
System Prefix : iqn.2002-12.com.brocade

Select FC Targets

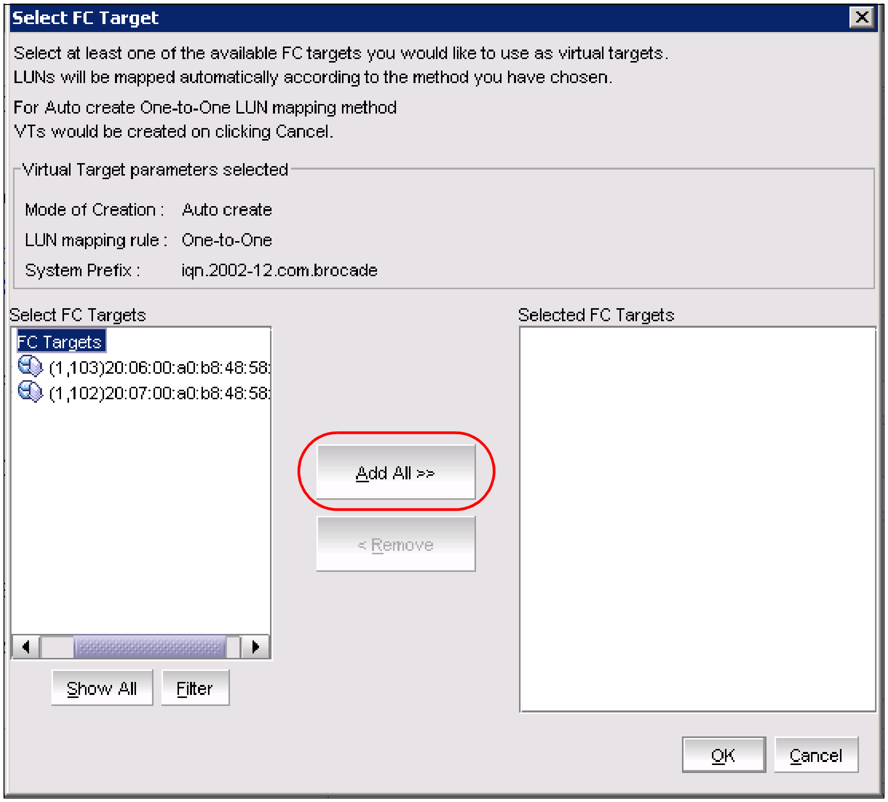
FC Targets
(1,103)20:06:00:a0:b8:48:58:
(1,102)20:07:00:a0:b8:48:58:

Selected FC Targets

(1,103)20:06:00:a0:b8:48:58:a2

Figure 11-22 Selected FC targets

Another way is to select **FC Targets** at the top of the Select FC Targets list. The **Add** button changes to an **Add All** button, as shown in Figure 11-23.



Select FC Target

Select at least one of the available FC targets you would like to use as virtual targets.
LUNs will be mapped automatically according to the method you have chosen.

For Auto create One-to-One LUN mapping method
VTs would be created on clicking Cancel.

Virtual Target parameters selected

Mode of Creation : Auto create
LUN mapping rule : One-to-One
System Prefix : iqn.2002-12.com.brocade

Select FC Targets

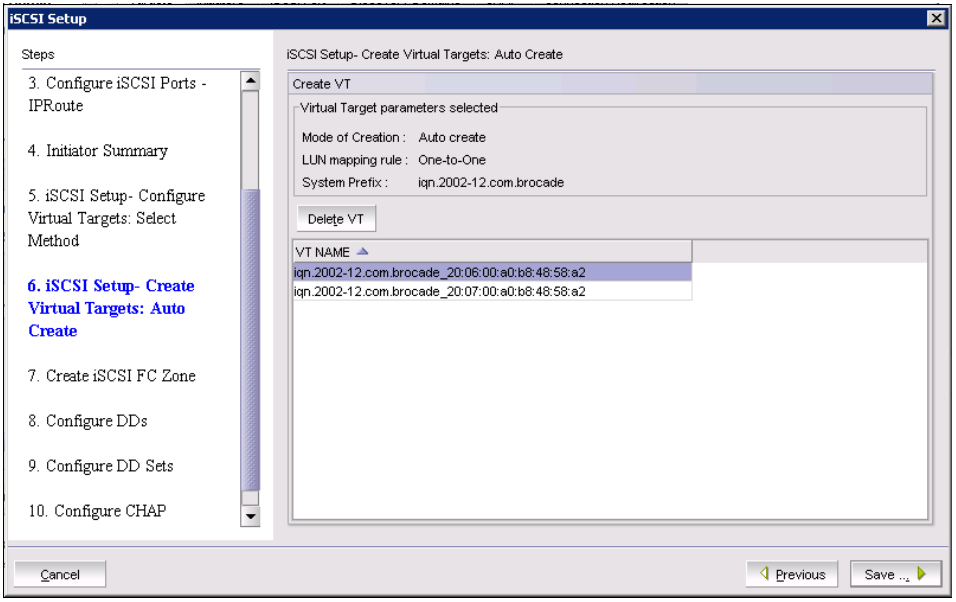
FC Targets
(1,103)20:06:00:a0:b8:48:58:
(1,102)20:07:00:a0:b8:48:58:

Selected FC Targets

Figure 11-23 Adding all FC targets

Click **OK** to close the “Select FC Target” window.

A summary is displayed, as shown in Figure 11-24. In this window the auto-generated IQNs for the iSCSI VTs are listed. The default suffix is the FC target port WWN with an underscore (_) in front. Confirm the information by clicking **Save**.



iSCSI Setup

Steps

3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. **iSCSI Setup- Create Virtual Targets: Auto Create**
7. Create iSCSI FC Zone
8. Configure DDs
9. Configure DD Sets
10. Configure CHAP

iSCSI Setup- Create Virtual Targets: Auto Create

Create VT

Virtual Target parameters selected

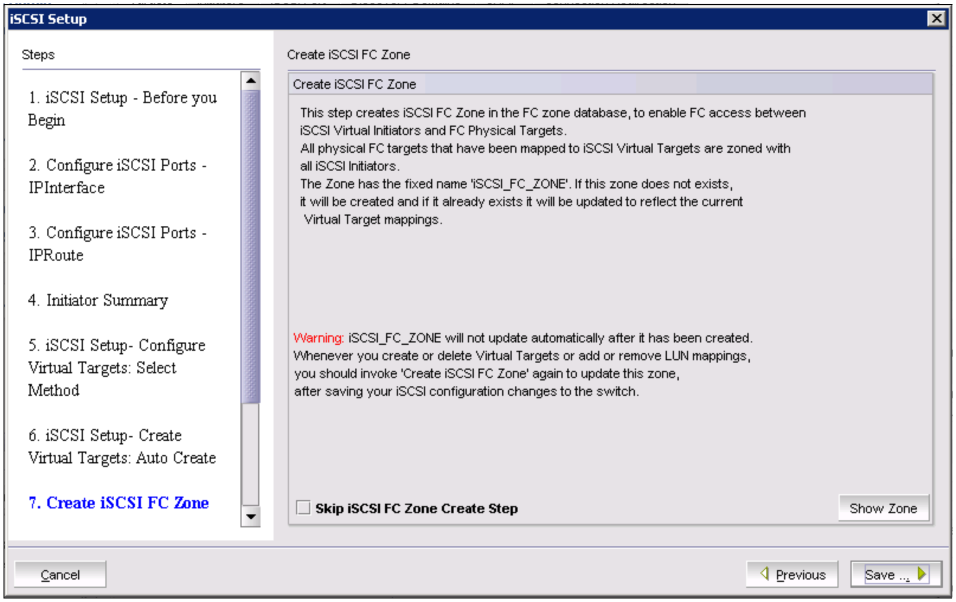
Mode of Creation : Auto create
LUN mapping rule : One-to-One
System Prefix : iqn.2002-12.com.brocade

VT NAME
iqn.2002-12.com.brocade_20:06:00:a0:b8:48:58:a2
iqn.2002-12.com.brocade_20:07:00:a0:b8:48:58:a2

Figure 11-24 iSCSI VT confirmation

We are then presented with a window that tells us that FC targets that have been mapped to iSCSI VTs must be zoned with all iSCSI virtual initiators (VI).

The wizard creates (or updates) the zone named iSCSI_FC_ZONE. See Figure 11-25.


iSCSI Setup
Steps
1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
Create iSCSI FC Zone
Create iSCSI FC Zone

This step creates iSCSI FC Zone in the FC zone database, to enable FC access between iSCSI Virtual Initiators and FC Physical Targets.
All physical FC targets that have been mapped to iSCSI Virtual Targets are zoned with all iSCSI Initiators.
The Zone has the fixed name 'iSCSI_FC_ZONE'. If this zone does not exists, it will be created and if it already exists it will be updated to reflect the current Virtual Target mappings.

Warning: iSCSI_FC_ZONE will not update automatically after it has been created.
Whenever you create or delete Virtual Targets or add or remove LUN mappings, you should invoke 'Create iSCSI FC Zone' again to update this zone, after saving your iSCSI configuration changes to the switch.

Figure 11-25 iSCSI FC Zone

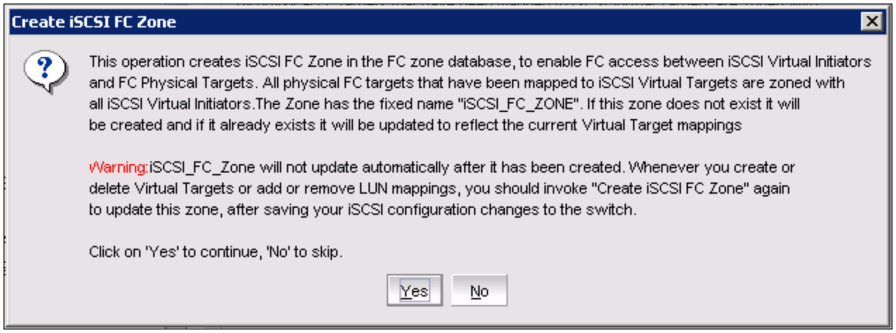
If the zone is not present, the wizard asks where to include the zone. It can be either in a defined configuration or integrated into the current effective configuration.

If you want to display the current zoning configuration in the FC fabric, select **Show Zone**.

If you do not want the wizard to perform the zoning, select the **Skip Create Step** check box. We choose to have the wizard perform the zoning

Click **Save** to continue.

A message (Figure 11-26), indicates that we must confirm the zone. Click **Yes** to continue.



Create iSCSI FC Zone

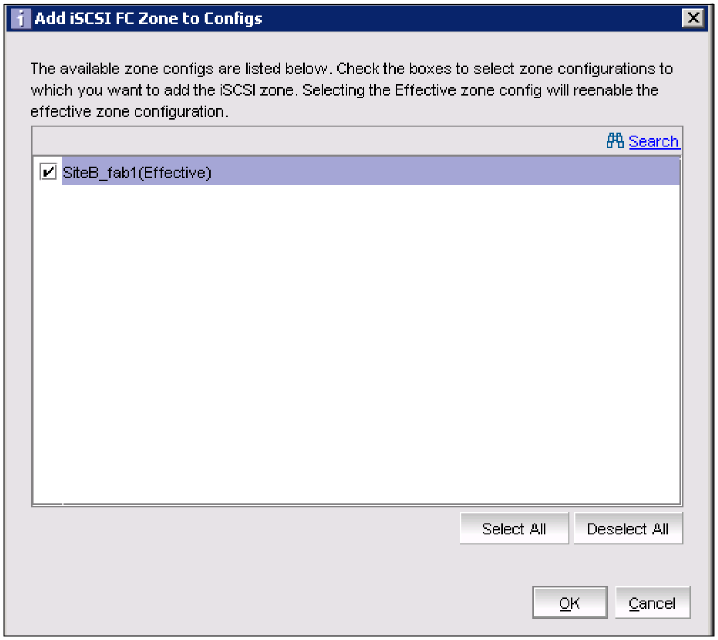
This operation creates iSCSI FC Zone in the FC zone database, to enable FC access between iSCSI Virtual Initiators and FC Physical Targets. All physical FC targets that have been mapped to iSCSI Virtual Targets are zoned with all iSCSI Virtual Initiators.The Zone has the fixed name "iSCSI_FC_ZONE". If this zone does not exist it will be created and if it already exists it will be updated to reflect the current Virtual Target mappings

Warning:iSCSI_FC_Zone will not update automatically after it has been created. Whenever you create or delete Virtual Targets or add or remove LUN mappings, you should invoke "Create iSCSI FC Zone" again to update this zone, after saving your iSCSI configuration changes to the switch.

Click on 'Yes' to continue, 'No' to skip.

Figure 11-26 iSCSI FC Zone confirmation.

7. In our fabric, we have an effective zone, SiteB_fab1. The wizard notifies us about this and asks us to select the zone configuration to which to add the iSCSI_FC_Zone (Figure 11-27). Select the appropriate zone configuration and click **OK.**



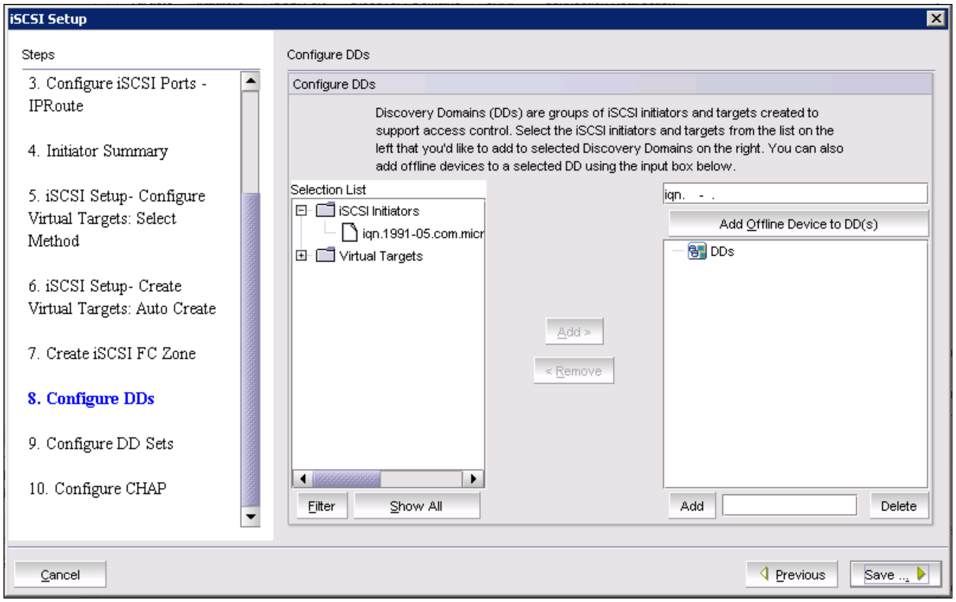
Add iSCSI FC Zone to Configs

The available zone configs are listed below. Check the boxes to select zone configurations to which you want to add the iSCSI zone. Selecting the Effective zone config will reenable the effective zone configuration.

☑ SiteB_fab1(Effective)

Figure 11-27 Zone configuration selection

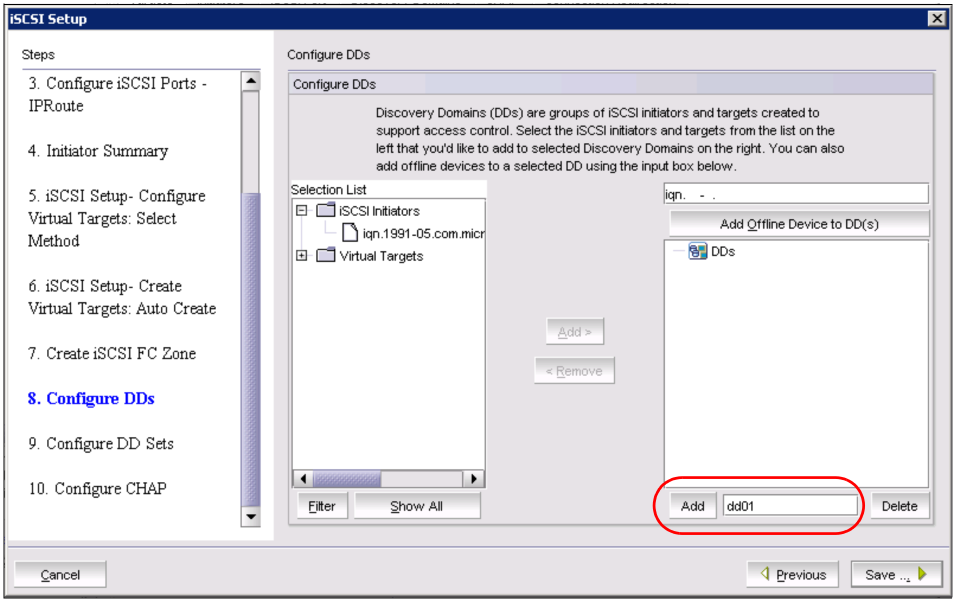
8. Define the access control between iSCSI VIs and iSCSI VTs. This is done using Discovery Domains (DDs) and Discovery Domain Sets (DDSet). DDs can be compared to FC zones and DDSets to FC zone configurations. See Figure 11-28.



