



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*



## **Cisco Fabric Manager Interfaces Configuration Guide**

Cisco Fabric Manager Release 5.0(1a) Through 5.0(3)  
July 2010

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

*Cisco Fabric Manager Interfaces Configuration Guide*  
© 2010 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **New and Changed Information**   xi

### **Preface**   xiii

Audience   xiii

Organization   xiii

Document Conventions   xiv

Related Documentation   xv

    Release Notes   xv

    Regulatory Compliance and Safety Information   xv

    Compatibility Information   xv

    Hardware Installation   xv

    Software Installation and Upgrade   xv

    Cisco NX-OS   xvi

    Cisco Fabric Manager   xvi

    Command-Line Interface   xvi

    Intelligent Storage Networking Services Configuration Guides   xvi

    Troubleshooting and Reference   xvii

Obtaining Documentation and Submitting a Service Request   xvii

xvii

---

## CHAPTER 1

### **Interfaces Overview**   1-1

Virtual Interfaces   1-1

Trunks and PortChannels   1-1

Fibre Channel Port Rate Limiting   1-2

Extended Credits   1-2

N Port Virtualization   1-2

FlexAttach   1-2

---

## CHAPTER 2

### **Configuring Interfaces**   2-1

Common Interface Configuration   2-2

Fibre Channel Interfaces   2-2

    Generation 1 Interfaces Configuration Guidelines   2-3

    About Interface Modes   2-3

        E Port   2-4

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

F Port	2-5
FL Port	2-5
NP Ports	2-5
TL Port	2-5
TE Port	2-6
TF Port	2-6
TNP Port	2-6
SD Port	2-6
ST Port	2-7
Fx Port	2-7
B Port	2-7
Auto Mode	2-7
About Interface States	2-8
Administrative States	2-8
Operational States	2-8
Reason Codes	2-8
Configuring Fibre Channel Interfaces	2-10
Graceful Shutdown	2-11
Setting the Interface Administrative State	2-11
Configuring Interface Modes	2-12
Configuring Port Administrative Speeds	2-12
Autosensing	2-13
Configuring the Interface Description	2-13
Specifying a Port Owner	2-13
Displaying the Owned Ports	2-15
Frame Encapsulation	2-16
Identifying the Beacon LEDs	2-16
About Speed LEDs	2-17
Configuring Beacon Mode	2-17
About Bit Error Thresholds	2-17
Switch Port Attribute Default Values	2-18
About SFP Transmitter Types	2-18
Displaying SFP Transmitter Types	2-19
Gathering Interface Statistics	2-19
TL Ports for Private Loops	2-20
About TL Ports	2-20
Configuring TL Ports	2-22
About TL Port ALPA Caches	2-22
Configuring Port Guard	2-22



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Configuring Port Monitor	2-26
Port Group Charting	2-26
Management Interfaces	2-27
About Management Interfaces	2-27
Configuring Management Interfaces	2-27
VSAN Interfaces	2-28
About VSAN Interfaces	2-28
Creating VSAN Interfaces	2-28
Default Settings	2-29

## CHAPTER 3

### Configuring Ethernet Interfaces 3-1

About Ethernet Interfaces	3-1
Displaying Interface Information	3-1
Displaying Interface Information Using Fabric Manager	3-1
Displaying Interface Information Using Device Manager	3-2
Default Settings	3-3

## CHAPTER 4

### Configuring Virtual Fibre Channel Interfaces 4-1

About Virtual Fibre Channel Interfaces	4-1
Guidelines and Limitations	4-1
Configuring Virtual Fibre Channel Interfaces	4-2
Overview	4-2
Configuring a Virtual Fibre Channel Interface	4-2
Configuring a Virtual Fibre Channel Interface Using Fabric Manager	4-2
Configuring a Virtual Fibre Channel Interface Using Device Manager	4-4
Mapping VLANs to VSANs	4-5
Mapping VLANs to VSANs Using Fabric Manager	4-5
Mapping VLANs to VSANs Using Device Manager	4-7
Assigning Fibre Channel VSAN Membership	4-8
Creating a Virtual Fibre Channel Interface	4-8
Using the FCoE Configuration Wizard	4-9
Creating a Virtual Fibre Channel Interface Using Fabric Manager	4-13
Creating a Virtual Fibre Channel Interface Using Device Manager	4-14
Deleting a Virtual Fibre Channel Interface	4-15
Default Settings	4-16

## CHAPTER 5

### Configuring Fibre Channel Interfaces 5-1

About Generations of Modules and Switches	5-1
---	-----

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Port Groups and Port Rate Modes	5-3
Port Groups	5-3
Port Rate Modes	5-4
Dedicated Rate Mode	5-6
Shared Rate Mode	5-7
Dedicated Rate Mode Configurations for the 8-Gbps Modules	5-7
Reserving Bandwidth Quickly for the 8-Gbps Modules	5-8
Dynamic Bandwidth Management	5-9
Out-of-Service Interfaces	5-10
Combining Generation 1, Generation 2, and Generation 3 Modules	5-10
Port Indexes	5-11
PortChannels	5-12
Configuring Module Interface Shared Resources	5-14
Configuration Guidelines for 48-Port, 24-Port, and 4/44-Port 8-Gbps Fibre Channel Switching Modules	5-15
Migrating from Shared Mode to Dedicated Mode	5-15
Migrating from Dedicated Mode to Shared Mode	5-16
Configuration Guidelines for 48-Port and 24-Port 4-Gbps Fibre Channel Switching Modules	5-16
Migrating from Shared Mode to Dedicated Mode	5-16
Migrating from Dedicated Mode to Shared Mode	5-17
Configuration Guidelines for 12-Port 4-Gbps Switching Module Interfaces	5-17
Configuration Guidelines for 4-Port 10-Gbps Switching Module Interfaces	5-18
Configuring Port Speed	5-18
Configuring Rate Mode	5-19
Configuring Oversubscription Ratio Restrictions	5-20
Disabling Restrictions on Oversubscription Ratios	5-22
Enabling Restrictions on Oversubscription Ratios	5-23
Configuring Bandwidth Fairness	5-24
Enabling Bandwidth Fairness	5-24
Disabling Bandwidth Fairness	5-26
Upgrade or Downgrade Scenario	5-26
Taking Interfaces Out of Service	5-26
Releasing Shared Resources in a Port Group	5-27
Displaying SFP Diagnostic Information	5-28
Default Settings	5-30

## CHAPTER 6

### Configuring Interface Buffers 6-1

About Buffer-to-Buffer Credits	6-1
--------------------------------	-----

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Configuring Buffer-to-Buffer Credits	6-2
About Performance Buffers	6-2
Configuring Performance Buffers	6-2
Buffer Pools	6-3
BB_Credit Buffers for Switching Modules	6-5
48-Port 8-Gbps Fibre Channel Module BB_Credit Buffers	6-6
24-Port 8-Gbps Fibre Channel Module BB_Credit Buffers	6-7
4/44-Port 8-Gbps Host-Optimized Fibre Channel Module BB_Credit Buffers	6-8
48-Port 4-Gbps Fibre Channel Module BB_Credit Buffers	6-9
24-Port 4-Gbps Fibre Channel Module BB_Credit Buffers	6-10
18-Port Fibre Channel/4-Port Gigabit Ethernet Multiservice Module BB_Credit Buffers	6-11
12-Port 4-Gbps Switching Module BB_Credit Buffers	6-12
4-Port 10-Gbps Switching Module BB_Credit Buffers	6-13
BB_Credit Buffers for Fabric Switches	6-14
Cisco MDS 9148 Fabric Switch BB_Credit Buffers	6-14
Cisco MDS 9134 Fabric Switch BB_Credit Buffers	6-14
Cisco MDS 9124 Fabric Switch BB_Credit Buffers	6-15
Cisco MDS 9222i Multiservice Modular Switch BB_Credit Buffers	6-15
About Extended BB_Credits	6-16
Extended BB_credits on Generation 1 Switching Modules	6-16
Extended BB_credits on Generation 2 and Generation 3 Switching Modules	6-17
Configuring Extended BB_credits	6-18
Enabling Buffer-to-Buffer Credit Recovery	6-19
About Receive Data Field Size	6-19
Configuring Receive Data Field Size	6-19