Discovery Domains (DDs) are groups of iSCSI initiators and targets created to support access control. Select the iSCSI initiators and targets from the list on the left that you'd like to add to selected Discovery Domains on the right. You can also add offline devices to a selected DD using the input box below.

Figure 11-28 iSCSI DD configuration

9. Enter a DD named `dd001` and click **Add**. See Figure 11-29.



iSCSI Setup

Steps

3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
8. Configure DDs
9. Configure DD Sets
10. Configure CHAP

Configure DDs

Configure DDs

Discovery Domains (DDs) are groups of iSCSI initiators and targets created to support access control. Select the iSCSI initiators and targets from the list on the left that you'd like to add to selected Discovery Domains on the right. You can also add offline devices to a selected DD using the input box below.

Selection List: iSCSI Initiators / iqn.1991-05.com.micr / Virtual Targets

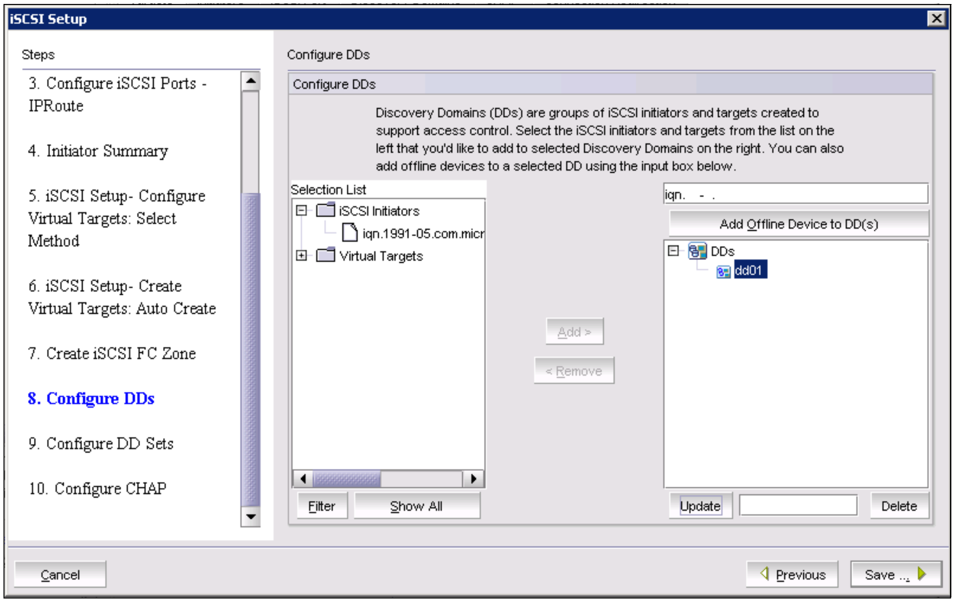
iqn. - .

DDs

Add: dd01

Figure 11-29 iSCSI create dd001

This DD is added to the list, as shown in Figure 11-30. Click **Save**.



iSCSI Setup

Steps

3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
8. Configure DDs
9. Configure DD Sets
10. Configure CHAP

Configure DDs

Configure DDs

Discovery Domains (DDs) are groups of iSCSI initiators and targets created to support access control. Select the iSCSI initiators and targets from the list on the left that you'd like to add to selected Discovery Domains on the right. You can also add offline devices to a selected DD using the input box below.

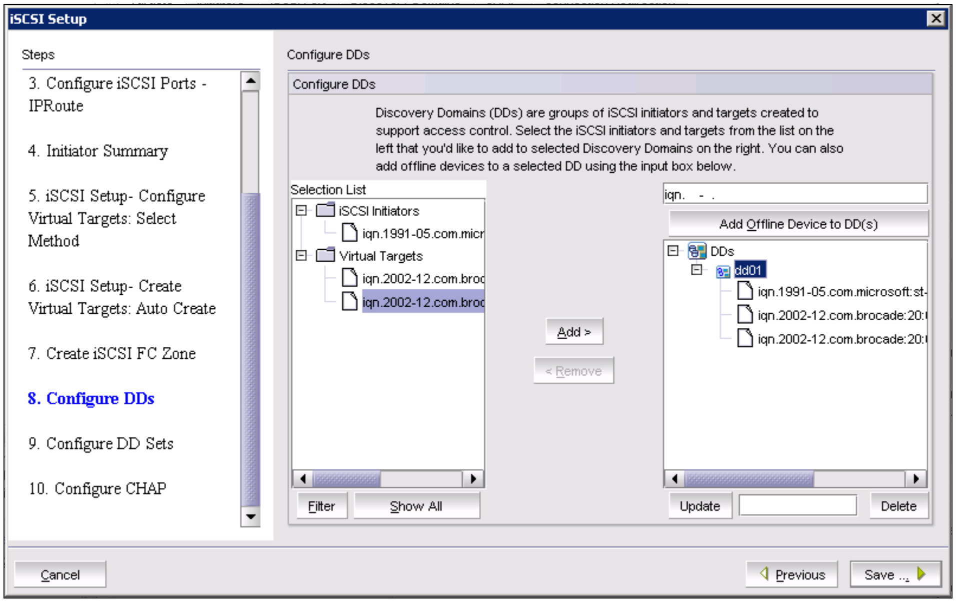
Selection List: iSCSI Initiators / iqn.1991-05.com.micr / Virtual Targets

iqn. - .

DDs / dd01

Figure 11-30 iSCSI add dd001

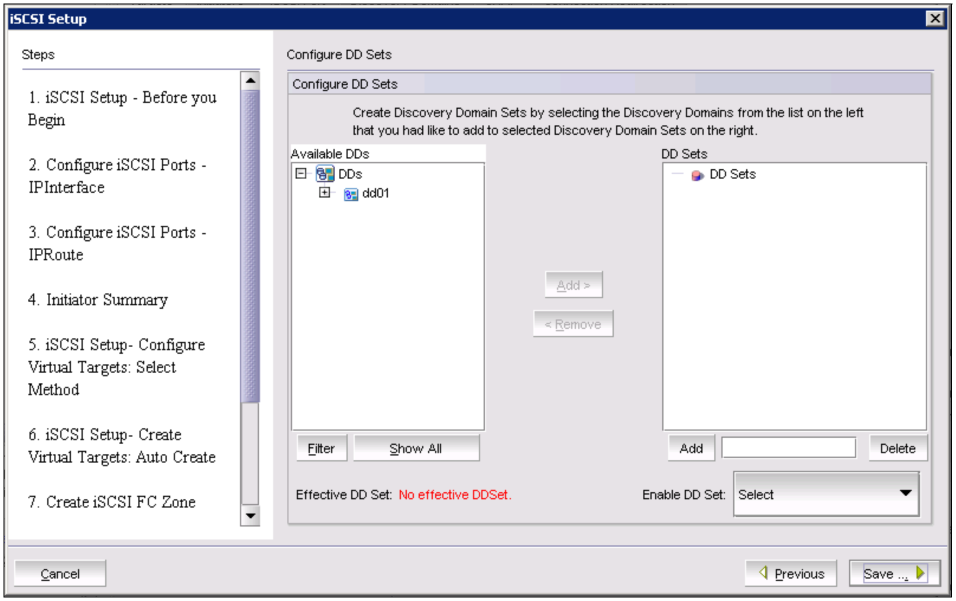
10.Add both the iSCSI VTs and the iSCSI initiator (Figure 11-31). Click **Save**.


iSCSI Setup
Steps
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
8. Configure DDs
9. Configure DD Sets
10. Configure CHAP
Configure DDs
Configure DDs

Discovery Domains (DDs) are groups of iSCSI initiators and targets created to support access control. Select the iSCSI initiators and targets from the list on the left that you'd like to add to selected Discovery Domains on the right. You can also add offline devices to a selected DD using the input box below.

Figure 11-31   iSCSI Add VTs and Initiator to dd001

The “Configure DD Sets” panel (Figure 11-32) opens.


iSCSI Setup
Steps
1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
Configure DD Sets
Configure DD Sets

Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

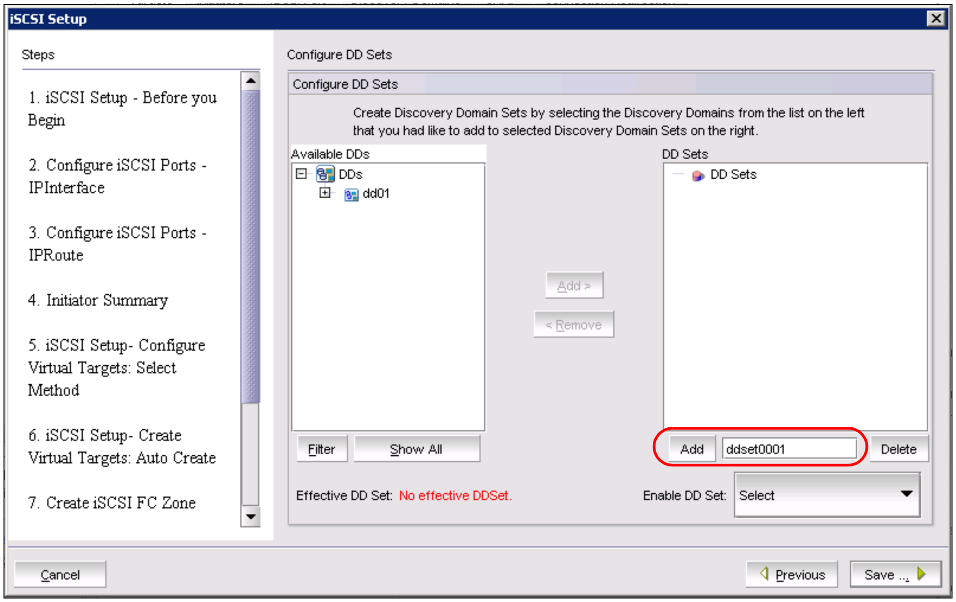
Available DDs
DDs
dd01
DD Sets
DD Sets
Add >
< Remove
Filter
Show All
Add
Delete

Effective DD Set: No effective DDSet.

Enable DD Set: Select

Figure 11-32   DD Sets configuration view

11. Create a DD Set and include dd001. Enter `ddset001` for the name and click **Add**, as shown in Figure 11-33.



iSCSI Setup

Steps

1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone

Configure DD Sets

Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

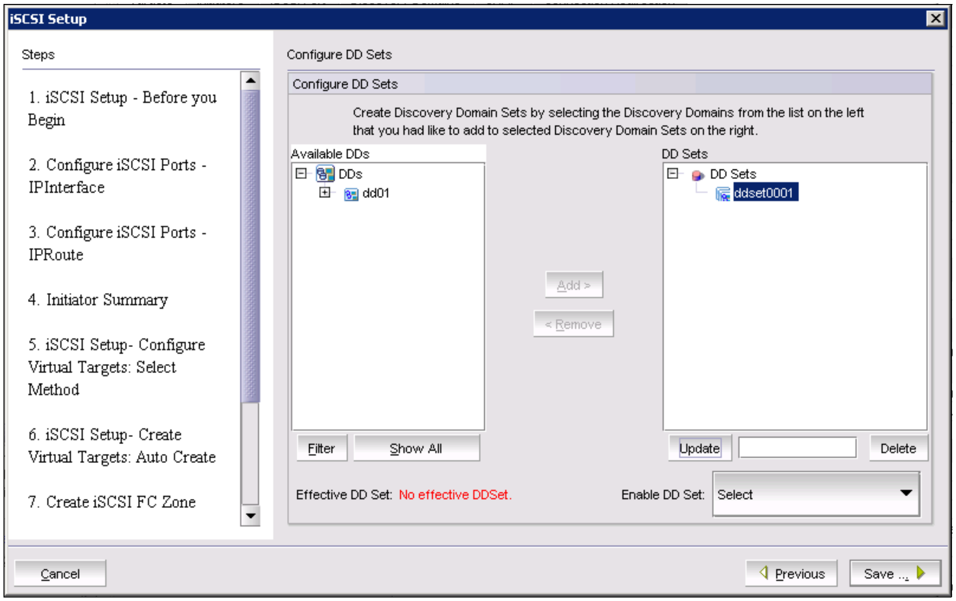
Add: ddset0001

Effective DD Set: No effective DDSet.

Enable DD Set: Select

Figure 11-33 Creating DD Set

The DD Set ddset001 is now defined, as shown in Figure 11-34.



iSCSI Setup

Steps

1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone

Configure DD Sets

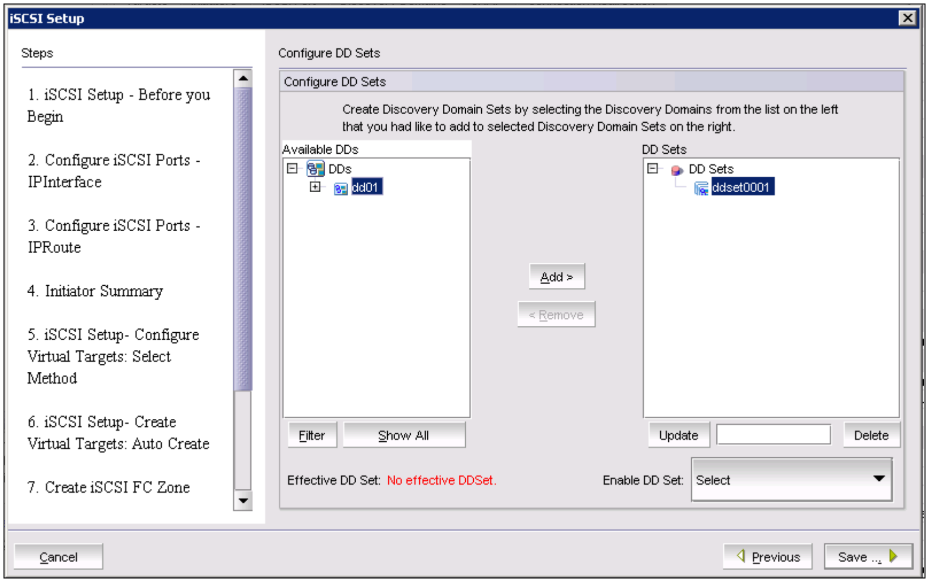
Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

Effective DD Set: No effective DDSet.

Enable DD Set: Select

Figure 11-34 DD Set ddset001 defined

12. Add the DD into the DD Set by selecting both **dd001** and **ddset001** and clicking the **Add** button, as shown in Figure 11-35.



iSCSI Setup

Steps

1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone

Configure DD Sets

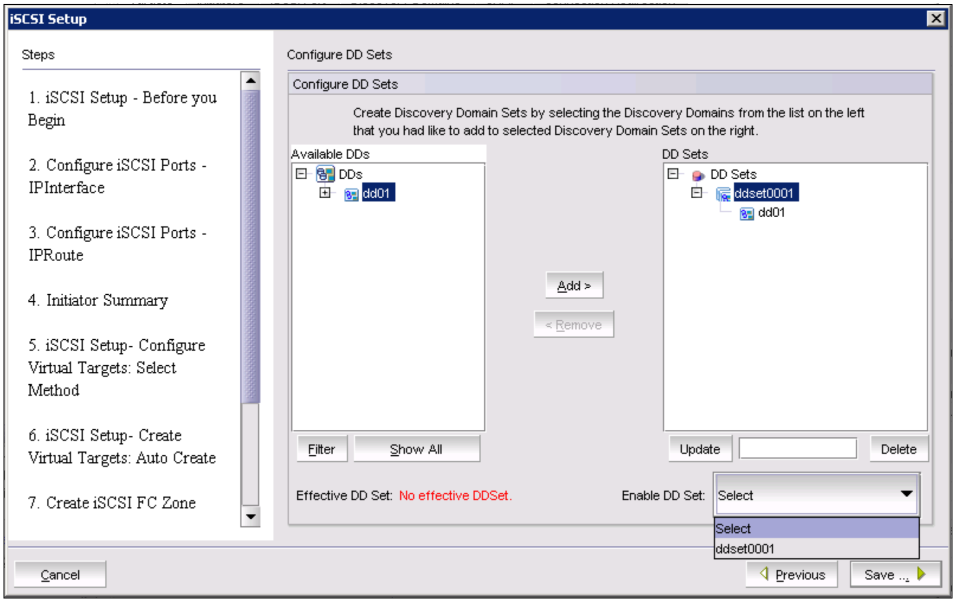
Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

Effective DD Set: No effective DDSet.