## CHAPTER 7

<b>Configuring Trunking</b>	<b>7-1</b>
About Trunking	7-1
Trunking E Ports	7-2
Trunking F Ports	7-2
Key Concepts	7-3
Trunking Guidelines and Restrictions	7-3
Trunking Misconfiguration Examples	7-4
Upgrade and Downgrade Restrictions	7-5
Difference Between TE Ports and TF-TNP Ports	7-5
Enabling the Trunking Protocols	7-6
About Trunking Protocols	7-6
Enabling the F Port Trunking and Channeling Protocol	7-7
Configuring Trunk Mode and VSAN List	7-7

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

About Trunk Modes	7-7
Configuring Trunk Mode	7-8
About Trunk-Allowed VSAN Lists and VF_IDs	7-9
Configuring an Allowed-Active List of VSANs	7-11
Default Settings	7-11

## CHAPTER 8

<b>Configuring PortChannels</b>	<b>8-1</b>
About PortChannels	8-1
About E PortChannels	8-2
About F and TF PortChannels	8-3
About PortChanneling and Trunking	8-3
About Load Balancing	8-4
About PortChannel Modes	8-6
Configuration Guidelines and Restrictions	8-7
Generation 1 PortChannel Restrictions	8-7
F and TF PortChannel Restrictions	8-8
PortChannel Configuration	8-9
About PortChannel Configuration	8-10
Configuring PortChannels Using the Wizard	8-11
Configuring the PortChannel Mode	8-16
About PortChannel Deletion	8-16
Deleting PortChannels	8-16
Interfaces in a PortChannel	8-17
About Interface Addition to a PortChannel	8-17
Compatibility Check	8-18
Suspended and Isolated States	8-18
Adding an Interface to a PortChannel	8-18
Forcing an Interface Addition	8-19
About Interface Deletion from a PortChannel	8-20
Deleting an Interface from a PortChannel	8-20
PortChannel Protocols	8-20
About Channel Group Creation	8-21
About Autocreation	8-22
Enabling and Configuring Autocreation	8-23
About Manually Configured Channel Groups	8-23
Converting to Manually Configured Channel Groups	8-23
Verifying the PortChannel Configuration	8-24
Default Settings	8-25

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## CHAPTER 9

### Configuring N Port Virtualization 9-1

- About N Port Identifier Virtualization 9-1
  - Enabling N Port Identifier Virtualization 9-2
- About N Port Virtualization 9-2
  - NPV Mode 9-4
  - NP Ports 9-4
  - NP Links 9-4
    - Internal FLOGI Parameters 9-4
  - Default Port Numbers 9-6
  - NPV CFS Distribution over IP 9-6
  - NPV Traffic Management 9-6
    - Auto 9-6
    - Traffic Map 9-6
    - Disruptive 9-7
  - Multiple VSAN Support 9-7
- NPV Guidelines and Requirements 9-7
  - NPV Traffic Management Guidelines 9-8
- Configuring NPV 9-8
  - Configuring NPV Traffic Management 9-10
    - Configuring List of External Interfaces per Server Interface 9-10
    - Enabling the Global Policy for Disruptive Load Balancing 9-12
    - Displaying the External Interface Usage for Server Interfaces 9-13
  - Using the NPV Setup Wizard 9-14
  - DPVM Configuration 9-33
  - NPV and Port Security 9-33

## CHAPTER 10

### Configuring FlexAttach Virtual pWWN 10-1

- About FlexAttach Virtual pWWN 10-1
- FlexAttach Virtual pWWN Guidelines and Requirements 10-2
- Configuring FlexAttach Virtual pWWN 10-2
  - Enabling FlexAttach Virtual pWWN 10-2
    - Automatically Enabling FlexAttach Virtual pWWN 10-2
  - Launching FlexAttach in Fabric Manager 10-3
    - Manually Enabling FlexAttach Virtual pWWN 10-4
    - Mapping pWWN to Virtual pWWN 10-6
  - Debugging FlexAttach Virtual pWWN 10-8
  - Security Settings for FlexAttach Virtual pWWN 10-8
  - FlexAttach Virtual pWWN CFS Distribution 10-9

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Using the Server Admin FlexAttach Wizards	10-9
Pre-Configuring FlexAttach for a New Server	10-9
Pre-Configuring FlexAttach for All the Ports	10-10
Pre-Configuring FlexAttach for Each Port Individually	10-12
Moving a Server to Another Port or Switch	10-15
Replacing a Server with Another Server	10-19
Replacing a Server on the Same Port	10-19
Replacing the Server to a Different Port on the Same Switch	10-22
Replacing with a Server on a Different Switch	10-24
Difference Between San Device Virtualization and FlexAttach Port Virtualization	10-25



## New and Changed Information

---

As of Cisco MDS NX-OS Release 4.2(1), software configuration information is available in new feature-specific configuration guides for the following information:

- System management
- Interfaces
- Fabric
- Quality of service
- Security
- IP services
- High availability and redundancy

The information in these new guides previously existed in the *Cisco MDS 9000 Family CLI Configuration Guide* and in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*. Those configuration guides remain available on Cisco.com and should be used for all software releases prior to MDS NX-OS Release 4.2(1). Each guide addresses the features introduced in or available in a particular release. Select and view the configuration guide that pertains to the software installed in your switch.

For a complete list of document titles, see the list of Related Documentation in the “Preface.”

To find additional information about Cisco MDS NX-OS Release 4.2(x), see the *Cisco MDS 9000 Family Release Notes* available at the following Cisco Systems website:

[http://www.cisco.com/en/US/products/ps5989/prod\\_release\\_notes\\_list.htm](http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm)

### About This Guide

The information in the new *Cisco Fabric Manager Interfaces Configuration Guide* previously existed in Part 3: Switch Configuration of the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

[Table 1](#) lists the New and Changed features for this guide, starting with MDS NX-OS Release 5.0(1a).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 1**      **New and Changed Features for Cisco MDS Fabric Manager Release 5.0(1a)**

<b>Feature</b>	<b>GUI Change</b>	<b>Description</b>	<b>Changed in Release</b>	<b>Where Documented</b>
FlexAttach	Disable FlexAttach	Added information about disabling FlexAttach.	5.0(1a)	<a href="#">Chapter 10, “Configuring FlexAttach Virtual pWWN”</a>
Port Group Monitoring Enhancements	Check Oversubscription > Monitor	Added information about monitoring a selected port group.	5.0(1a)	<a href="#">Chapter 2, “Configuring Interfaces”</a>





## Preface

---

This preface describes the audience, organization, and conventions of the *Cisco Fabric Manager Interfaces Configuration Guide*. It also provides information on how to obtain related documentation.

## Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches.

## Organization

The *Cisco Fabric Manager Interfaces Configuration Guide* is organized as follows:

Chapter	Title	Description
<a href="#">Chapter 1</a>	<a href="#">Interfaces Overview</a>	Provides an overview of all the features in this guide.
<a href="#">Chapter 2</a>	<a href="#">Configuring Interfaces</a>	Explains Generation 1 and Generation 2 module port and operational state concepts in Cisco MDS 9000 Family switches and provides details on configuring ports and interfaces.
<a href="#">Chapter 3</a>	<a href="#">Configuring Ethernet Interfaces</a>	Explains configuring Ethernet Interfaces on Nexus 5000 Series switches.
<a href="#">Chapter 4</a>	<a href="#">Configuring Virtual Fibre Channel Interfaces</a>	Explains configuring Virtual Interfaces on Nexus 5000 Series switches.
<a href="#">Chapter 5</a>	<a href="#">Configuring Fibre Channel Interfaces</a>	Explains configuration concepts for Fibre Channel module ports and interfaces.
<a href="#">Chapter 6</a>	<a href="#">Configuring Interface Buffers</a>	Explains configuration concepts for Interface Buffers.
<a href="#">Chapter 7</a>	<a href="#">Configuring Trunking</a>	Explains TE ports and trunking concepts.
<a href="#">Chapter 8</a>	<a href="#">Configuring PortChannels</a>	Explains PortChannels and load balancing concepts and provides details on configuring PortChannels, adding ports to PortChannels, and deleting ports from PortChannels.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

Chapter	Title	Description
Chapter 9	Configuring N Port Virtualization	Provides an overview of N Port Virtualization and includes guidelines and requirements for configuring and verifying NPV.
Chapter 10	Configuring FlexAttach Virtual pWWN	FlexAttach virtual pWWN feature facilitates server and configuration management. In a SAN environment, the server installation or replacement, requires interaction and coordination among the SAN and server administrators.

## Document Conventions

Command descriptions use these conventions:

<b>boldface font</b>	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

screen font	Terminal sessions and information the switch displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:



### Note

Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.



### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

[http://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/roadmaps/doclocator.htm](http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm)

## Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*
- *Release Notes for Cisco MDS 9000 Family Fabric Manager*

## Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

## Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

## Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

## Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

## Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

## Cisco Fabric Manager

- *Cisco Fabric Manager Fundamentals Configuration Guide*
- *Cisco Fabric Manager System Management Configuration Guide*
- *Cisco Fabric Manager Interfaces Configuration Guide*
- *Cisco Fabric Manager Fabric Configuration Guide*
- *Cisco Fabric Manager Quality of Service Configuration Guide*
- *Cisco Fabric Manager Security Configuration Guide*
- *Cisco Fabric Manager IP Services Configuration Guide*
- *Cisco Fabric Manager Intelligent Storage Services Configuration Guide*
- *Cisco Fabric Manager High Availability and Redundancy Configuration Guide*
- *Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*
- *Cisco Fabric Manager Online Help*
- *Cisco Fabric Manager Web Services Online Help*

## Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

## Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 Family I/O Accelerator Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

## Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*
- *Cisco MDS 9000 Family Fabric Manager Server Database Schema*

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***



# CHAPTER 1

## Interfaces Overview

---

This chapter describes the basic interfaces that are used with Fabric Manager. These interfaces include Gigabit Ethernet interfaces, Fiber Channel interfaces, virtual interfaces on Nexus hardware, buffer credits, management interfaces, VSAN interfaces, shared interface resources, trunking, PortChanneling, N port virtualization (NPV), and FlexAttach virtual pWWN.

This chapter includes the following topics:

- [Virtual Interfaces, page 1-1](#)
- [Trunks and PortChannels, page 1-1](#)
- [Fibre Channel Port Rate Limiting, page 1-2](#)
- [Extended Credits, page 1-2](#)
- [N Port Virtualization, page 1-2](#)
- [FlexAttach, page 1-2](#)

## Virtual Interfaces

Cisco Nexus 5000 Series switches support Fibre Channel over Ethernet (FCoE), which allows Fibre Channel and Ethernet traffic to be carried on the same physical Ethernet connection between the switch and the servers.

The Fibre Channel portion of FCoE is configured as a virtual Fibre Channel interface. Logical Fibre Channel features (such as interface mode) can be configured on virtual Fibre Channel interfaces.

## Trunks and PortChannels

Trunking, also known as VSAN trunking, is a feature specific to switches in the Cisco MDS 9000 Family. Trunking enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link. Trunking is supported on E ports and F ports.

PortChannels aggregate multiple physical ISLs into one logical link with higher bandwidth and port resiliency for both Fibre Channel and FICON traffic. With this feature, up to 16 expansion ports (E-ports) or trunking E-ports (TE-ports) can be bundled into a PortChannel. ISL ports can reside on any switching module, and they do not need a designated master port. If a port or a switching module fails, the PortChannel continues to function properly without requiring fabric reconfiguration.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Cisco NX-OS software uses a protocol to exchange PortChannel configuration information between adjacent switches to simplify PortChannel management, including misconfiguration detection and autocreation of PortChannels among compatible ISLs. In the autoconfigure mode, ISLs with compatible parameters automatically form channel groups; no manual intervention is required.

PortChannels load balance Fibre Channel traffic using a hash of source FC-ID and destination FC-ID, and optionally the exchange ID. Load balancing using PortChannels is performed over both Fibre Channel and FCIP links. Cisco NX-OS software also can be configured to load balance across multiple same-cost FSPF routes.

## Fibre Channel Port Rate Limiting

The Fibre Channel port rate-limiting feature for the Cisco MDS 9100 Series controls the amount of bandwidth available to individual Fibre Channel ports within groups of four host-optimized ports. Limiting bandwidth on one or more Fibre Channel ports allows the other ports in the group to receive a greater share of the available bandwidth under high-utilization conditions. Port rate limiting is also beneficial for throttling WAN traffic at the source to help eliminate excessive buffering in Fibre Channel and IP data network devices.

## Extended Credits

Full line-rate Fibre Channel ports provide at least 255 buffer credits standard. Adding credits lengthens distances for Fibre Channel SAN extension. Using extended credits, up to 4095 buffer credits from a pool of more than 6000 buffer credits for a module can be allocated to ports as needed to greatly extend the distance for Fibre Channel SANs.

## N Port Virtualization

Cisco NX-OS software supports industry-standard N port identifier virtualization (NPIV), which allows multiple N port fabric logins concurrently on a single physical Fibre Channel link. HBAs that support NPIV can help improve SAN security by enabling zoning and port security to be configured independently for each virtual machine (OS partition) on a host. In addition to being useful for server connections, NPIV is beneficial for connectivity between core and edge SAN switches.

N port virtualizer (NPV) is a complementary feature that reduces the number of Fibre Channel domain IDs in core-edge SANs. Cisco MDS 9000 family fabric switches operating in the NPV mode do not join a fabric; they only pass traffic between core switch links and end devices, which eliminates the domain IDs for these switches. NPIV is used by edge switches in the NPV mode to log in to multiple end devices that share a link to the core switch. This feature is available only for Cisco MDS Blade Switch Series, the Cisco MDS 9124 Multilayer Fabric Switch, and the Cisco MDS 9134 Multilayer Fabric Switch.

## FlexAttach

Cisco NX-OS supports the FlexAttach feature. One of the main problems in a SAN environment is the time and effort required to install and replace servers. The process involves both SAN and server administrators, and the interaction and coordination between them can make the process time consuming. To alleviate the need for interaction between SAN and server administrators, the SAN



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

configuration should not be changed when a new server is installed or an existing server is replaced. FlexAttach addresses these problems, reducing configuration changes and the time and coordination required by SAN and server administrators when installing and replacing servers. This feature is available only for Cisco MDS 9000 Blade Switch Series, the Cisco MDS 9124, and the Cisco MDS 9134 when NPV mode is enabled.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***



## CHAPTER 2

# Configuring Interfaces

---

The main function of a switch is to relay frames from one data link to another. To relay the frames, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Fibre Channel interfaces, Gigabit Ethernet interfaces, the management interface (mgmt0), or VSAN interfaces.

This chapter describes the basic interface configuration to get your switch up and running. It includes the following sections:

- [Common Interface Configuration, page 2-2](#)
- [Fibre Channel Interfaces, page 2-2](#)
- [TL Ports for Private Loops, page 2-20](#)
- [Configuring Port Guard, page 2-22](#)
- [Management Interfaces, page 2-27](#)
- [VSAN Interfaces, page 2-28](#)
- [Default Settings, page 2-29](#)

For more information on configuring mgmt0 interfaces, refer to the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide* and *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*.

See the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide* for more information on configuring Gigabit Ethernet interfaces.



### Tip

Before you begin configuring the switch, ensure that the modules in the chassis are functioning as designed. See the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*.



### Tip

Before you begin configuring the switch, ensure that the modules in the chassis are functioning as designed. For information about verifying the module status, refer to the *Cisco NX-OS Fundamentals Configuration Guide*.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

## Common Interface Configuration

Some configuration settings are similar for Fibre Channel, management, and VSAN interfaces. You can configure interfaces from Fabric Manager by expanding **Switches > Interfaces** and selecting the interface type from the Physical Attributes pane.

Figure 2-1 shows a sample of what you might see in the Information pane for Fibre Channel interfaces.

**Figure 2-1** Fibre Channel Interface Configuration

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	Failure Cause	Was Enabled	Last Change
172.22.46.180	fc1/1	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/2	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/3	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/4	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/5	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/6	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/7	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/8	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/9	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/10	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/11	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/12	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/13	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc1/14	auto	auto	1	n/a		auto	n/a	dedicated	in	down	down	adminDown	false	n/a
172.22.46.180	fc3/1	FX	auto	1	n/a		auto	n/a	shared	in	down	down	adminDown	false	n/a
172.22.46.180	fc3/2	FX	auto	1	n/a		auto	n/a	shared	in	down	down	adminDown	false	n/a

## Fibre Channel Interfaces

This section describes Fibre Channel interface characteristics, including (but not limited to) modes, frame encapsulation, states, SFPs, and speeds.