Enable DD Set: Select

Figure 11-35 Add DD dd001 to DDSet ddset001

13. Select a DD Set to become the active DD Set with the Enable DD Set drop-down list. See Figure 11-36.



iSCSI Setup

Steps

1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone

Configure DD Sets

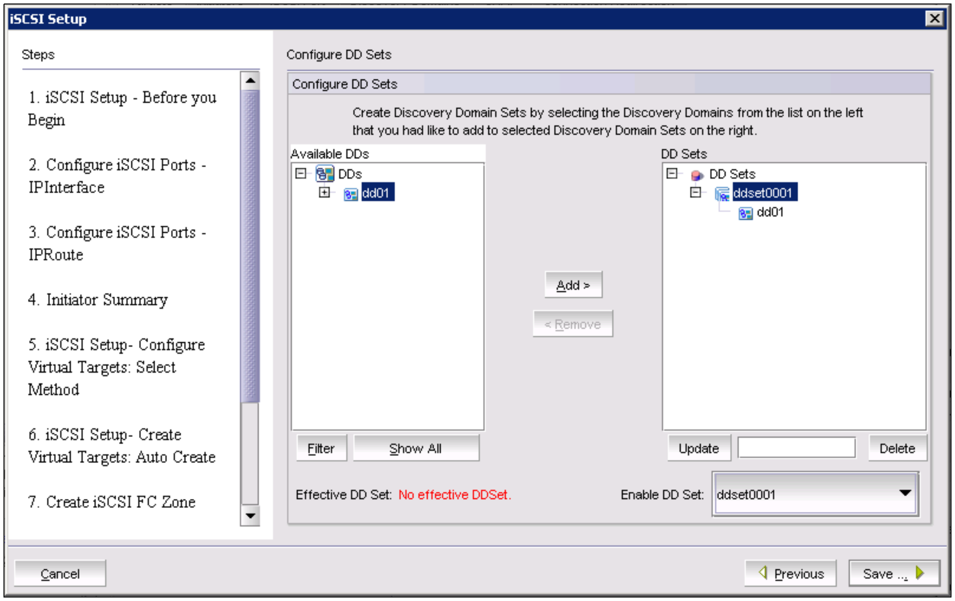
Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

Effective DD Set: No effective DDSet.

Enable DD Set: Select

Figure 11-36 Enable DDSet

14. Select **ddset001**, then click **Save** to proceed. See Figure 11-37.


iSCSI Setup
Steps
1. iSCSI Setup - Before you Begin
2. Configure iSCSI Ports - IPInterface
3. Configure iSCSI Ports - IPRoute
4. Initiator Summary
5. iSCSI Setup- Configure Virtual Targets: Select Method
6. iSCSI Setup- Create Virtual Targets: Auto Create
7. Create iSCSI FC Zone
Configure DD Sets
Configure DD Sets
Available DDs
DDs
dd01
DD Sets
DD Sets
ddset0001
dd01
Add >
< Remove
Filter
Show All
Update
Delete
Cancel
Previous
Save ...

Create Discovery Domain Sets by selecting the Discovery Domains from the list on the left that you had like to add to selected Discovery Domain Sets on the right.

Effective DD Set: No effective DDSet.

Enable DD Set: ddset0001

Figure 11-37 Enable ddset001 and save

15. A window for configuring CHAP authentication opens. Skip this step and click **Finish** to finish the wizard, as shown in Figure 11-38.

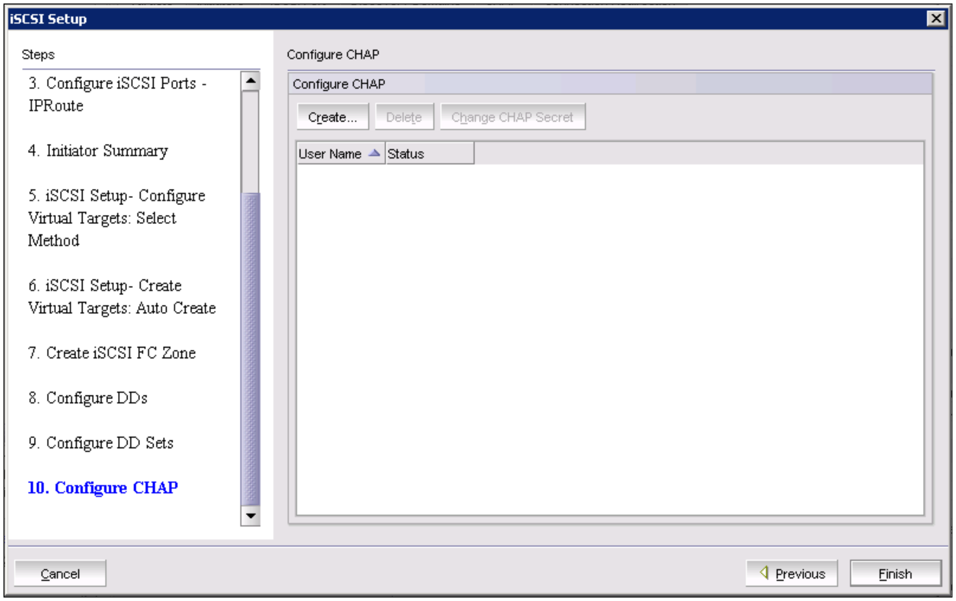
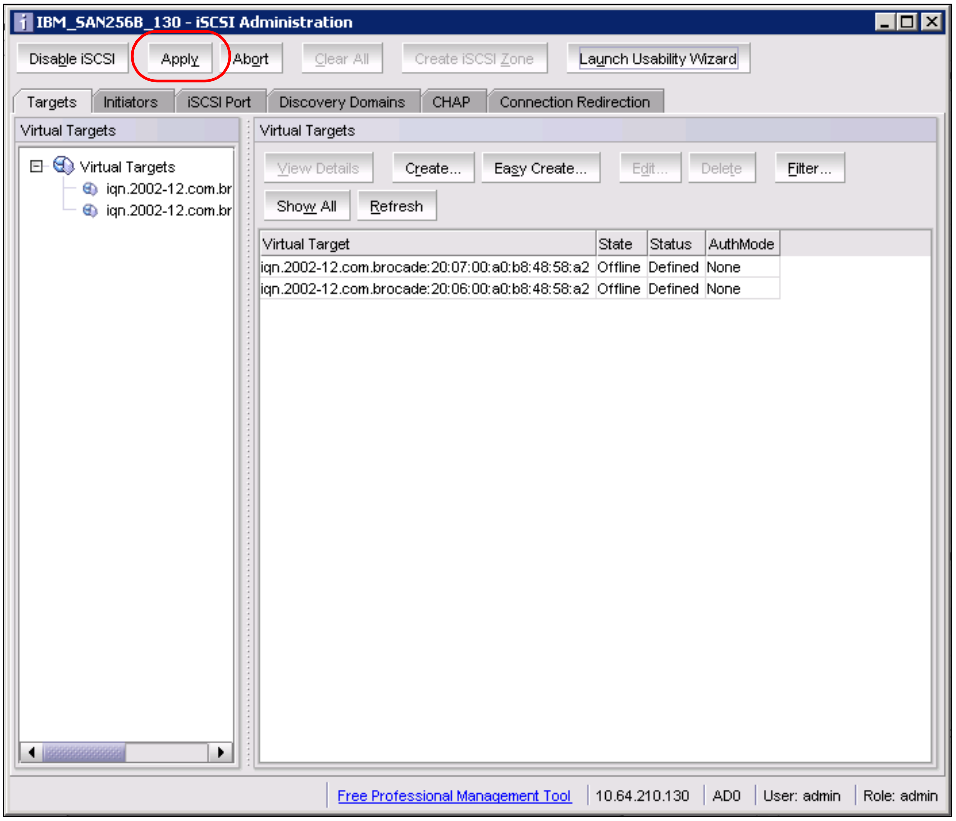


Figure 11-38 CHAP configuration

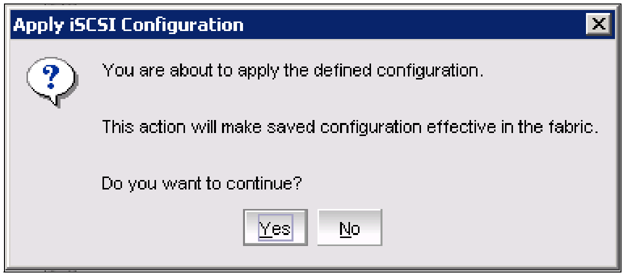
16. This completes the iSCSI Launch Usability Wizard. Return to the port view of the iSCSI administration main page (Figure 11-39). For the configuration created by the wizard to become effective, click **Apply**.



Virtual Target	State	Status	AuthMode
iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2	Offline	Defined	None
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2	Offline	Defined	None

Figure 11-39 Apply changes to iSCSI configuration

17. Click **Yes** in the “Apply iSCSI Configuration” dialog box (Figure 11-40) to confirm the changes.



You are about to apply the defined configuration.

This action will make saved configuration effective in the fabric.

Do you want to continue?

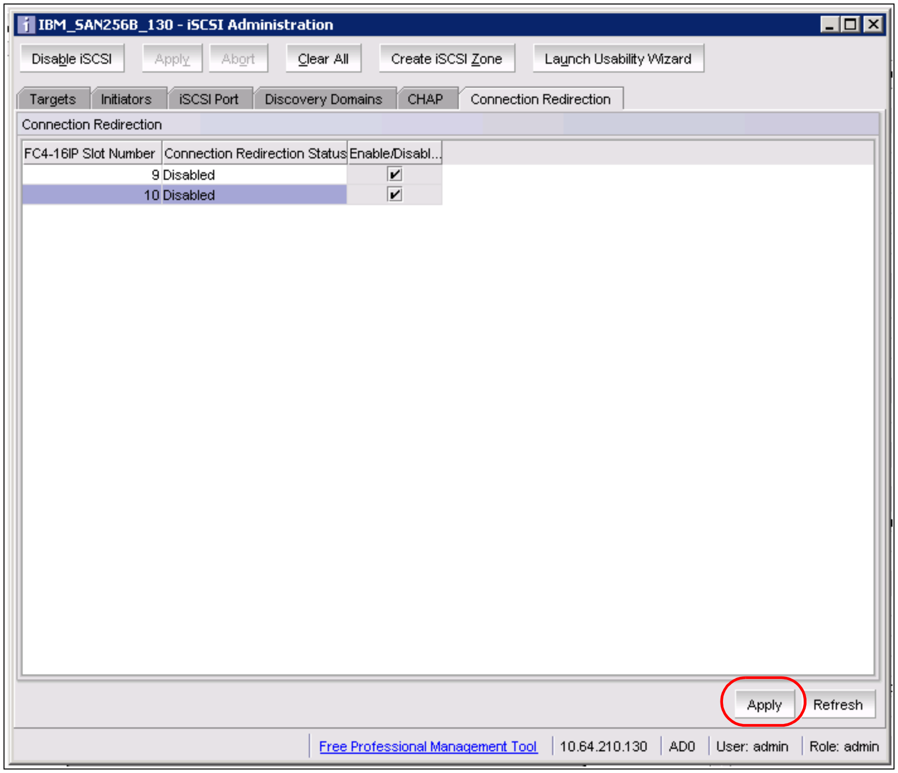
Figure 11-40 Confirm iSCSI configuration changes

11.2.3 Enabling connection redirection

Because we have configured multiple GbE ports, and thereby multiple iSCSI portals, we want to allow the iSCSI gateway service to inform iSCSI initiators of this. This allows for an iSCSI initiator to be configured to connect to only one iSCSI portal and then automatically receive information about other available iSCSI portals. This is useful for both failover situations and load balancing across the GbE ports. In scenarios where control is needed over which iSCSI portals a given iSCSI host can access, this function should not be enabled. All allowed iSCSI portals should be added manually in the iSCSI initiator for target discovery.

> **Note:** When enabling connection redirection ensure that all configured iSCSI portals are reachable through the IP networks used to connect iSCSI hosts to iSCSI portals. This could be limited by IP routing or firewall issues.

1. In the Connection Redirection tab, from the iSCSI Administration GUI, select the **Enable/Disable Connection Redirection** check box.
2. Click **Apply** to commit the configuration. See Figure 11-41.



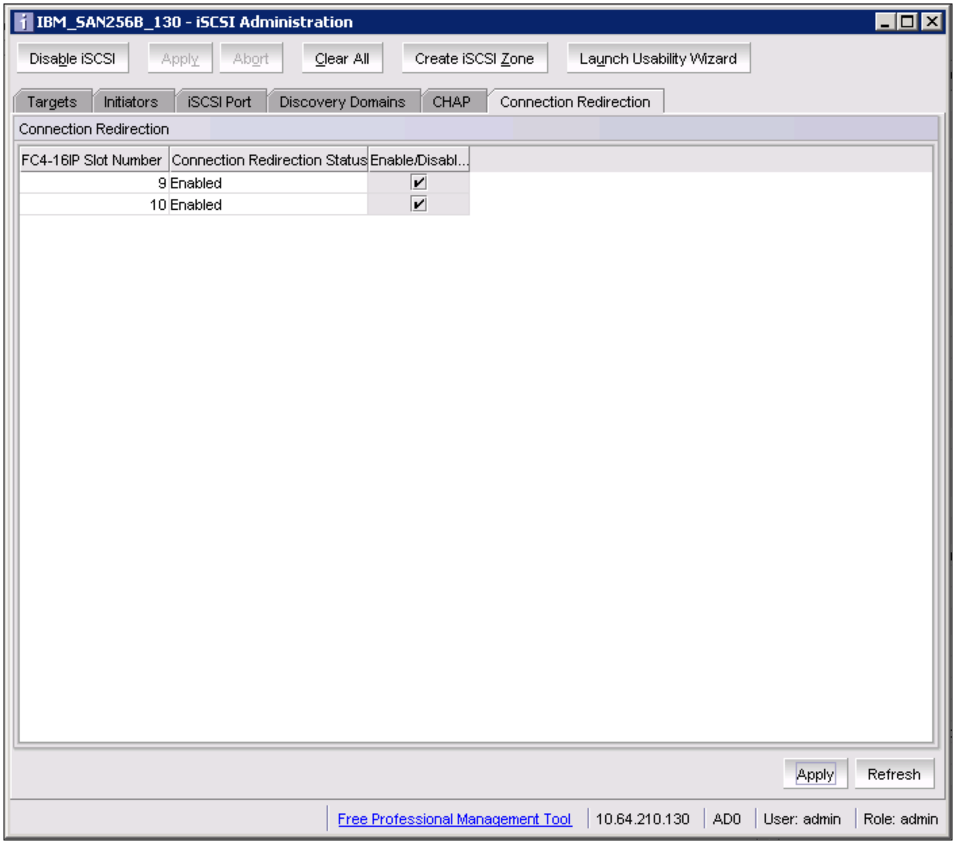
Connection Redirection

FC4-16IP Slot Number	Connection Redirection Status	Enable/Disabl...
9	Disabled	☑
10	Disabled	☑

Free Professional Management Tool | 10.64.210.130 | AD0 | User: admin | Role: admin

Figure 11-41 Enable connection redirection

The Connection Redirection status changes to **Enabled**, as shown in Figure 11-42.



FC4-16IP Slot Number	Connection Redirection Status	Enable/Disabl...
9	Enabled	☑
10	Enabled	☑

Figure 11-42 Connection redirection enabled

11.2.4 Configuring the iSCSI initiator

With the iSCSI gateway service now configured and enabled, the last step is to configure the iSCSI initiator from the host OS, and add it to the dd001 DD.

1. Confirm that no iSCSI initiators are logged into the iSCSI gateway service. Do this from the Initiators tab in the main administration window (Figure 11-43).