This section includes the following topics:

- [Generation 1 Interfaces Configuration Guidelines, page 2-3](#)
- [About Interface Modes, page 2-3](#)
- [About Interface States, page 2-8](#)
- [Configuring Fibre Channel Interfaces, page 2-10](#)
- [Graceful Shutdown, page 2-11](#)
- [Configuring Interface Modes, page 2-12](#)
- [Configuring Port Administrative Speeds, page 2-12](#)
- [Specifying a Port Owner, page 2-13](#)
- [Configuring Port Guard, page 2-22](#)
- [Frame Encapsulation, page 2-16](#)
- [Identifying the Beacon LEDs, page 2-16](#)
- [Configuring Beacon Mode, page 2-17](#)
- [About Bit Error Thresholds, page 2-17](#)
- [About SFP Transmitter Types, page 2-18](#)
- [Displaying SFP Transmitter Types, page 2-19](#)

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Generation 1 Interfaces Configuration Guidelines

The 32-port switching module guidelines apply to the following hardware:

- The 32-port, 2-Gbps or 1-Gbps switching module
- The Cisco MDS 9124 and 9134 switches

**Note**

Due to the hardware design of the MDS 9134 switch, we do not support interface out-of-service action on either of its two 10-Gigabit ports. This is because no internal port hardware resource is released when an out-of-service action is performed on these 10-Gigabit ports.

When configuring these host-optimized ports, the following port mode guidelines apply:

- You can configure only the first port in each 4-port group (for example, the first port in ports 1-4, the fifth port in ports 5-8, and so on) as an E port. If the first port in the group is configured as an E port, the other three ports in each group (ports 2-4, 6-8, and so on) are not usable and remain shutdown.
- If you execute the **write erase** command on a 32-port switching module, and then copy a saved configuration to the switch from a text file that contains the **no system default switchport shutdown** command, you need to copy the text file to the switch again for the E ports to come up without manual configuration.
- If any of the other three ports are enabled, you cannot configure the first port as an E port. The other three ports continue to remain enabled.
- The auto mode is not allowed in a 32-port switching module or the host-optimized ports in the Cisco 9100 Series (16 host-optimized ports in the Cisco MDS 9120 switch and 32 host-optimized ports in the Cisco MDS 9140 switch).
- The default port mode is Fx (Fx negotiates to F or FL) for 32-port switching modules.
- The 32-port switching module does not support FICON.

**Note**

We recommend that you configure your E ports on a 16-port switching module. If you must configure an E port on a 32-port host-optimized switching module, the other three ports in that 4-port group cannot be used.

**Note**

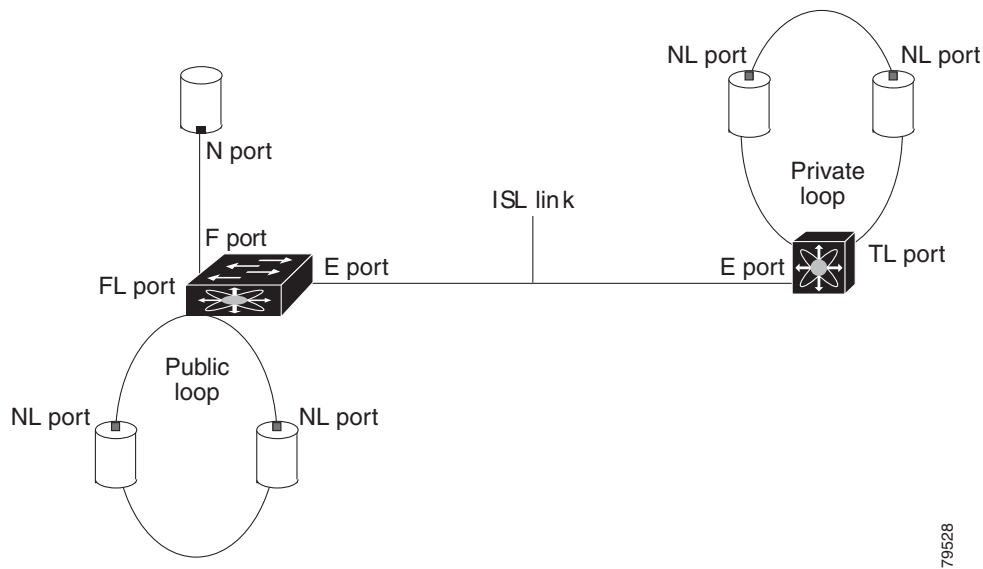
In the Cisco MDS 9100 Series, the groups of ports that are located on the left and outlined in white are full line rate. The other ports are host-optimized. Each group of 4 host-optimized ports have the same features as for the 32-port switching module.

## About Interface Modes

Each physical Fibre Channel interface in a switch may operate in one of several port modes: E port, F port, FL port, TL port, TE port, SD port, ST port, and B port (see [Figure 2-2](#)). Besides these modes, each interface may be configured in auto or Fx port modes. These two modes determine the port type during interface initialization.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 2-2 Cisco MDS 9000 Family Switch Port Modes**



**Note**

Interfaces are created in VSAN 1 by default. See the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.

Each interface has an associated administrative configuration and an operational status:

- The administrative configuration does not change unless you modify it. This configuration has various attributes that you can configure in administrative mode.
- The operational status represents the current status of a specified attribute like the interface speed. This status cannot be changed and is read-only. Some values may not be valid when the interface is down (for example, the operational speed).



**Note**

When a module is removed and replaced with the same type of module, the configuration is retained. If a different type of module is inserted, then the original configuration is no longer retained.

Each interface is briefly described in the sections that follow.

## E Port

In expansion port (E port) mode, an interface functions as a fabric expansion port. This port may be connected to another E port to create an Inter-Switch Link (ISL) between two switches. E ports carry frames between switches for configuration and fabric management. They serve as a conduit between switches for frames destined to remote N ports and NL ports. E ports support class 2, class 3, and class F service.

An E port connected to another switch may also be configured to form a PortChannel (see [Chapter 8, “Configuring PortChannels”](#)).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Note**

We recommend that you configure E ports on 16-port modules. If you must configure an E port on a 32-port oversubscribed module, then you can only use the first port in a group of four ports (for example, ports 1 through 4, 5 through 8, and so forth). The other three ports cannot be used.

## F Port

In fabric port (F port) mode, an interface functions as a fabric port. This port may be connected to a peripheral device (host or disk) operating as an N port. An F port can be attached to only one N port. F ports support class 2 and class 3 service.

## FL Port

In fabric loop port (FL port) mode, an interface functions as a fabric loop port. This port may be connected to one or more NL ports (including FL ports in other switches) to form a public arbitrated loop. If more than one FL port is detected on the arbitrated loop during initialization, only one FL port becomes operational and the other FL ports enter nonparticipating mode. FL ports support class 2 and class 3 service.

**Note**

FL port mode is not supported on 4-port 10-Gbps switching module interfaces.

## NP Ports

An NP port is a port on a device that is in NPV mode and connected to the core switch via an F port. NP ports function like N ports except that in addition to providing N port operations, they also function as proxies for multiple, physical N ports.

**Note**

A Cisco Nexus 5000 Series switch in NPV mode that runs Cisco NX-OS Release 4.2(1) or later releases supports trunking F port mode on NP ports. You can enable either, or both, VSAN trunking and an F port on an NP port.

For more details about NP ports and NPV, see [Chapter 9, “Configuring N Port Virtualization.”](#)

## TL Port

In translatable loop port (TL port) mode, an interface functions as a translatable loop port. It may be connected to one or more private loop devices (NL ports). TL ports are specific to Cisco MDS 9000 Family switches and have similar properties as FL ports. TL ports enable communication between a private loop device and one of the following devices:

- A device attached to any switch on the fabric
- A device on a public loop anywhere in the fabric
- A device on a different private loop anywhere in the fabric
- A device on the same private loop

TL ports support class 2 and class 3 services.

## ***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Private loop devices refer to legacy devices that reside on arbitrated loops. These devices are not aware of a switch fabric because they only communicate with devices on the same physical loop (see the [“About TL Port ALPA Caches” section on page 2-22](#)).



### **Tip**

We recommend configuring devices attached to TL ports in zones that have up to 64 zone members.



### **Note**

TL port mode is not supported on Generation 2 switching module interfaces.