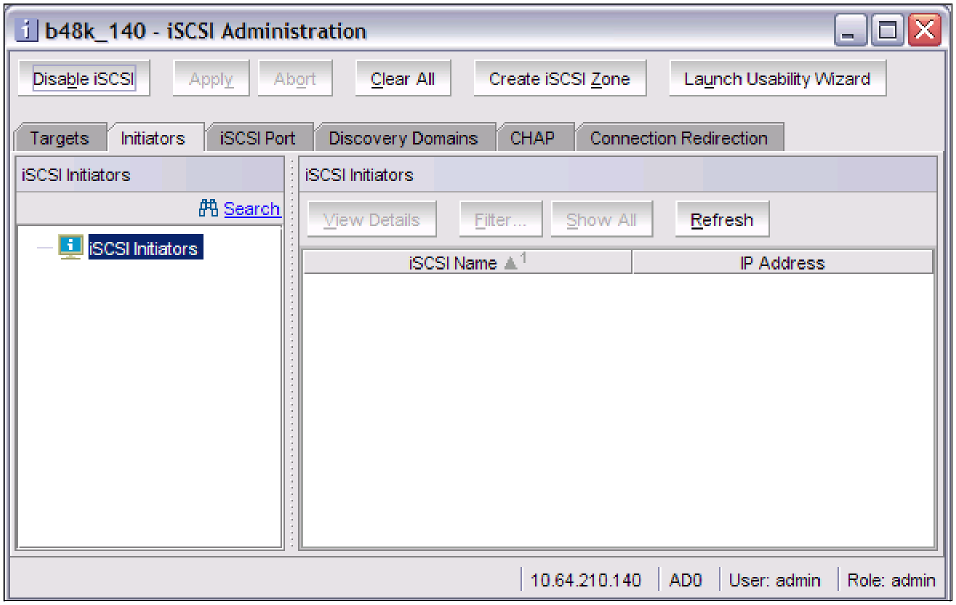


Figure 11-43 Empty iSCSI initiators view

2. Log on to the host where the Microsoft iSCSI initiator Version 2.07 is already installed. Accessing the iSCSI initiator properties reveals the IQN, which we note has a format that is similar to the ones used with iSCSI gateway service. The IQN value is:

   ```
   iqn.1991-05.com.microsoft:ibmbld1-035.englab.brocade.com
   ```

   This is shown in Figure 11-47 on page 288.

Note: The installation and configuration of iSCSI initiators is not within the scope of this book. Only limited information is presented to facilitate the scenarios. For detailed information about a specific iSCSI initiator, refer to the product documentation.

3. Add one of the two configured iSCSI portals to the initiator's discovery list to make the IQN present to the iSCSI gateway. This is done in the Discovery tab, shown in Figure 11-44.

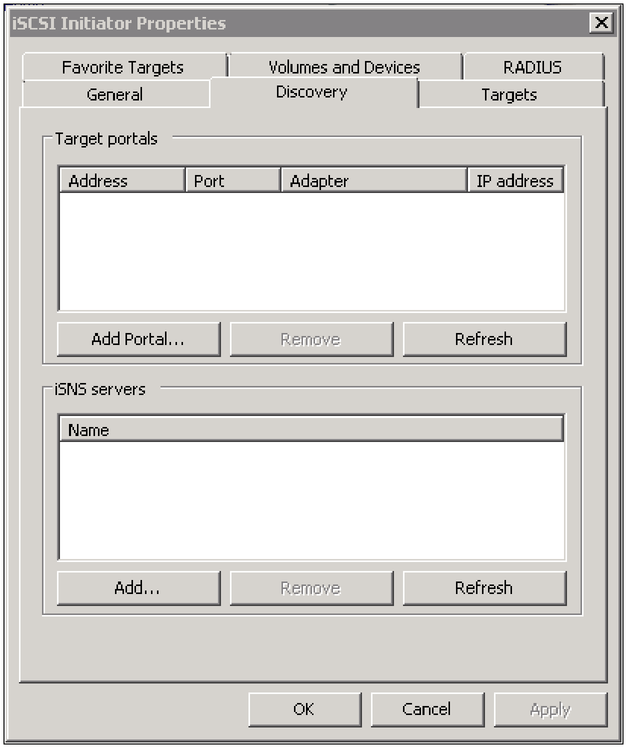
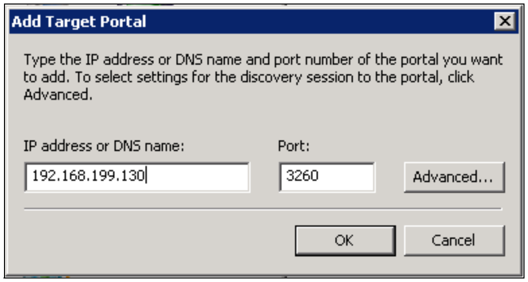


Figure 11-44 iSCSI initiator properties

4. Click **Add Portal** under target portals to enter the IP address of the iSCSI portal associated with GbE port 0 on the iSCSI blade (IP: 192.168.199.130). The port number remains at the default value of 3260, and no advanced settings need to be configured. See Figure 11-45.


Add Target Portal

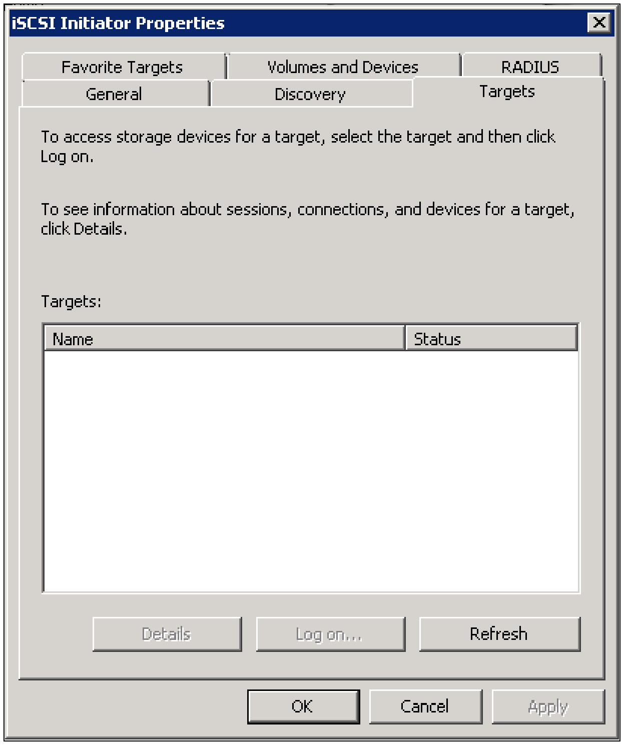
Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.

IP address or DNS name: 192.168.199.130

Port: 3260

Figure 11-45 Add iSCSI portal to initiator

With the iSCSI portal added, notice that no iSCSI targets are visible yet. This is because no access is allowed through any DDs. Although no targets are visible, the iSCSI initiator has now logged into the iSCSI gateway service. See Figure 11-46.



To access storage devices for a target, select the target and then click Log on.

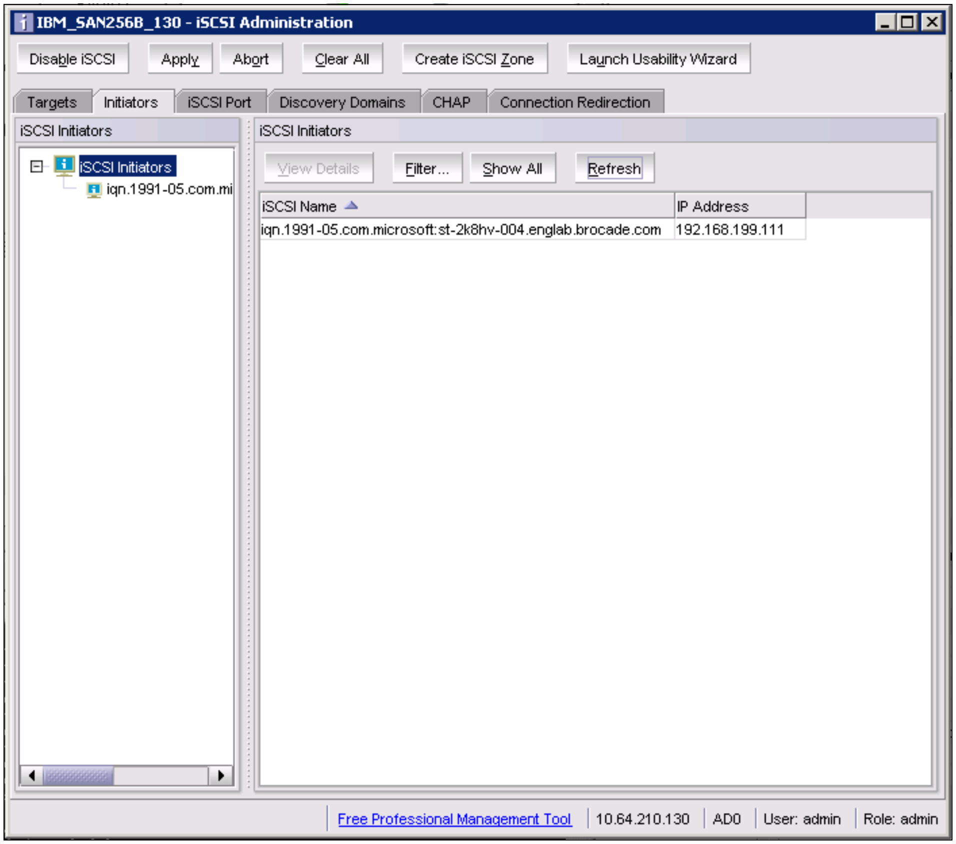
To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status

Figure 11-46 No targets discovered

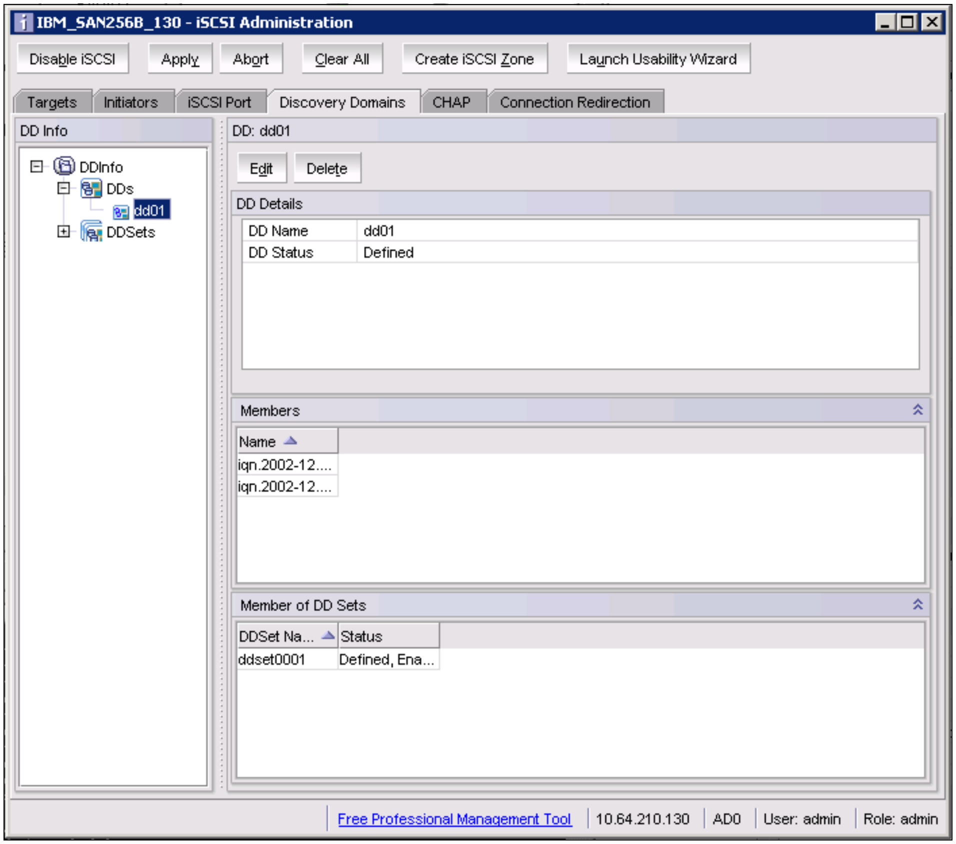
5. Access the iSCSI administration window on the SAN256B Web Tools to confirm that the iSCSI initiator is logged in. View this on the Initiators tab (Figure 11-47).



iSCSI Name	IP Address
iqn.1991-05.com.microsoft:st-2k8hv-004.englab.brocade.com	192.168.199.111

Figure 11-47 iSCSI initiator listing

6. To allow the targets to be discovered at the host, we must include the initiator in the dd001 DD. Go to the Discovery Domains tab. From here we expand the **DDs** listing and select **dd001**, as shown in Figure 11-48.



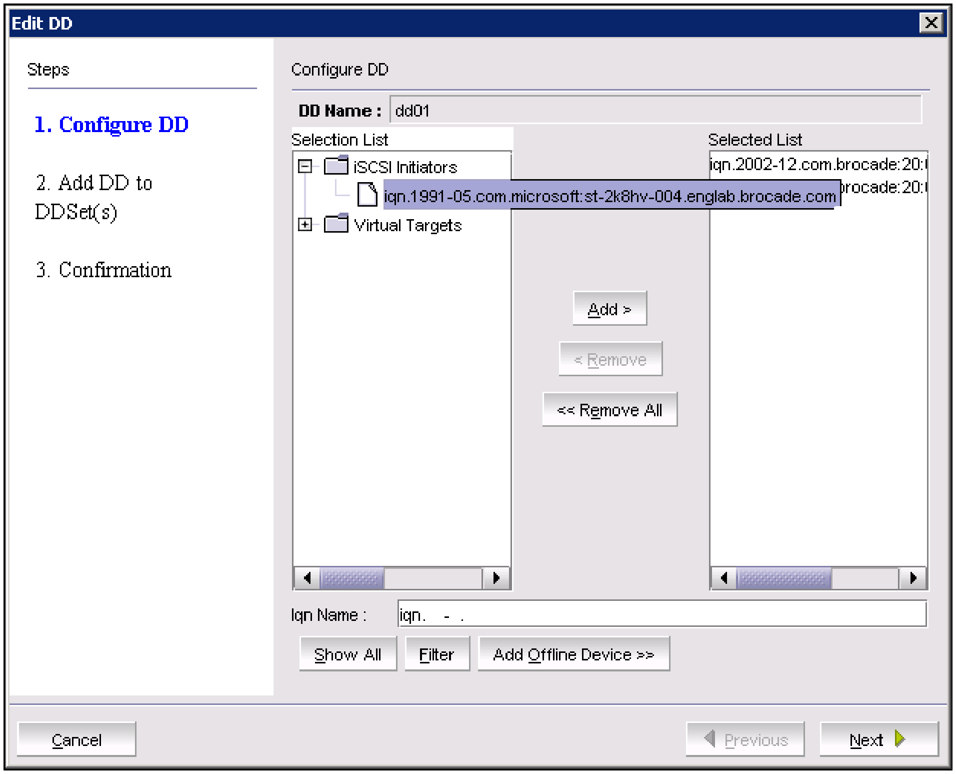
DD Name	dd01
DD Status	Defined

Name
iqn.2002-12....
iqn.2002-12....

DDSet Na...	Status
ddset0001	Defined, Ena...

Figure 11-48 DD configuration

7. Click **Edit to** open the Edit DD wizard, which enables us to modify the DD. Note that the initiator is now available for selection, as shown in Figure 11-49.

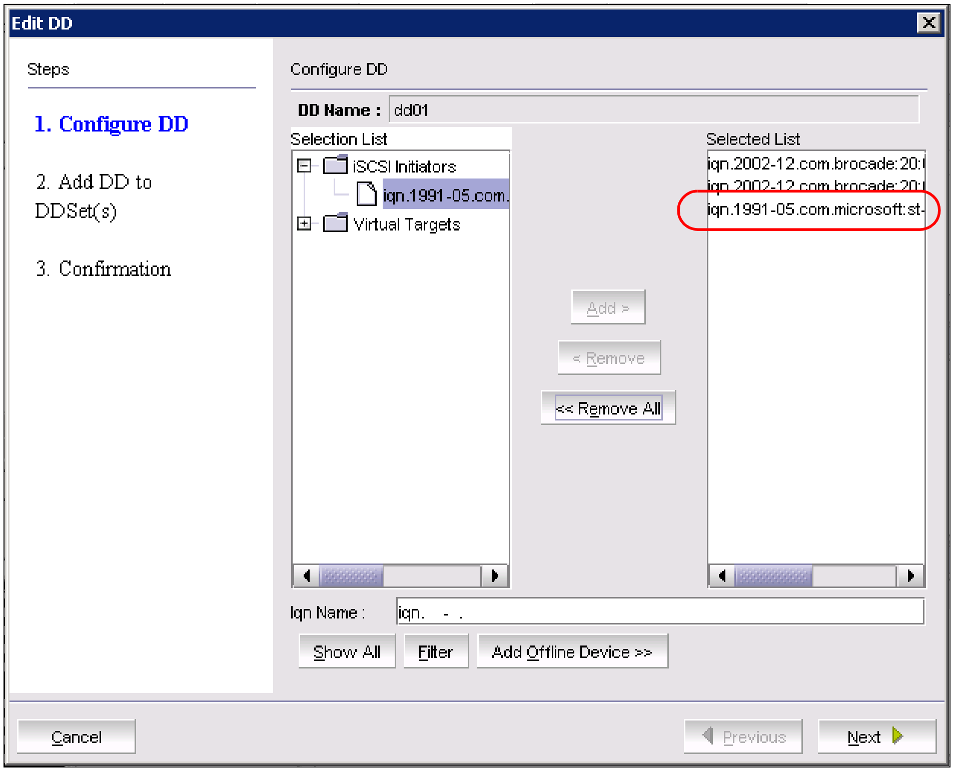


DD Name : dd01

Iqn Name : iqn. - .

Figure 11-49 Edit DD

8. Add the initiator to the Selected List by highlighting it and clicking **Add**, as in Figure 11-50.



DD Name : dd01

Selection List: iqn.1991-05.com.

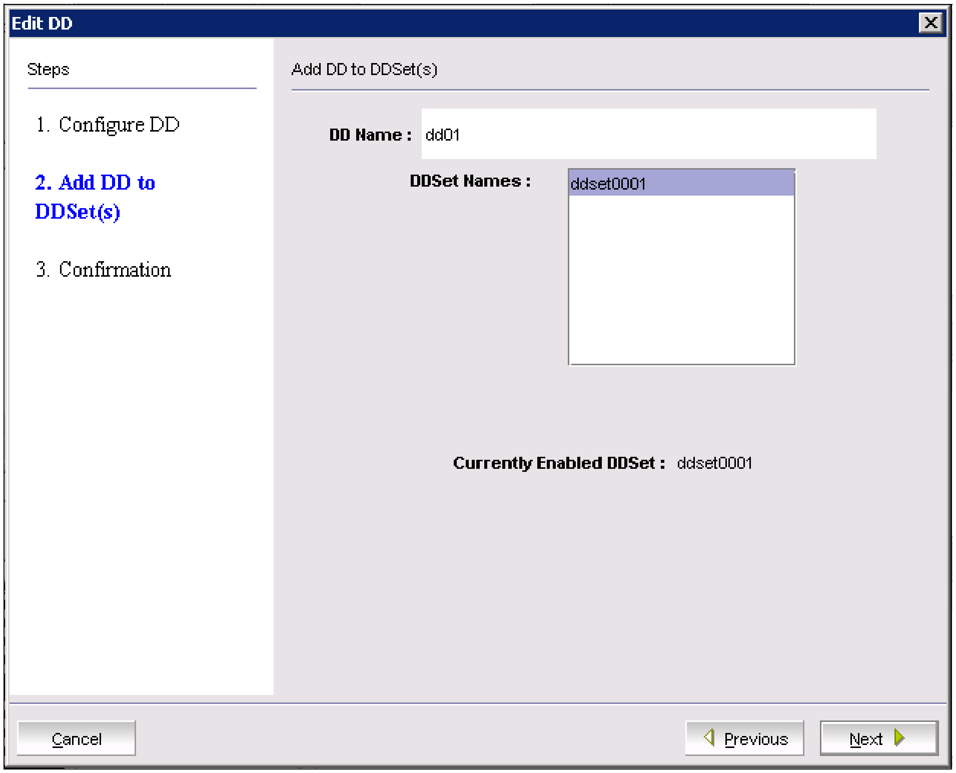
Selected List:
iqn.2002-12.com.brocade:20:
iqn.2002-12.com.brocade:20:
iqn.1991-05.com.microsoft:st-

Iqn Name : iqn. - .

Figure 11-50 Add Initiator

Click **Next**.

9. Add DDs to DDSets, as shown in Figure 11-51. Because dd001 is already included in DDSet ddset001, no changes are needed.


Edit DD

Steps

1. Configure DD

2. Add DD to DDSet(s)

3. Confirmation

Add DD to DDSet(s)

DD Name : dd01

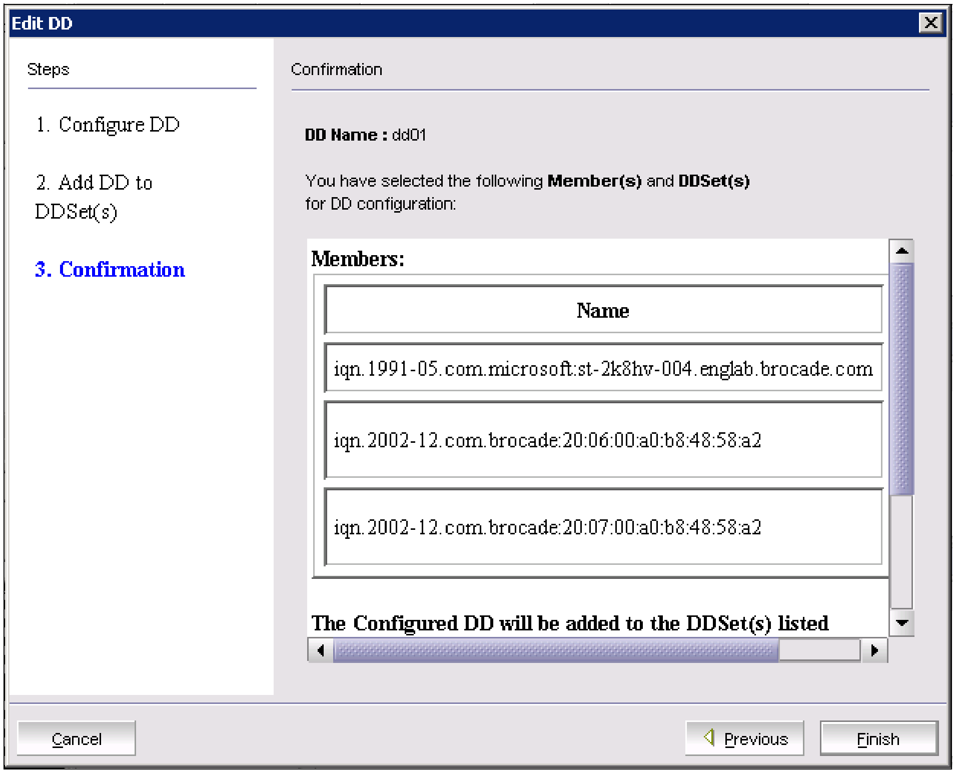
DDSet Names : ddset0001

Currently Enabled DDSet : ddset0001

Figure 11-51 Add DD to DDSet

Click **Next**.

The confirmation window opens, as shown in Figure 11-52.



DD Name : dd01

You have selected the following **Member(s)** and **DDSet(s)** for DD configuration:

Members:

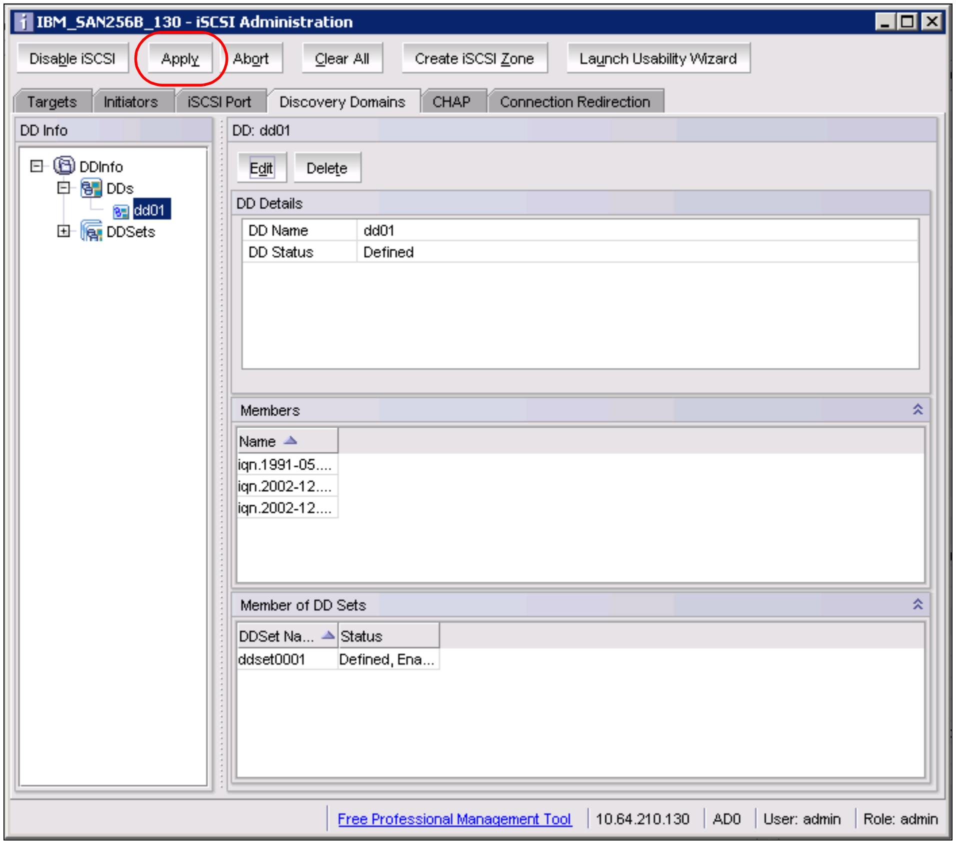
Name
iqn.1991-05.com.microsoft:st-2k8hv-004.englab.brocade.com
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2
iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2

The Configured DD will be added to the DDSet(s) listed

Figure 11-52 Edit DD confirmation window

10.Confirm the new DD configuration and click **Finish** to complete the DD modification wizard.

11. At the main window (Figure 11-53), we click **Apply** to commit the new configuration.


IBM_SAN256B_130 - iSCSI Administration

DD Details

DD Name	dd01
DD Status	Defined

Members

Name
iqn.1991-05....
iqn.2002-12....
iqn.2002-12....

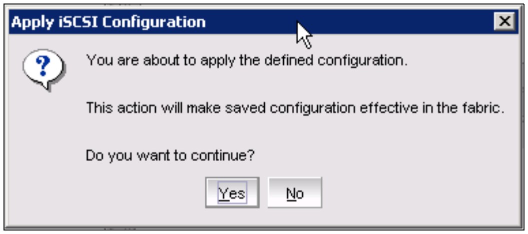
Member of DD Sets

DDSet Na...	Status
ddset0001	Defined, Ena...

Free Professional Management Tool | 10.64.210.130 | AD0 | User: admin | Role: admin

Figure 11-53 Apply DD modifications

12. An Apply Configuration dialog box (Figure 11-54) opens. Click **Yes** to continue.


Apply iSCSI Configuration

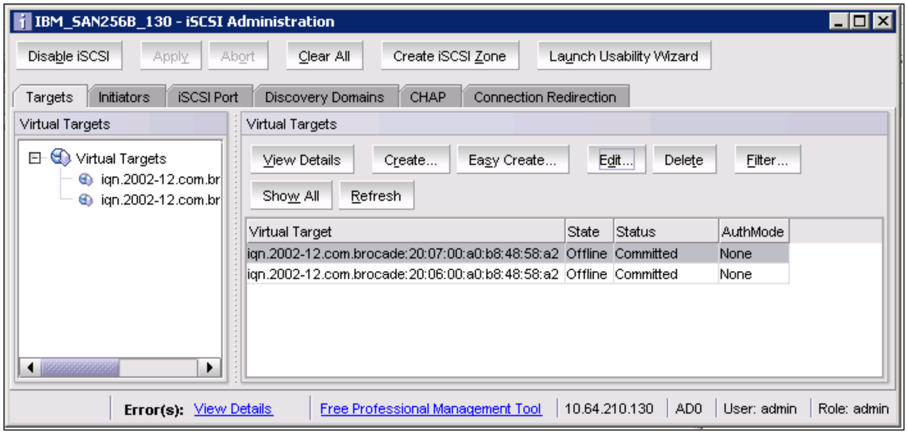
You are about to apply the defined configuration.

This action will make saved configuration effective in the fabric.

Do you want to continue?

Figure 11-54 Apply Configuration dialog box

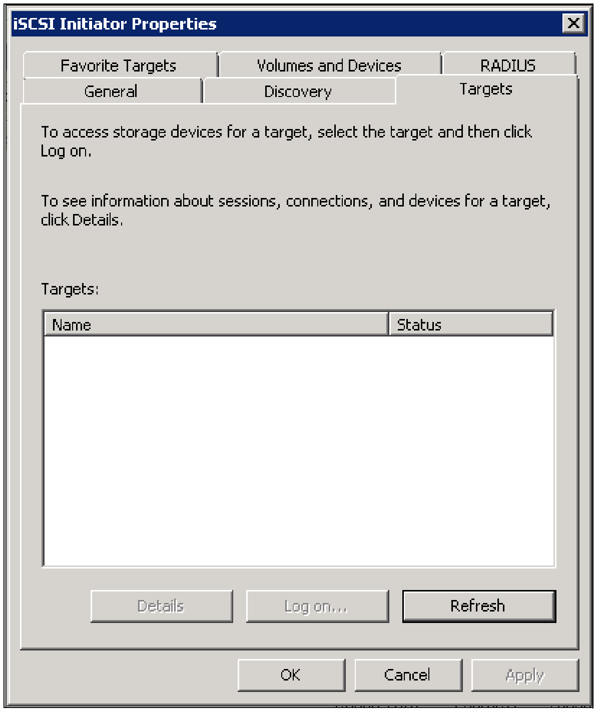
At this point the targets are committed, but offline because they do not have any LUNs mapped to them as shown in Figure 11-55.



Virtual Target	State	Status	AuthMode
iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2	Offline	Committed	None
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2	Offline	Committed	None

Figure 11-55 Offline virtual targets

If you check with the Windows iSCSI initiator Properties and Disk Management, you cannot see any Virtual Targets (Figure 11-56) or disks (Figure 11-57 on page 296).



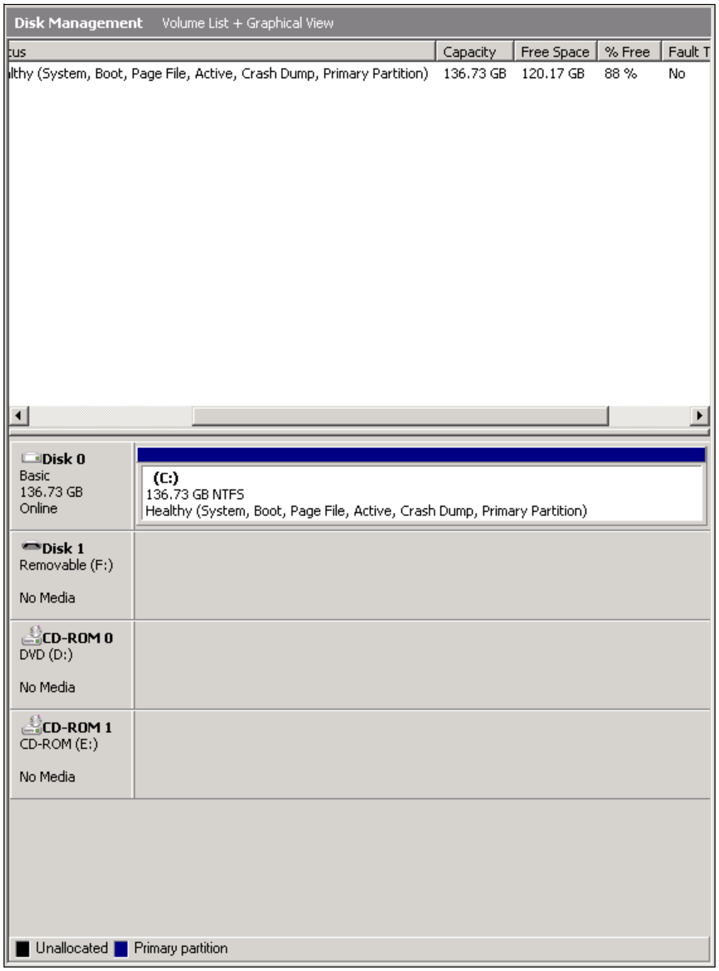
To access storage devices for a target, select the target and then click Log on.