## **TE Port**

In trunking E port (TE port) mode, an interface functions as a trunking expansion port. It may be connected to another TE port to create an extended ISL (EISL) between two switches. TE ports are specific to Cisco MDS 9000 Family switches. They expand the functionality of E ports to support the following:

- VSAN trunking
- Transport quality of service (QoS) parameters
- Fibre Channel trace (fctrace) feature

In TE port mode, all frames are transmitted in EISL frame format, which contains VSAN information. Interconnected switches use the VSAN ID to multiplex traffic from one or more VSANs across the same physical link. This feature is referred to as trunking in the Cisco MDS 9000 Family switches (see [Chapter 7, “Configuring Trunking”](#)). TE ports support class 2, class 3, and class F service.

## **TF Port**

In trunking F port (TF port) mode, an interface functions as a trunking expansion port. It may be connected to another trunked N port (TN port) or trunked NP port (TNP port) to create a link between a core switch and an NPV switch or an HBA to carry tagged frames. TF ports are specific to Cisco MDS 9000 Family switches. They expand the functionality of F ports to support VSAN trunking.

In TF port mode, all frames are transmitted in EISL frame format, which contains VSAN information. Interconnected switches use the VSAN ID to multiplex traffic from one or more VSANs across the same physical link. This feature is referred to as trunking in the Cisco MDS 9000 Family (see [Chapter 7, “Configuring Trunking”](#)). TF ports support class 2, class 3, and class F service.

## **TNP Port**

In trunking NP port (TNP port) mode, an interface functions as a trunking expansion port. It may be connected to a trunked F port (TF port) to create a link to a core NPIV switch from an NPV switch to carry tagged frames.

## **SD Port**

In SPAN destination port (SD port) mode, an interface functions as a switched port analyzer (SPAN). The SPAN feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic that passes through a Fibre Channel interface. This monitoring is done using a standard Fibre Channel analyzer (or a similar switch probe) that is attached to an SD port. SD ports do not receive frames, they



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

only transmit a copy of the source traffic. The SPAN feature is nonintrusive and does not affect switching of network traffic for any SPAN source ports (see the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*).

## ST Port

In the SPAN tunnel port (ST port) mode, an interface functions as an entry point port in the source switch for the RSPAN Fibre Channel tunnel. The ST port mode and the remote SPAN (RSPAN) feature are specific to switches in the Cisco MDS 9000 Family. When configured in ST port mode, the interface cannot be attached to any device, and thus cannot be used for normal Fibre Channel traffic (see the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*).



### Note

ST port mode is not supported on the Cisco MDS 9124 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

## Fx Port

Interfaces configured as Fx ports can operate in either F port or FL port mode. The Fx port mode is determined during interface initialization depending on the attached N port or NL port. This administrative configuration disallows interfaces to operate in any other mode—for example, preventing an interface to connect to another switch.

## B Port

While E ports typically interconnect Fibre Channel switches, some SAN extender devices, such as the Cisco PA-FC-1G Fibre Channel port adapter, implement a bridge port (B port) model to connect geographically dispersed fabrics. This model uses B ports as described in the T11 Standard FC-BB-2.

If an FCIP peer is a SAN extender device that only supports Fibre Channel B ports, you need to enable the B port mode for the FCIP link. When a B port is enabled, the E port functionality is also enabled and they coexist. If the B port is disabled, the E port functionality remains enabled (see the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*).

## Auto Mode

Interfaces configured in auto mode can operate in one of the following modes: F port, FL port, E port, TE port, or TF port. The port mode is determined during interface initialization. For example, if the interface is connected to a node (host or disk), it operates in F port or FL port mode depending on the N port or NL port mode. If the interface is attached to a third-party switch, it operates in E port mode. If the interface is attached to another switch in the Cisco MDS 9000 Family, it may become operational in TE port mode (see [Chapter 7, “Configuring Trunking”](#)).

TL ports and SD ports are not determined during initialization and are administratively configured.



### Note

Fibre Channel interfaces on Storage Services Modules (SSMs) cannot be configured in auto mode.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## About Interface States

The interface state depends on the administrative configuration of the interface and the dynamic state of the physical link.

### Administrative States

The administrative state refers to the administrative configuration of the interface as described in [Table 2-1](#).

**Table 2-1 Administrative States**

Administrative State	Description
Up	Interface is enabled.
Down	Interface is disabled. If you administratively disable an interface by shutting down that interface, the physical link layer state change is ignored.

### Operational States

The operational state indicates the current operational state of the interface as described in [Table 2-2](#).

**Table 2-2 Operational States**

Operational State	Description
Up	Interface is transmitting or receiving traffic as desired. To be in this state, an interface must be administratively up, the interface link layer state must be up, and the interface initialization must be completed.
Down	Interface cannot transmit or receive (data) traffic.
Trunking	Interface is operational in TE or TF mode.

### Reason Codes

Reason codes are dependent on the operational state of the interface as described in [Table 2-3](#).

**Table 2-3 Reason Codes for Interface States**

Administrative Configuration	Operational Status	Reason Code
Up	Up	None.
Down	Down	Administratively down—If you administratively configure an interface as down, you disable the interface. No traffic is received or transmitted.
Up	Down	See <a href="#">Table 2-4</a> .



#### Note

Only some of the reason codes are listed in [Table 2-4](#).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

If the administrative state is up and the operational state is down, the reason code differs based on the nonoperational reason code as described in [Table 2-4](#).

**Table 2-4 Reason Codes for Nonoperational States**

Reason Code (long version)	Description	Applicable Modes
Link failure or not connected	The physical layer link is not operational.	All
SFP not present	The small form-factor pluggable (SFP) hardware is not plugged in.	
Initializing	The physical layer link is operational and the protocol initialization is in progress.	
Reconfigure fabric in progress	The fabric is currently being reconfigured.	
Offline	The Cisco NX-OS software waits for the specified R_A_TOV time before retrying initialization.	
Inactive	The interface VSAN is deleted or is in a suspended state.  To make the interface operational, assign that port to a configured and active VSAN.	
Hardware failure	A hardware failure is detected.	
Error disabled	Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: <ul style="list-style-type: none"> <li>Configuration failure.</li> <li>Incompatible buffer-to-buffer credit configuration.</li> </ul> To make the interface operational, you must first fix the error conditions causing this state; and next, administratively shut down or enable the interface.	
FC redirect failure	A port is isolated because a Fibre Channel redirect is unable to program routes.	
No port activation license available	A port is not active because it does not have a port license.	
SDM failure	A port is isolated because SDM is unable to program routes.	

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 2-4 Reason Codes for Nonoperational States (continued)**

<b>Reason Code (long version)</b>	<b>Description</b>	<b>Applicable Modes</b>
Isolation due to ELP failure	The port negotiation failed.	Only E ports and TE ports
Isolation due to ESC failure	The port negotiation failed.	
Isolation due to domain overlap	The Fibre Channel domains (fcdomain) overlap.	
Isolation due to domain ID assignment failure	The assigned domain ID is not valid.	
Isolation due to the other side of the link E port isolated	The E port at the other end of the link is isolated.	
Isolation due to invalid fabric reconfiguration	The port is isolated due to fabric reconfiguration.	
Isolation due to domain manager disabled	The fcdomain feature is disabled.	
Isolation due to zone merge failure	The zone merge operation failed.	
Isolation due to VSAN mismatch	The VSANs at both ends of an ISL are different.	
Nonparticipating	FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode.	Only FL ports and TL ports
PortChannel administratively down	The interfaces belonging to the PortChannel are down.	Only PortChannel interfaces
Suspended due to incompatible speed	The interfaces belonging to the PortChannel have incompatible speeds.	
Suspended due to incompatible mode	The interfaces belonging to the PortChannel have incompatible modes.	
Suspended due to incompatible remote switch WWN	An improper connection is detected. All interfaces in a PortChannel must be connected to the same pair of switches.	

## Configuring Fibre Channel Interfaces

For the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter, you can configure a range of interfaces among internal ports or external ports, but you cannot mix both interface types within the same range. For example, “bay 1-10, bay 12” or “ext 0, ext 15-18” are valid ranges, but “bay 1-5, ext 15-17” is not.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Graceful Shutdown

Interfaces on a port are shut down by default (unless you modified the initial configuration).

The Cisco NX-OS software implicitly performs a graceful shutdown in response to either of the following actions for interfaces operating in the E port mode:

- If you shut down an interface.
- If a Cisco NX-OS software application executes a port shutdown as part of its function.