To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status

Figure 11-56 Virtual Targets undiscovered display



Disk Management Volume List + Graphical View

tus	Capacity	Free Space	% Free	Fault T
lthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)	136.73 GB	120.17 GB	88 %	No

Disk 0
Basic
136.73 GB
Online

(C:)
136.73 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

Disk 1
Removable (F:)

No Media

CD-ROM 0
DVD (D:)

No Media

CD-ROM 1
CD-ROM (E:)

No Media

■ Unallocated 🟦 Primary partition

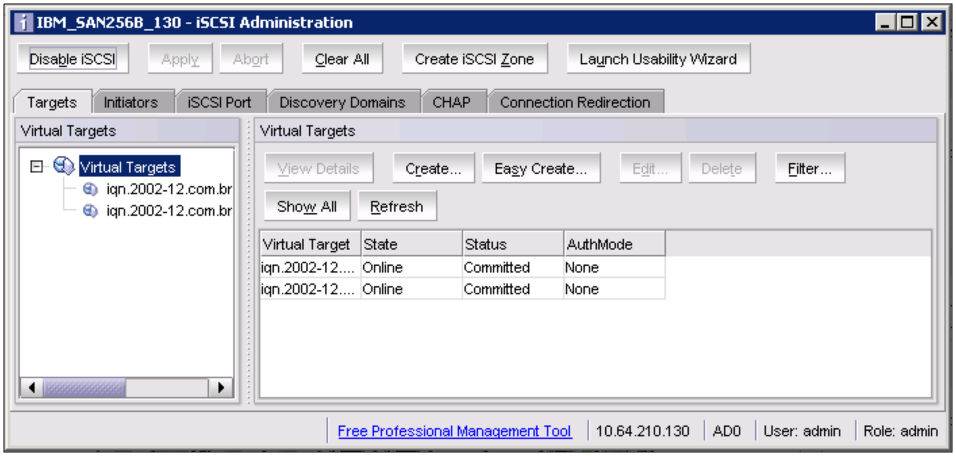
Figure 11-57 Initial Windows Disk Management

13. Map the available LUNs on the storage system to LUNs on the virtual target. Use the CLI and **iscsicfg** commands, shown in Example 11-1.

Example 11-1 Adding LUNs to Virtual Target

```
IBM_SAN256B_130:admin> iscsicfg --show tgt
Number of records found: 2

Name:                   iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2
State/Status:           Offline/Committed

Name:                   iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2
State/Status:           Offline/Committed

IBM_SAN256B_130:admin> iscsicfg --show lun
No records were found in the database.

IBM_SAN256B_130:admin> iscsicfg --add lun -t
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2 -w 20:06:00:a0:b8:48:58:a2 -l 1,2:1,2
The operation completed successfully.

IBM_SAN256B_130:admin> iscsicfg --add lun -t
iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2 -w 20:07:00:a0:b8:48:58:a2 -l 1,2:1,2
The operation completed successfully.

IBM_SAN256B_130:admin> iscsicfg --commit all
This will commit ALL database changes made to all iSCSI switches in fabric.
This could be a long-running operation.
Continue (yes, y, no, n) [n]: y
The operation completed successfully.

IBM_SAN256B_130:admin> iscsicfg --show lun
Number of targets found: 2

Target: iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2
Number of LUN Maps: 2
FC WWN                          Virtual LUN(s)      Physical LUN(s)
20:06:00:a0:b8:48:58:a2         1                   1
20:06:00:a0:b8:48:58:a2         2                   2

Target: iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2
Number of LUN Maps: 2
FC WWN                          Virtual LUN(s)      Physical LUN(s)
20:07:00:a0:b8:48:58:a2         1                   1
20:07:00:a0:b8:48:58:a2         2                   2
```

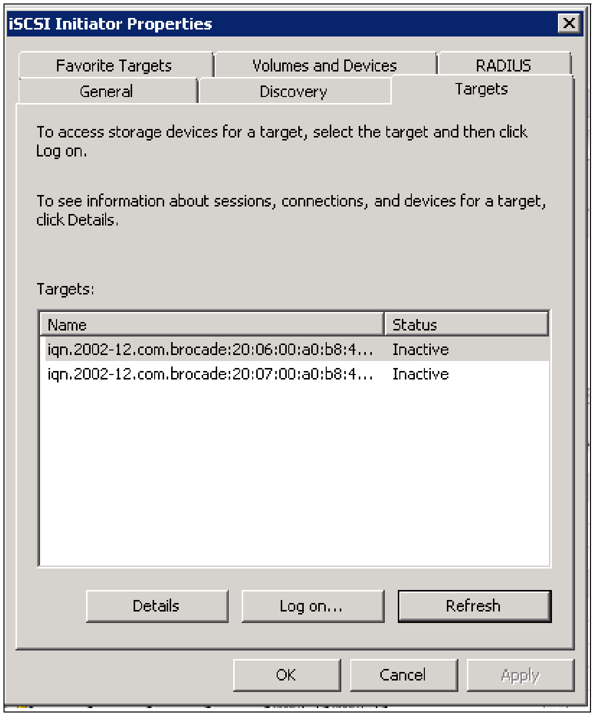
The Virtual Targets are now online, as shown in Figure 11-58.



Virtual Target	State	Status	AuthMode
iqn.2002-12....	Online	Committed	None
iqn.2002-12....	Online	Committed	None

Figure 11-58 Virtual Targets online

14. With proper access control now in place, rescan for iSCSI targets on our host by clicking **Refresh** on the Targets tab of the iSCSI Initiator Properties window (Figure 11-58). The two iSCSI targets are now visible.



To access storage devices for a target, select the target and then click Log on.

To see information about sessions, connections, and devices for a target, click Details.

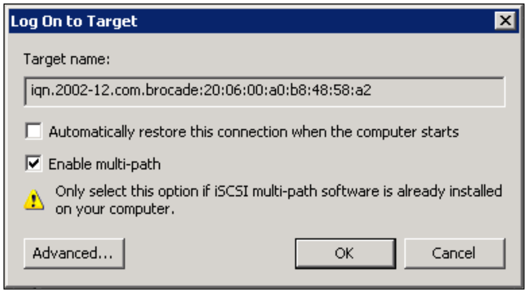
Targets:

Name	Status
iqn.2002-12.com.brocade:20:06:00:a0:b8:4...	Inactive
iqn.2002-12.com.brocade:20:07:00:a0:b8:4...	Inactive

Figure 11-59 Virtual Targets visible

15. The status of Inactive indicates that the targets are not yet accessible to the host OS. To connect the first target, select the target and click **Log on**, which opens a dialog box where connection properties can be set.

    Earlier, we enabled connection redirection for the iSCSI gateway service. We now activate multi-path support on the initiator to benefit from the redirection. Because this is a test setup, do not reconnect the target across host reboots. No advanced properties must be configured, and we confirm the connection by clicking **OK**. See Figure 11-60.



Log On to Target

Target name:

iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2

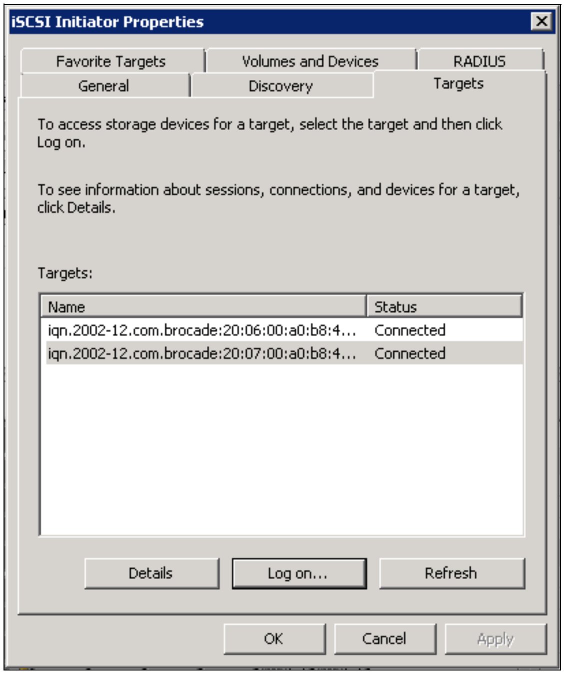
□ Automatically restore this connection when the computer starts

☑ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

Figure 11-60 Log on to Target dialog box

By repeating the connection process for the second target, both targets are now connected to the host, as seen in Figure 11-61.



iSCSI Initiator Properties

To access storage devices for a target, select the target and then click Log on.

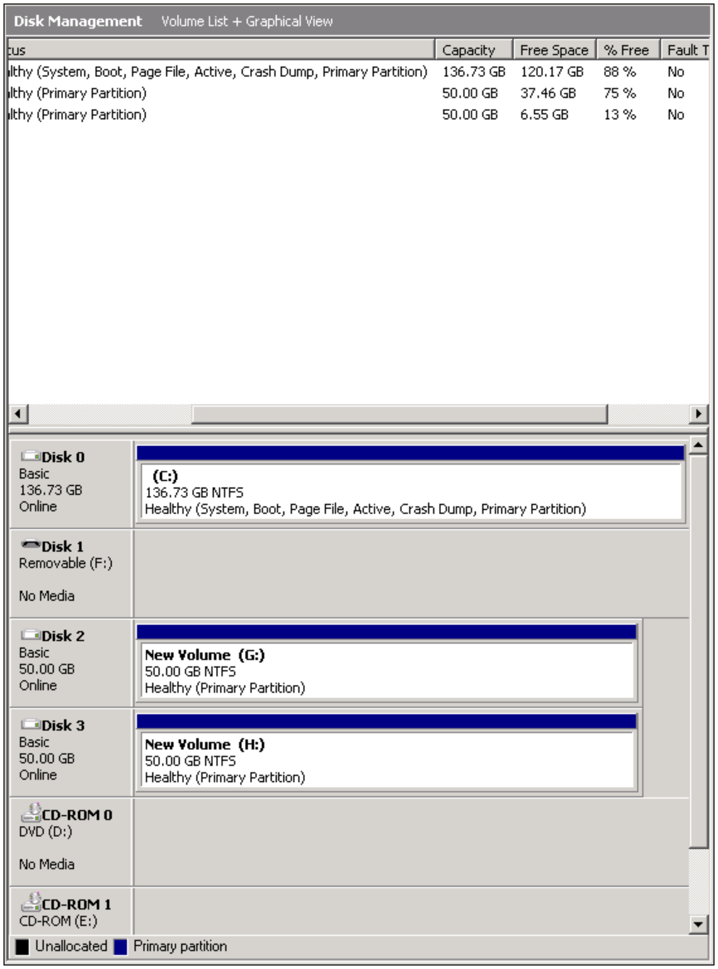
To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.2002-12.com.brocade:20:06:00:a0:b8:4...	Connected
iqn.2002-12.com.brocade:20:07:00:a0:b8:4...	Connected

Figure 11-61 iSCSI targets connected

16. With both iSCSI targets connected, scan for disk devices from the host disk management, and the two new disk devices come online (disk 2 and disk 3). These can then be initialized, partitioned, and formatted. See Figure 11-62.



Disk Management   Volume List + Graphical View

tus	Capacity	Free Space	% Free	Fault T
lthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)	136.73 GB	120.17 GB	88 %	No
lthy (Primary Partition)	50.00 GB	37.46 GB	75 %	No
lthy (Primary Partition)	50.00 GB	6.55 GB	13 %	No

Disk 0
Basic
136.73 GB
Online

(C:)
136.73 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

Disk 1
Removable (F:)

No Media

Disk 2
Basic
50.00 GB
Online

New Volume (G:)
50.00 GB NTFS
Healthy (Primary Partition)

Disk 3
Basic
50.00 GB
Online

New Volume (H:)
50.00 GB NTFS
Healthy (Primary Partition)

CD-ROM 0
DVD (D:)

No Media

CD-ROM 1
CD-ROM (E:)

■ Unallocated 🟦 Primary partition

Figure 11-62 iSCSI disk devices come online from the host

This concludes the initial deployment of the iSCSI blade for the SAN256B director.

11.3 Configuring the iSCSI gateway service

In this section, we show how basic configuration tasks are done after the initial deployment of the iSCSI blade.

11.3.1 CHAP authentication

Besides DD configuration, security between the iSCSI initiator and the ISCSI gateway can be further strengthened by the use of CHAP. This approach prohibits rogue hosts that spoof an IQN to gain access to an iSCSI VT. The iSCSI gateway service on the iSCSI blade for the SAN256B director supports the following three strategies for CHAP authentication:

- One way

  Only the iSCSI VT authenticates the iSCSI session.

- Mutual

  Both the iSCSI initiator and the iSCSI VT authenticates the iSCSI session.

- Binding user names

  iSCSI VTs can be configured to only allow specific CHAP users access.

Configuring iSCSI VTs for CHAP authentication

In our example, we configure the two iSCSI VTs created in the initial deployment scenario earlier in this chapter for one-way CHAP authentication. We do this by first creating a new CHAP record that consists of a CHAP user and an associated CHAP secret.

1. Click **Create**, which is on the CHAP tab of the iSCSI Administration window of the Web Tools GUI, as shown in Figure 11-63.

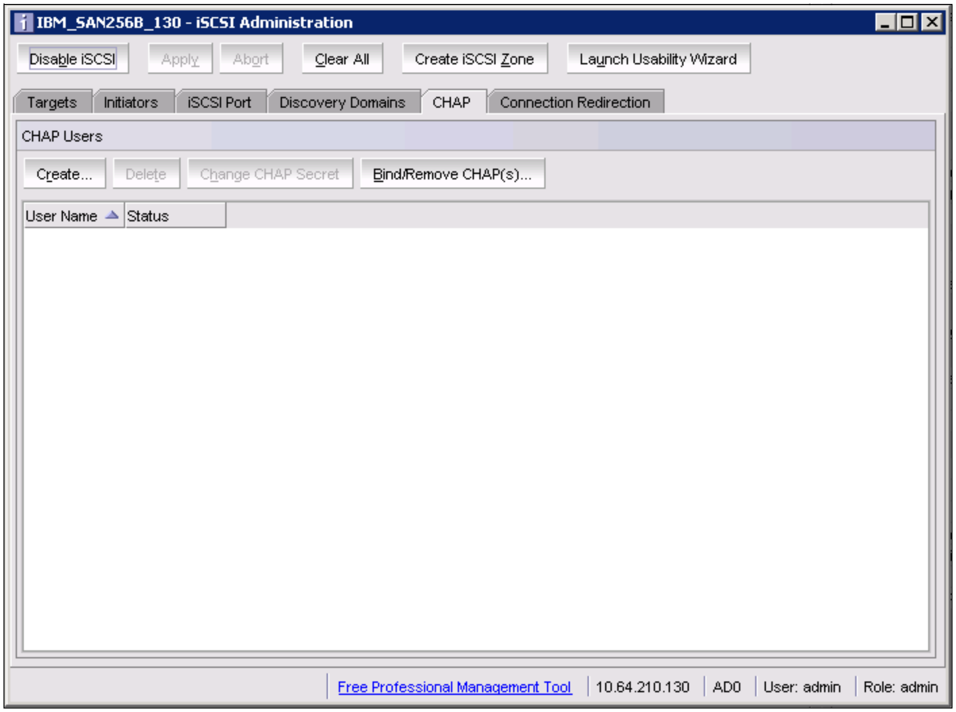
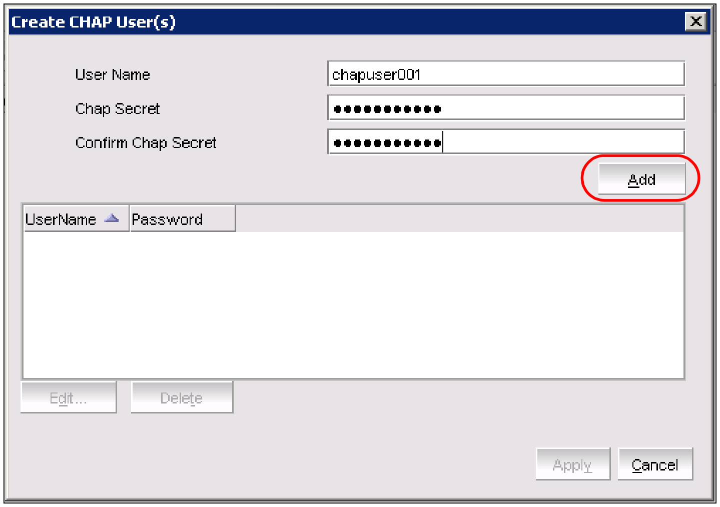


Figure 11-63 Create CHAP record

2. Type in the user name `chapuser001` and the CHAP secret, which we set to `chap_secret0001`. See Figure 11-64. Click **Add** to add the new user to the list.