A graceful shutdown ensures that no frames are lost when the interface is shutting down. When a shutdown is triggered either by you or the Cisco NX-OS software, the switches connected to the shutdown link coordinate with each other to ensure that all frames in the ports are safely sent through the link before shutting down. This enhancement reduces the chance of frame loss.

A graceful shutdown is not possible in the following situations:

- If you physically remove the port from the switch.
- If in-order delivery (IOD) is enabled (for information about IOD, refer to the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*).
- If the Min\_LS\_interval interval is higher than 10 seconds. For information about FSPF global configuration, refer to the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.



### Note

This feature is only triggered if both switches at either end of this E port interface are MDS switches and are running Cisco SAN-OS Release 2.0(1b) or later, or MDS NX-OS Release 4.1(1a) or later.

## Setting the Interface Administrative State

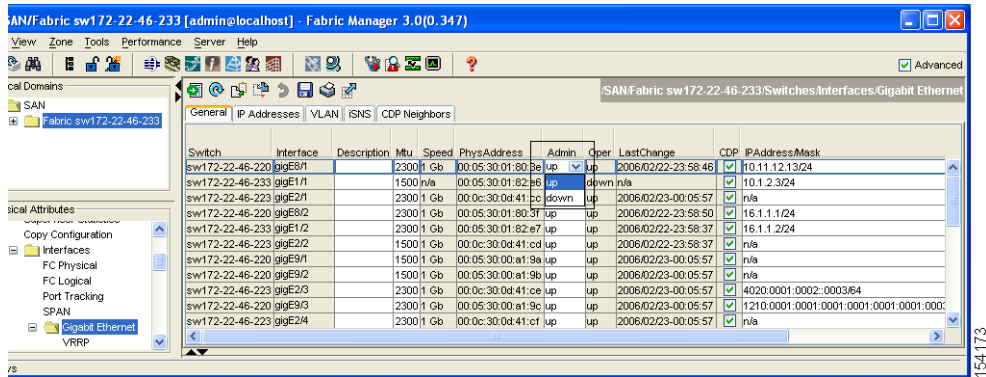
To disable or enable an interface using Fabric Manager, follow these steps:

- Step 1** Either expand **Switches > Interfaces** and then select **Gigabit Ethernet** or expand **Switches > Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
- Step 2** Click the **General** tab.
- Step 3** Click **Admin**.

You see the drop-down box shown in [Figure 2-3](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 2-3** Changing the Administrative Status of a Switch



- Step 4** Set the status to down (disable) or up (enable).
- Step 5** (Optional) Set other configuration parameters using the other tabs.
- Step 6** Click **Apply Changes**.

## Configuring Interface Modes

To configure the interface mode using Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Interfaces**, and then select **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** Click the **General** tab.
- Step 3** Click **Mode Admin**. Set the desired interface mode from the Admin drop-down menu.
- Step 4** (Optional) Set other configuration parameters using the other tabs.
- Step 5** Click **Apply Changes** icon.

## Configuring Port Administrative Speeds

By default, the port administrative speed for an interface is automatically calculated by the switch.



**Caution**

Changing the port administrative speed is a disruptive operation.

To configure administrative speed of the interface using Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Interfaces**, and then select **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** Click the **General** tab.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Step 3** Click **Speed Admin**. Set the desired speed from the drop-down menu.

The number indicates the speed in megabits per second (Mbps). You can set the speed to 1-Gbps, 2-Gbps, 4-Gbps, 8-Gbps, or **auto** (default).



**Note** On a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(2), you can configure the 8-Gbps administrative speed only on a M1060 switch module. You can configure the speed to 1-Gbps, 2-Gbps, or 4-Gbps on all switch modules on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(2) or earlier releases.

**Step 4** Click **Apply Changes**.

For internal ports on the Cisco Fabric Switch for HP c\_Class BladeSystem and Cisco Fabric Switch for IBM BladeCenter, a port speed of 1 Gbps is not supported. Auto-negotiation is supported between 2 Gbps and 4 Gbps only. Also, if the BladeCenter is a T chassis, then port speeds are fixed at 2 Gbps and auto-negotiation is not enabled.

## Autosensing

Autosensing speed is enabled on all 4-Gbps and 8-Gbps switching module interfaces by default. This configuration enables the interfaces to operate at speeds of 1 Gbps, 2 Gbps, or 4 Gbps on the 4-Gbps switching modules, and 8 Gbps on the 8-Gbps switching modules. When autosensing is enabled for an interface operating in dedicated rate mode, 4 Gbps of bandwidth is reserved, even if the port negotiates at an operating speed of 1 Gbps or 2 Gbps.

To avoid wasting unused bandwidth on 48-port and 24-port 4-Gbps and 8-Gbps Fibre Channel switching modules, you can specify that only 2 Gbps of required bandwidth be reserved, not the default of 4 Gbps or 8 Gbps. This feature shares the unused bandwidth within the port group provided that it does not exceed the rate limit configuration for the port. You can also use this feature for shared rate ports that are configured for autosensing.



**Tip**

When migrating a host that supports up to 2-Gbps traffic (that is, not 4 Gbps with autosensing capabilities) to the 4-Gbps switching modules, use autosensing with a maximum bandwidth of 2 Gbps. When migrating a host that supports up to 4-Gbps traffic (that is, not 8 Gbps with autosensing capabilities) to the 8-Gbps switching modules, use autosensing with a maximum bandwidth of 4 Gbps.

## Configuring the Interface Description

Interface descriptions enable you to identify the traffic or the use for that interface. The interface description can be any alphanumeric string.

## Specifying a Port Owner

Using the port owner feature, you can specify the owner of a port and the purpose for which a port is used so that the other administrators are informed.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Note**

The port guard and port owner features are available for all ports regardless of the operational mode.

To specify or remove the port owner using the Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** Click the **General** tab (see [Figure 2-4](#)) and then select the port.

**Figure 2-4 Fabric Manager - Port Owner**

Interface	Description	VSAN Id Port	VSAN Id Dynamic	Mode Admin	Mode Oper	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	Status FailureCause	Status WasEnabled	Status LastChange	Owner
fc1/1		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	abcdef
fc1/2		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/3		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	user1
fc1/4		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/9		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/12		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/15		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/16		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/17		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/18		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/19		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/20		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/21		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/22		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/23		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	
fc1/24		1	n/a	auto	auto	auto	n/a	dedicated	in	down	down	adminDown	false	n/a	

- Step 3** In the Owner text box, enter a port owner and the purpose for which port is used.



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

To specify or remove the port owner using the Device Manager, follow these steps:

- Step 1** Double-click the interface in the modules panel.
- Step 2** Click the **General** tab (see [Figure 2-5](#)).

**Figure 2-5** *Device Manager - Port Owner*

The screenshot shows the 'Device Manager - Port Owner' window for interface '172.23.147.148 - fc1/3'. The 'General' tab is selected. The window contains the following fields and options:

- Description:** A text input field.
- PortVSAN:** A dropdown menu set to '1'.
- DynamicVSAN:** A text input field.
- Mode:**
  - Admin: Radio buttons for auto (selected), F, FL, E, FX, SD, TL, FV, ST, NP.
  - Oper: auto
- Speed:**
  - Admin: Radio buttons for auto (selected), 1Gb, 2Gb, 4Gb, autoMax2G, 8Gb, autoMax4G.
  - Oper: n/a
  - RateMode: Radio buttons for dedicated (selected), shared.
- Status:**
  - Service: Radio buttons for in (selected), out.
  - Admin: Radio buttons for up, down (selected).
  - Oper: down
  - FailureCause: adminDown
  - WasEnabled: false
  - LastChange: n/a
- Others:**
  - Owner: A text input field containing 'user1'.

At the bottom right, there are four buttons: Apply, Refresh, Help, and Close.

- Step 3** In the Owner text box, enter a port owner and the purpose for which the port is used.
- Step 4** Click **Apply**.

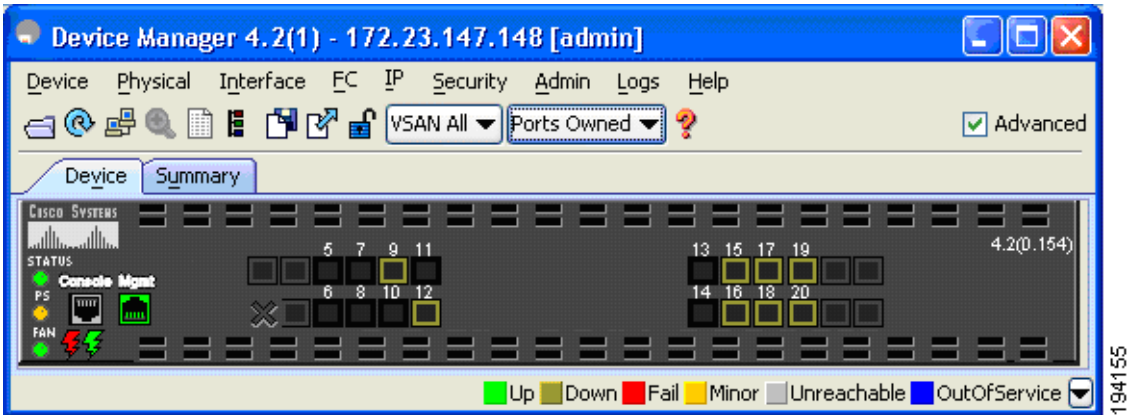
## Displaying the Owned Ports

To display the interfaces owned using the Device Manager, follow these steps:

- Step 1** From the menu bar, click the **Ports All** drop-down button, .

Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Figure 2-6 Device Manager - Ports Owned



Step 2 Select **Ports Owned** from the drop-down list (see [Figure 2-6](#)).

## Frame Encapsulation

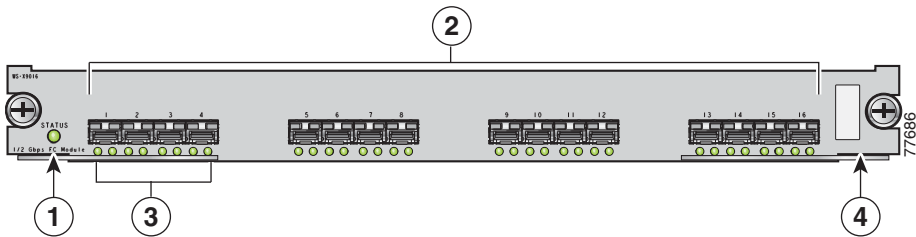
You can set the frame format to EISL for all frames transmitted by the interface in SD port mode. If you sent the frame encapsulation to EISL, all outgoing frames are transmitted in the EISL frame format, regardless of the SPAN sources. See the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*.

Refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide* to configure frame encapsulation on an interface.

## Identifying the Beacon LEDs

[Figure 2-7](#) displays the status, link, and speed LEDs in a 16-port switching module.

Figure 2-7 Cisco MDS 9000 Family Switch Interface Modes



1	Status LED <sup>1</sup>	3	Link LEDs <sup>1</sup> and speed LEDs <sup>2</sup>
2	1/2-Gbps Fibre Channel port group	4	Asset tag <sup>3</sup>

1. See the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*.
2. See the “About Speed LEDs” section on [page 2-17](#).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

3. Refer to the Cisco MDS 9000 Family hardware installation guide for your platform.

## About Speed LEDs

Each port has one link LED on the left and one speed LED on the right.

The speed LED displays the speed of the port interface:

- Off—The interface attached to that port is functioning at 1000 Mbps.
- On (solid green)—The interface attached to that port is functioning at 2000 Mbps (for 2 Gbps interfaces).

The speed LED also displays if the beacon mode is enabled or disabled:

- Off or solid green—Beacon mode is disabled.
- Flashing green—The beacon mode is enabled. The LED flashes at one-second intervals.



**Note**

Generation 2 and Generation 3 modules and fabric switches do not have speed LEDs.

## Configuring Beacon Mode

By default, the beacon mode is disabled on all switches. The beacon mode is indicated by a flashing green light that helps you identify the physical location of the specified interface. Configuring the beacon mode has no effect on the operation of the interface.

To enable beacon mode for a specified interface or range of interfaces using Fabric Manager, follow these steps:

---

**Step 1** Expand **Switches > Interfaces** and then select **Gigabit Ethernet**.

You see the interface configuration in the Information pane.

**Step 2** Enable the Beacon Mode option for the selected switch.

**Step 3** Click **Apply Changes**.

---



**Note**

The flashing green light turns on automatically when an external loopback is detected that causes the interfaces to be isolated. The flashing green light overrides the beacon mode configuration. The state of the LED is restored to reflect the beacon mode configuration after the external loopback is removed.

## About Bit Error Thresholds

The bit error rate threshold is used by the switch to detect an increased error rate before performance degradation seriously affects traffic.

The bit errors can occur for the following reasons:

- Faulty or bad cable.
- Faulty or bad GBIC or SFP.

## Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

- GBIC or SFP is specified to operate at 1 Gbps but is used at 2 Gbps.
- GBIC or SFP is specified to operate at 2 Gbps but is used at 4 Gbps.
- Short haul cable is used for long haul or long haul cable is used for short haul.
- Momentary sync loss.
- Loose cable connection at one or both ends.
- Improper GBIC or SFP connection at one or both ends.

A bit error rate threshold is detected when 15 error bursts occur in a 5-minute period. By default, the switch disables the interface when the threshold is reached. You can enter a **shutdown** and **no shutdown** command sequence to reenable the interface.

You can configure the switch to not disable an interface when the threshold is crossed. By default, the threshold disables the interface.

Refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide* to disable the bit error threshold for an interface.



### Note

Regardless of disabling the switch port ignore bit-error threshold for an interface, the switch generates a syslog message when bit-error threshold events are detected.

## Switch Port Attribute Default Values

You can configure attribute default values for various switch port attributes. These attributes will be applied globally to all future switch port configurations, even if you do not individually specify them at that time.

Refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide* to configure switch port attributes.

## About SFP Transmitter Types

The small form-factor pluggable (SFP) hardware transmitters are identified by their acronyms when displayed. [Table 2-5](#) defines the acronyms used for SFPs.

**Table 2-5 SFP Transmitter Acronym Definitions**

Definition	Acronym
<b>Standard transmitters defined in the GBIC specifications</b>	
short wavelaser	swl
long wavelaser	lwl
long wavelaser cost reduced	lwcr
electrical	elec
<b>Extended transmitters assigned to Cisco-supported SFPs</b>	
CWDM-1470	c1470
CWDM-1490	c1490
CWDM-1510	c1510

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 2-5 SFP Transmitter Acronym Definitions (continued)**

Definition	Acronym
<b>Standard transmitters defined in the GBIC specifications</b>	
CWDM-1530	c1530
CWDM-1550	c1550
CWDM-1570	c1570
CWDM-1590	c1590
CWDM-1610	c1610

See the “[Displaying SFP Transmitter Types](#)” section on page 2-19.

## Displaying SFP Transmitter Types

To show the SFP types for an interface using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
- Step 2** Click the **Physical** tab to see the transmitter type for the selected interface.
- 

## Gathering Interface Statistics

You can use Fabric Manager or Device Manager to collect interface statistics on any switch. These statistics are collected at intervals that you can set.



### Note

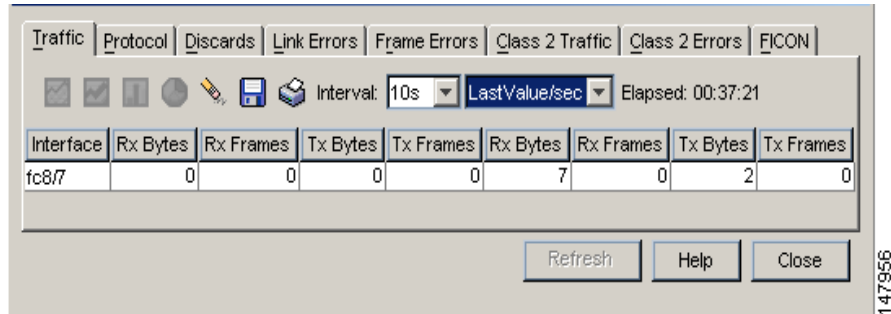
In Fabric Manager, you can collect interface statistics by expanding **Switches > ISLs** and selecting **Statistics** from the Physical Attributes pane.