Create CHAP User(s)

User Name: chapuser001

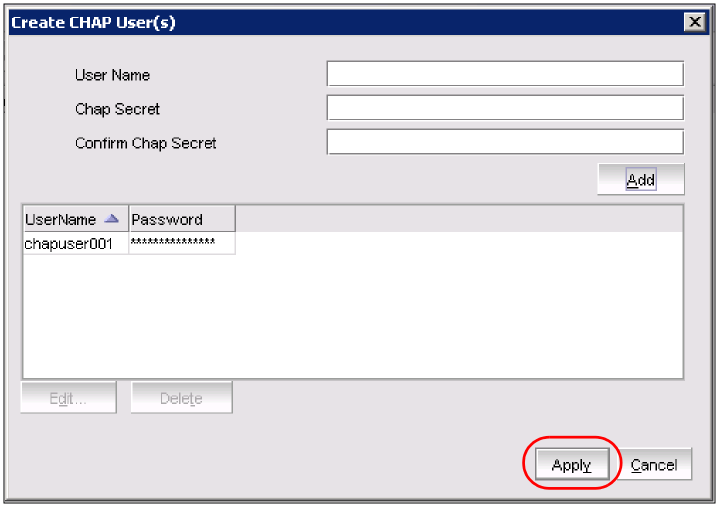
Chap Secret: ●●●●●●●●●●●

Confirm Chap Secret: ●●●●●●●●●●●

UserName	Password

Figure 11-64 Entering information for new CHAP user

3. Click **Apply** to commit the new changes. See Figure 10-64.



Create CHAP User(s)

User Name:

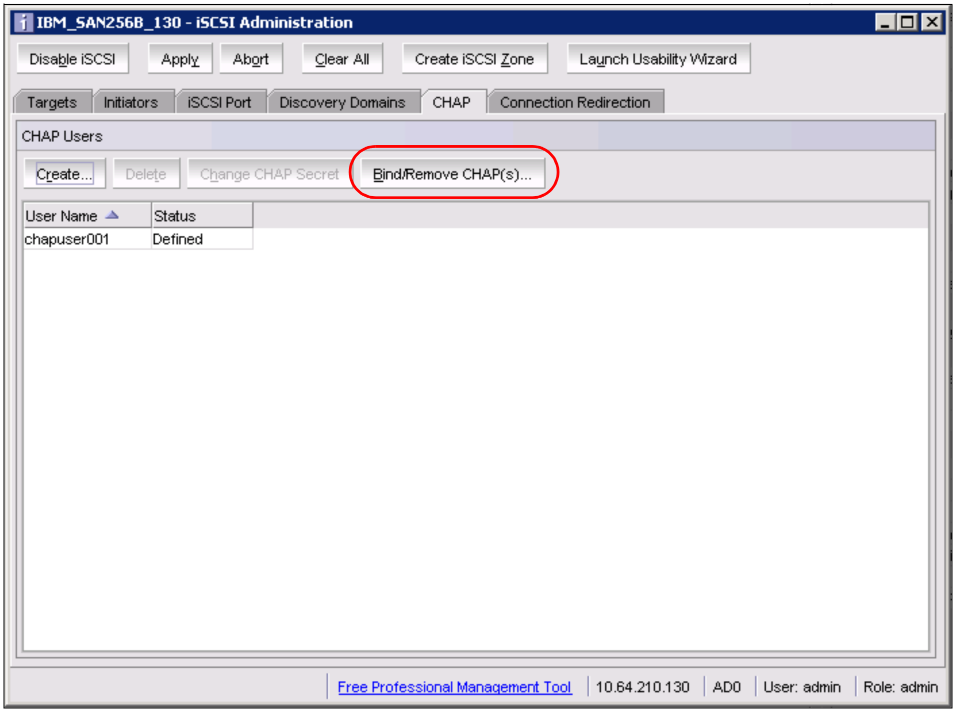
Chap Secret:

Confirm Chap Secret:

UserName	Password
chapuser001	***************

Figure 11-65 Committing CHAP user changes

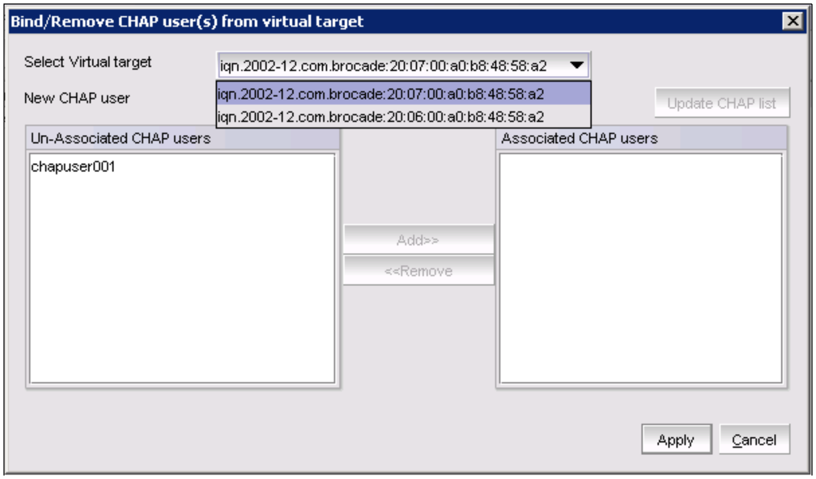
4. On the CHAP tab, where our CHAP user is now listed, configure the two iSCSI VTs for CHAP authentication by clicking **Bind/Remove CHAP(s)**. See Figure 11-66.



User Name	Status
chapuser001	Defined

Figure 11-66 Newly created CHAP user listed

5. A window opens to show where CHAP users can be associated with iSCSI VTs. From the Select Virtual Target list, select the first iSCSI VT, shown in Figure 11-67.


Bind/Remove CHAP user(s) from virtual target

Select Virtual target: iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2

iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2

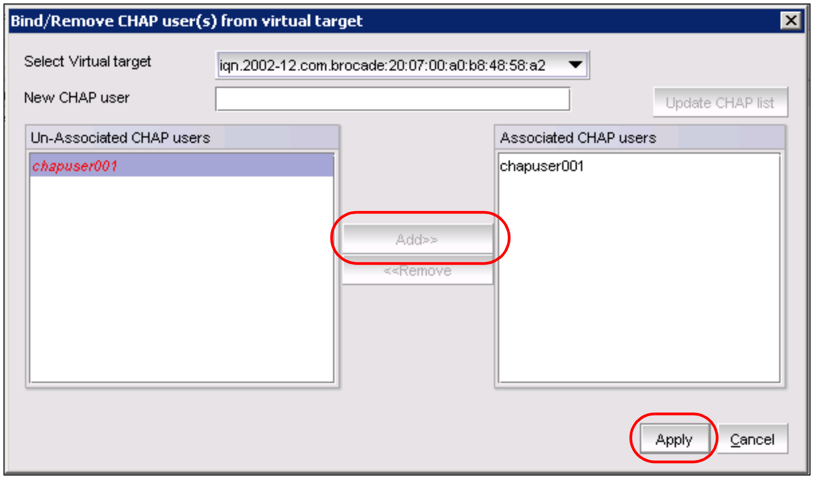
New CHAP user:

Un-Associated CHAP users: chapuser001

Associated CHAP users:

Figure 11-67 iSCSI VT selected for CHAP configuration

6. Select **chapuser001** in the Un-Associated CHAP users list, click **Add** to add chapuser001 to the Associated CHAP users list, and click **Apply** to commit the change. See Figure 11-68.


Bind/Remove CHAP user(s) from virtual target

Select Virtual target: iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2

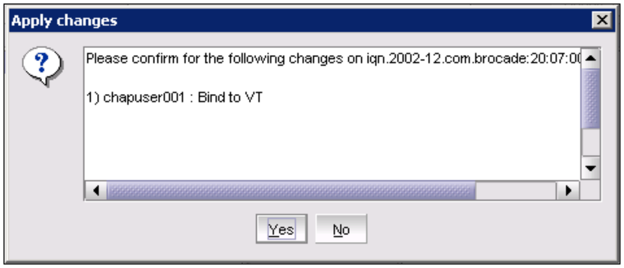
New CHAP user:

Un-Associated CHAP users: chapuser001

Associated CHAP users: chapuser001

Figure 11-68 Associate CHAP users to iSCSI VTs

The “Apply changes” dialog box (Figure 11-69) opens, where we confirm the binding of chapuser001 to the VT. Click **Yes**.



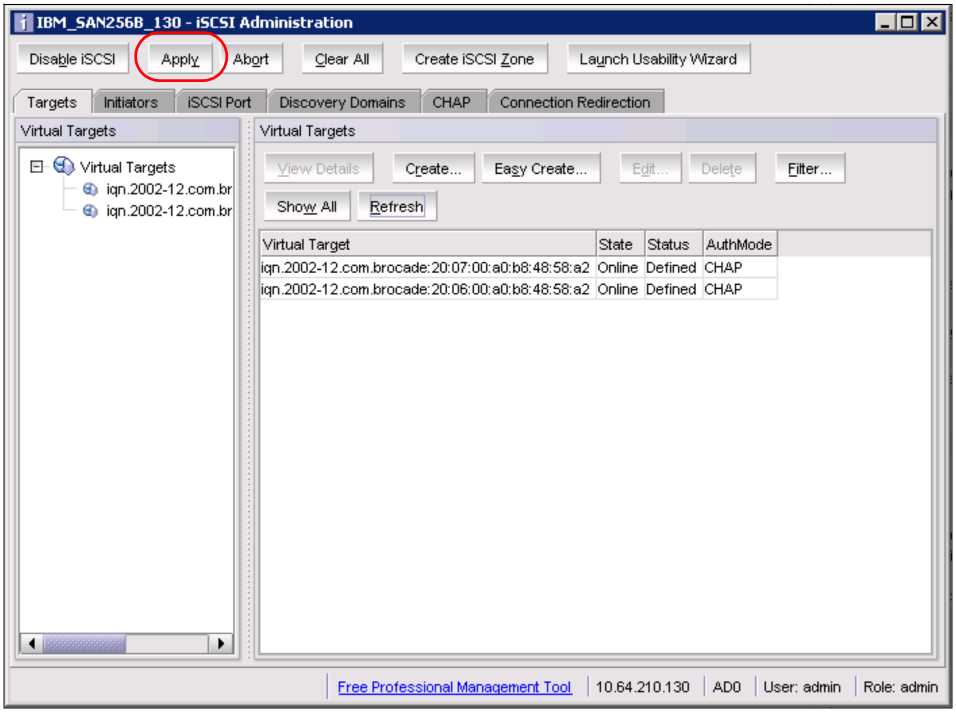
Apply changes

Please confirm for the following changes on iqn.2002-12.com.brocade:20:07:0(

1) chapuser001 : Bind to VT

Figure 11-69 Binding Confirmation dialog box

7. Repeat the process for the other iSCSI VT.
8. Returning to the main iSCSI administration window, select the **Targets** tab and note that the two iSCSI VTs are now listed as having CHAP as the authentication method. See Figure 11-70. Click **Apply** to commit the configuration.

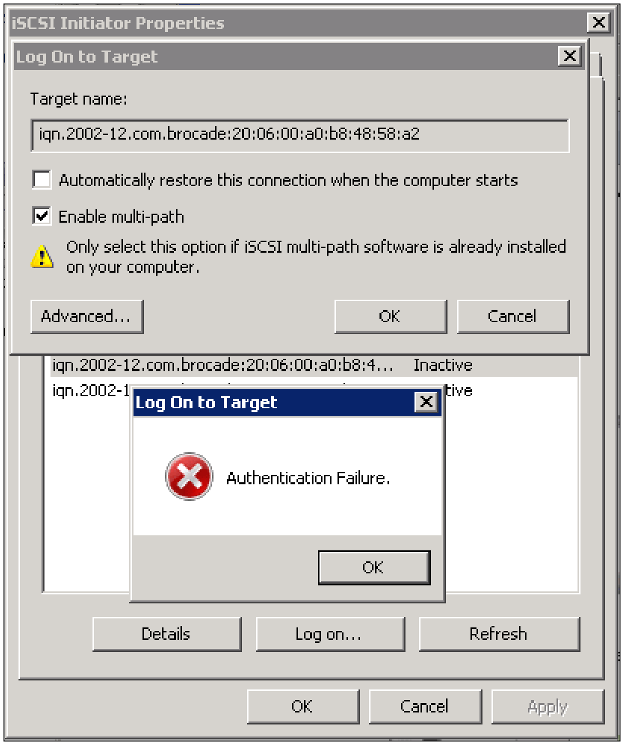


IBM_SAN256B_130 - iSCSI Administration

Virtual Target	State	Status	AuthMode
iqn.2002-12.com.brocade:20:07:00:a0:b8:48:58:a2	Online	Defined	CHAP
iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2	Online	Defined	CHAP

Figure 11-70 iSCSI VTs listed with CHAP as authentication method

The next time an iSCSI initiator attempts to log on to one of the targets with CHAP authentication enabled, it will be denied if CHAP is not properly configured on the host driver. See Figure 11-71.



iSCSI Initiator Properties

Log On to Target

Target name:

iqn.2002-12.com.brocade:20:06:00:a0:b8:48:58:a2

☐ Automatically restore this connection when the computer starts

☑ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

iqn.2002-12.com.brocade:20:06:00:a0:b8:4...	Inactive
iqn.2002-1	tive

Log On to Target

Authentication Failure.

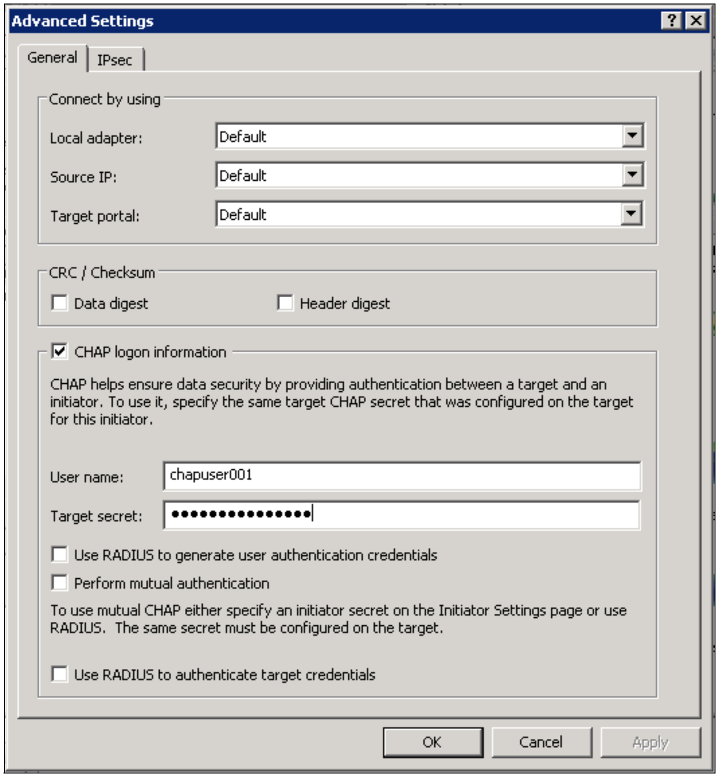
Figure 11-71 Microsoft iSCSI initiator log on error message

With the Microsoft iSCSI initiator, CHAP can be configured in either of the following ways:

– For the initiator by using the General tab of the iSCSI initiator properties.

– On a per-target basis through the “Advanced Options” window available when logging on to a target.

9. Enter the CHAP user name in the User name text box and the CHAP secret in the Target secret text box. See Figure 11-72.



Connect by using

Local adapter: Default

Source IP: Default

Target portal: Default

CRC / Checksum

□ Data digest □ Header digest

☑ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: chapuser001

Target secret: ●●●●●●●●●●●●●●●

□ Use RADIUS to generate user authentication credentials

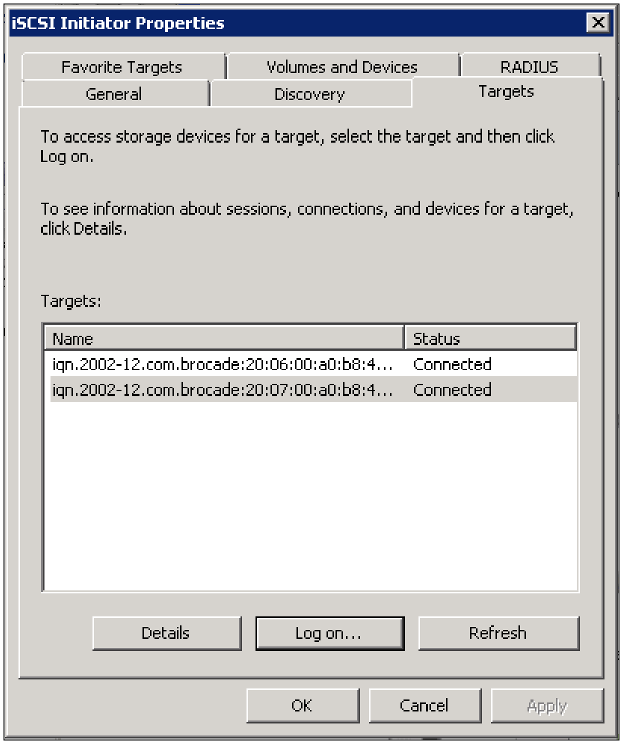
□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

Figure 11-72 CHAP information specified during log on to target

After successfully authenticated, the targets are connected to the host and the host can access the FC storage. See Figure 11-73.



To access storage devices for a target, select the target and then click Log on.

To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.2002-12.com.brocade:20:06:00:a0:b8:4...	Connected
iqn.2002-12.com.brocade:20:07:00:a0:b8:4...	Connected

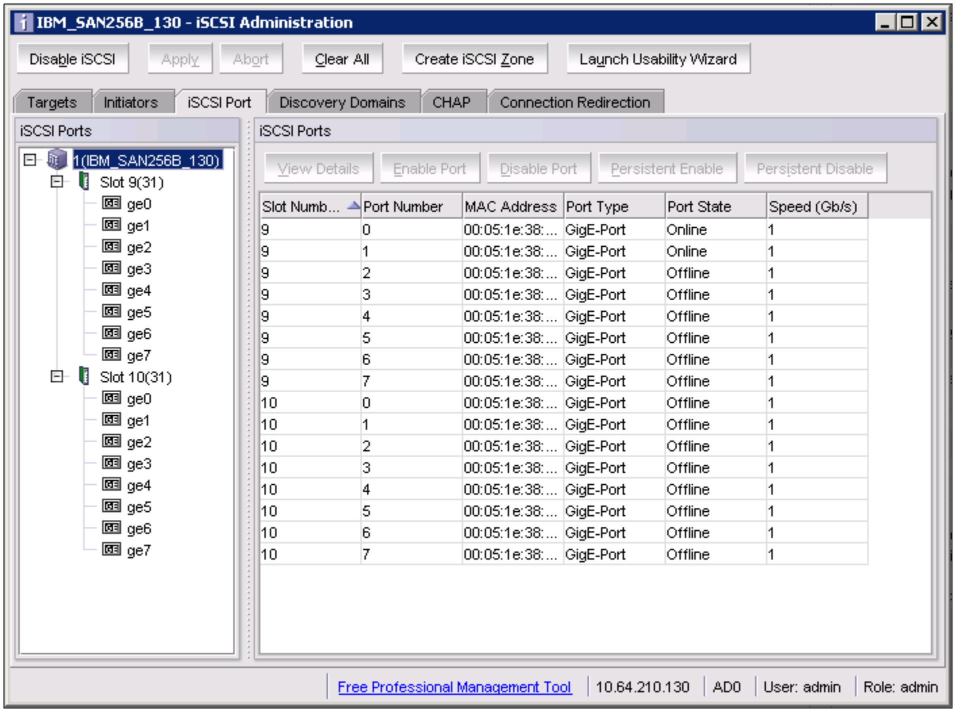
Figure 11-73 Authenticated, targets connected

11.3.2 Configuring more iSCSI portals

To configure iSCSI portals on GbE ports without using the Launch Usability Wizard, the iSCSI administration page can be used.

The **iSCSI port** tab (Figure 11-74) lists the inserted iSCSI blades by slot number and the GbE ports residing on them. Perform the followingsteps to configure more iSCSI portals:

1. Using the same initial setup details, connect the ge2 and ge3 ports on slot 9 to the dedicated iSCSI IP/Ethernet network.



Slot Numb...	Port Number	MAC Address	Port Type	Port State	Speed (Gb/s)
9	0	00:05:1e:38:...	GigE-Port	Online	1
9	1	00:05:1e:38:...	GigE-Port	Online	1
9	2	00:05:1e:38:...	GigE-Port	Offline	1
9	3	00:05:1e:38:...	GigE-Port	Offline	1
9	4	00:05:1e:38:...	GigE-Port	Offline	1
9	5	00:05:1e:38:...	GigE-Port	Offline	1
9	6	00:05:1e:38:...	GigE-Port	Offline	1
9	7	00:05:1e:38:...	GigE-Port	Offline	1
10	0	00:05:1e:38:...	GigE-Port	Offline	1
10	1	00:05:1e:38:...	GigE-Port	Offline	1
10	2	00:05:1e:38:...	GigE-Port	Offline	1
10	3	00:05:1e:38:...	GigE-Port	Offline	1
10	4	00:05:1e:38:...	GigE-Port	Offline	1
10	5	00:05:1e:38:...	GigE-Port	Offline	1
10	6	00:05:1e:38:...	GigE-Port	Offline	1
10	7	00:05:1e:38:...	GigE-Port	Offline	1

Figure 11-74 iSCSI port tab

2. Configure an IP interface on the ge2 port. Select port ge2 in the iSCSI Ports list, select the IP Interface tab, and click **Add**. See Figure 11-75.

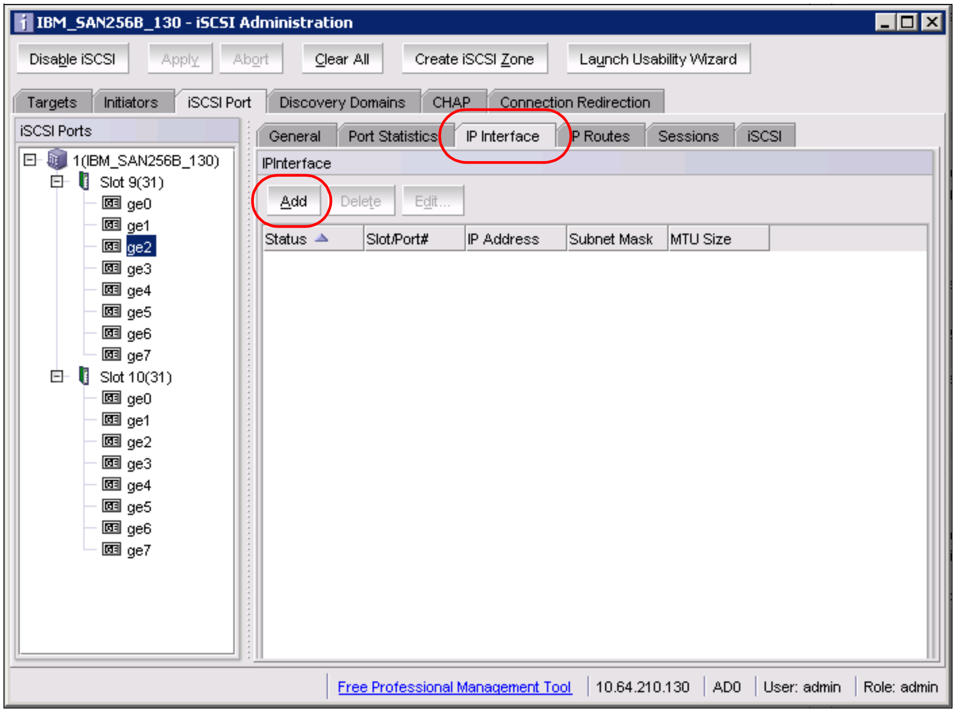
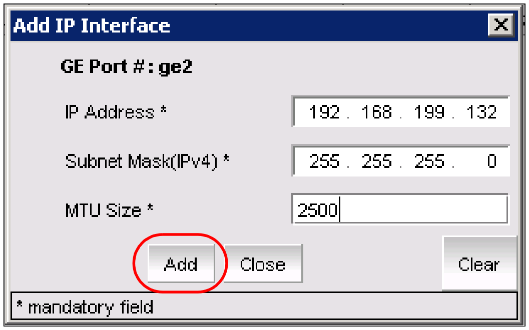


Figure 11-75 Add IP interface

3. Specify the IP address, subnet mask, and the Ethernet maximum transmission unit (MTU) size in the “Add IP Interface” dialog box (Figure 11-76). To add the new IP interface we click **Add**.


Add IP Interface

GE Port # : ge2

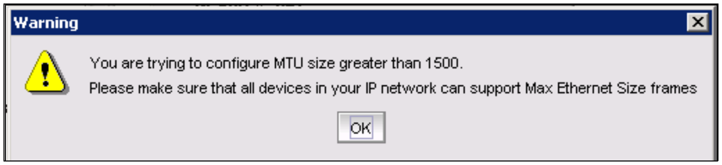
IP Address * 192 . 168 . 199 . 132

Subnet Mask(IPv4) * 255 . 255 . 255 . 0

MTU Size * 2500

Figure 11-76 Add IP details dialog box

The valid MTU value range is 1500 - 8256 bytes. A message box warns us if we specify an MTU value of more than 1500 bytes. See Figure 11-77. It is important that the IP/Ethernet network used for connecting the iSCSI host with the iSCSI blade can support this (Ethernet jumbo frames). We acknowledge this message, by clicking **OK**, and the IP interface is then created.



You are trying to configure MTU size greater than 1500.

Please make sure that all devices in your IP network can support Max Ethernet Size frames

Figure 11-77 Large MTU Warning

Note: Ethernet jumbo frames can increase data transmission performance by lowering the protocol overheads imposed by using iSCSI. When using this feature always ensure that the complete data path supports it, because connectivity problems and low performance might otherwise occur.

11.3.3 Updating the iSCSI FC zone

In zoned FC environments, zoning must be modified when new iSCSI VTs are created or existing ones modified. This approach allows the iSCSI VIs to access the FC targets.

The default behavior is that all iSCSI VIs have access to all iSCSI FC targets through the iSCSI_FC_ZONE, and under normal circumstances this is a good practice.

To keep the FC zoning updated, use the **Create iSCSI Zone** button at the top of the iSCSI administration GUI. By using this button after iSCSI VT configuration is modified, the iSCSI_FC_ZONE zone is updated and added to the zoning configuration.

11.3.4 LUN masking

A LUN masking function is normally used to facilitate access control on a disk storage subsystem.

To access storage on a disk storage subsystem with LUN masking enforcement, the WWN information of the SAN256B director and the iSCSI portals must be added to the Disk LUN masking method. The port WWN of the SAN256B director with the iSCSI blades inserted is used to query for LUNs on the FC SAN targets, and the port WWNs of the iSCSI VIs are used for accessing the LUNs.

To obtain WWN information from the SAN256B director, the **fclunquery -s** command is used. The port WWNs of the iSCSI VIs can be obtained by consulting the SAN256B name server.

In Example 11-2, the port WWNs of the SAN256B and the ge1 and ge2 iSCSI VIs are highlighted.

Example 11-2 Obtaining WWN information for SAN256B director and iSCSI VIs

```
IBM_SAN256B_130:admin> fclunquery -s
The following WWNs will be used for any lun query from this switch:
Node WWN: 10:00:00:60:69:80:45:0c
Port WWN: 21:fd:00:60:69:80:45:0c

IBM_SAN256B_130:admin> nsshow
{
 Type Pid    COS     PortName                NodeName                 TTL(sec)
N    016600;      3;20:07:00:a0:b8:48:58:a2;20:06:00:a0:b8:48:58:a0; na
    FC4s: FCP [IBM     1814      FAStT 0916]
    Fabric Port Name: 20:66:00:60:69:80:45:0c
    Permanent Port Name: 20:07:00:a0:b8:48:58:a2
    Port Index: 102
    Share Area: No
    Device Shared in Other AD: No
    Redirect: No
 N    016700;      3;20:06:00:a0:b8:48:58:a2;20:06:00:a0:b8:48:58:a0; na
    FC4s: FCP [IBM     1814      FAStT 0916]
    Fabric Port Name: 20:67:00:60:69:80:45:0c
    Permanent Port Name: 20:06:00:a0:b8:48:58:a2
    Port Index: 103
    Share Area: No
    Device Shared in Other AD: No
    Redirect: No
 N    016800;      3;50:06:06:98:04:50:c7:00;50:06:06:98:04:50:c7:01; na
    FC4s: FCP
    PortSymb: [23] "iSCSI Virtual Initiator"
    NodeSymb: [56] "IPAddr: 192.168.199.130 Slot/Port: 9/ge0 Logical pn: 104"
    Fabric Port Name: 20:68:00:60:69:80:45:0c
    Permanent Port Name: 50:06:06:98:04:50:c7:00--------> Used for LUN Masking
    Port Index: 104
    Share Area: No
    Device Shared in Other AD: No
    Redirect: No
 N    016900;      3;50:06:06:98:04:50:c7:08;50:06:06:98:04:50:c7:09; na
    FC4s: FCP
    PortSymb: [23] "iSCSI Virtual Initiator"
    NodeSymb: [56] "IPAddr: 192.168.199.131 Slot/Port: 9/ge1 Logical pn: 105"
    Fabric Port Name: 20:69:00:60:69:80:45:0c
    Permanent Port Name: 50:06:06:98:04:50:c7:08--------> Used for LUN Masking
    Port Index: 105
    Share Area: No
    Device Shared in Other AD: No
    Redirect: No
................
..................................................> Output truncated
................
The Local Name Server has 19 entries }
```

11.3.5 Hierarchical LUN addressing

For systems using hierarchical LUN IDs (multiple levels), the Web Tool's iSCSI Administration GUI might not correctly display the LUN ID because it uses a single byte for this information. If this is the case, use the CLI.

For information about the commands, refer to the *Fabric OS Command Reference Manual Supporting Fabric OS 6.2.0*, which can be obtained from the Brocade Technical Resource Center. You may also use the **`help|grep iscsi`** command to get an idea of the commands to use.

Related publications

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

IBM Redbooks publications

For information about ordering these publications, see “Help from IBM” on page 316. Note that several documents referenced here might be available in softcopy only.

- *Introduction to Storage Area Networks*, SG24-5470
- *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384
- *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches*, SG24-6116
- *Using iSCSI Solutions’ Planning and Implementation*, SG24-6291

Other resources

These publications are also relevant as further information sources:

- Clark, Tom*. IP SANs: An Introduction to iSCSI, iFCP, and FCIP Protocols for Storage Area Network*. Addison-Wesley Professional, first edition, December 2001. ISBN 0201752778.
- Judd, Josh. *Multiprotocol Routing for SAN*s. Infinity Publishing, October 2004. ISBN 0741423065.

Referenced web sites

These web sites are also relevant as further information sources:

- IBM TotalStorage hardware, software, and solutions:

  `http://www.storage.ibm.com`

- IBM TotalStorage storage area network:

  `http://www.storage.ibm.com/snetwork/index.html`

- Brocade:

  `http://www.brocade.com`

- QLogic:

  `http://www.qlogic.com`
- Emulex:

  `http://www.emulex.com`
- Finisar:

  `http://www.finisar.com`
- Veritas:

  `http://www.veritas.com`
- Tivoli:

  `http://www.tivoli.com`
- JNI:

  `http://www.Jni.com`
- IEEE:

  `http://www.ieee.org`
- Storage Networking Industry Association:

  `http://www.snia.org`
- SCSI Trade Association:

  `http://www.scsita.org`
- Internet Engineering Task Force:

  `http://www.ietf.org`
- American National Standards Institute:

  `http://www.ansi.org`
- Technical Committee T10:

  `http://www.t10.org`
- Technical Committee T11:

  `http://www.t11.org`

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

IBM System Storage b-type Multiprotocol Routing: An Introduction and Implementation

IBM System Storage b-type Multiprotocol Routing
An Introduction and Implementation

Read about the basics of the IBM/Brocade approach

Learn about the IBM/Brocade products and solutions

Understand how to install routers

The rapid spread and adoption of production storage area networks (SANs) has fueled the need for multiprotocol routers. The routers provide improved scalability, security, and manageability by enabling devices in separate SAN fabrics to communicate without merging fabrics into a single, large SAN fabric. This capability enables clients to deploy separate SAN solutions at the departmental and data center levels. Then, clients can consolidate these separate solutions into large enterprise SAN solutions as their experience and requirements grow and change.

Alternatively, multiprotocol routers can help to connect existing enterprise SANs for a variety of reasons. For instance, the introduction of Small Computer System Interface over IP (iSCSI) provides for the connection of low-end, low-cost hosts to enterprise SANs. The use of an Internet Protocol (IP) in the Fibre Channel (FC) environment provides for resource consolidation and disaster recovery planning over long distances. And the use of FC-FC routing services provides connectivity between two or more fabrics without having to merge them into a single SAN.

This IBM Redbooks publication targets storage network administrators, system designers, architects, and IT professionals who sell, design, or administer SANs. It introduces you to products, concepts, and technology in the IBM System Storage SAN Routing portfolio, which is based on Brocade products and technology. This book discusses the features of these products and provides examples of how you can deploy and use them.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7544-03 0738435325