To gather and display interface counters using Device Manager, follow these steps:

- 
- Step 1** Right-click an interface and select **Monitor**.  
You see the Interface Monitor dialog box.
- Step 2** Set both the number of seconds at which you want to poll the interface statistics and how you want the data represented in the Interval drop-down menus. For example, click **10s** and **LastValue/sec**.
- Step 3** Select any tab (see in [Figure 2-8](#)) to view those related statistics.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 2-8 Device Manager Interface Monitor Dialog Box**



- Step 4** (Optional) Click the **Pencil** icon to reset the cumulative counters.
- Step 5** (Optional) Click the **Save** icon to save the gathered statistics to a file or select the **Print** icon to print the statistics.
- Step 6** Click **Close** when you are finished gathering and displaying statistics.

## TL Ports for Private Loops

Private loops require setting the interface mode to TL. This section describes TL ports and includes the following sections:

- [About TL Ports, page 2-20](#)
- [Configuring TL Ports, page 2-22](#)
- [About TL Port ALPA Caches, page 2-22](#)

## About TL Ports

Private loop devices refer to legacy devices that reside on arbitrated loops. These devices are not aware of a switch fabric because they only communicate with devices on the same physical loop. The legacy devices are used in Fibre Channel networks, and devices outside the loop may need to communicate with them. The communication functionality is provided through TL ports. See the [“About Interface Modes” section on page 2-3](#).

TL port mode is not supported on the following hardware:

- Generation 2 switching module interfaces
- Cisco MDS 9124 Fabric Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

Follow these guidelines when configuring private loops:

- A maximum of 64 fabric devices can be proxied to a private loop.
- Fabric devices must be in the same zone as private loop devices to be proxied to the private loop.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Each private device on a TL port may be included in a different zone.
- All devices on the loop are treated as private loops. You cannot mix private and public devices on the loop if the configured port mode is TL.
- The only FC4-type supported by TL ports is SCSI (FCP).
- Communication between a private initiator to a private target on the same private loop does not invoke TL port services.

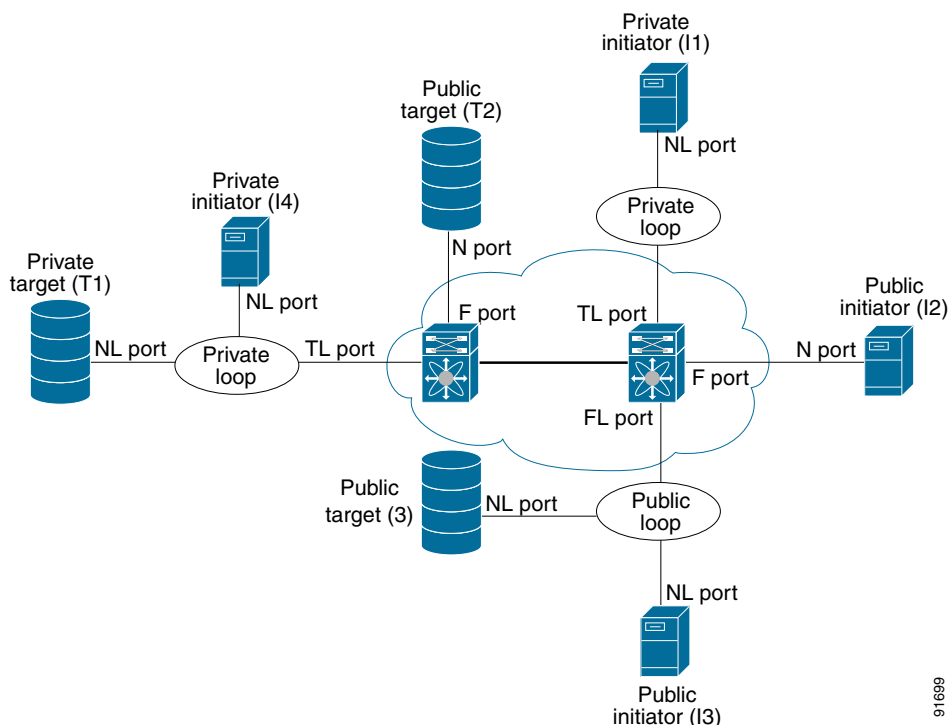
Table 2-6 lists the TL port translations supported in Cisco MDS 9000 Family switches.

**Table 2-6 Supported TL Port Translations**

Translation from	Translation to	Example
Private initiator	Private target	From I1 to T1 or vice versa
Private initiator	Public target — N port	From I1 to T2 or vice versa
Private initiator	Public target — NL port	From I4 to T3 or vice versa
Public initiator — N port	Private target	From I2 to T1 or vice versa
Public initiator — NL port	Private target	From I3 to T1 or vice versa

Figure 2-9 shows examples of TL port translation support.

**Figure 2-9 TL Port Translation Support Examples**



91669

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Configuring TL Ports

To configure the TL interface mode using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
  - Step 2** Click the **General** tab and click **Mode Admin**.
  - Step 3** Set the Mode Admin drop-down menu to **TL**.
  - Step 4** (Optional) Set other configuration parameters using the other tabs.
  - Step 5** Click **Apply Changes**.
- 

## About TL Port ALPA Caches

Although TL ports cannot be automatically configured, you can manually configure entries in arbitrated loop physical address (ALPA) caches. Generally, ALPA cache entries are automatically populated when an ALPA is assigned to a device. Each device is identified by its port world wide name (pWWN). When a device is allocated an ALPA, an entry for that device is automatically created in the ALPA cache.

A cache contains entries for recently allocated ALPA values. These caches are maintained on various TL ports. If a device already has an ALPA, the Cisco NX-OS software attempts to allocate the same ALPA to the device each time. The ALPA cache is maintained in persistent storage and saves information across switch reboots. The maximum cache size is 1000 entries. If the cache is full, and a new ALPA is allocated, the Cisco NX-OS software discards an inactive cache entry (if available) to make space for the new entry. See the [“TL Port” section on page 2-5](#) for more information on TL ports.

Refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide* to manage the TL Port ALPA cache.

## Configuring Port Guard

The port guard feature is intended for use in environments where the system and application environment does not adapt quickly and efficiently to a port going down and back up, or to a port rapidly cycling up and down, which can happen in some failure modes. For example, if a system takes five seconds to stabilize after a port goes down, but the port is going up and down once a second, this might ultimately cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after specified number of failures in a specified time period. This allows the SAN administrator to intervene and control the recovery, avoiding any problems caused by the cycling.

Using the port guard feature, you can restrict the number of error reports and bring a malfunctioning port to down state dynamically. A port can be configured to go into error-disabled state for specific types of failures.

A general link failure caused by link-down is the superset of all other causes. The sum of the number of all other causes equals to the number of link-down link failures. This means a port is brought to down state when it reaches the maximum number of allowed link failures or the number of specific causes.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

The causes of link failure can be any of the following:

- ESP trustsec-violation
- Bit-errors
- Signal loss
- Sync loss
- Link reset
- Credit loss
- Additional causes might be the following:
  - Not operational (NOS).
  - Too many interrupts.
  - Cable is disconnected.
  - Hardware recoverable errors.
  - The connected device rebooted (F ports only).
  - The connected linecard rebooted (ISL only).

Link down is the superset of all other causes. A port is brought to down state if the total number of other causes equals to the number of allowed link-down failures.

**Note**

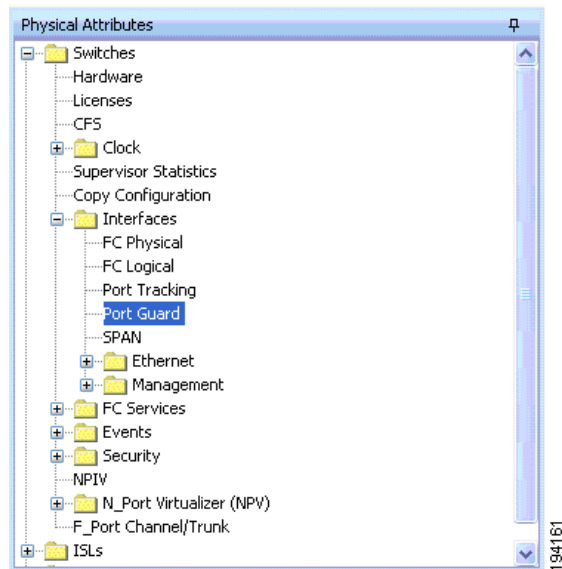
Even if the link does not flap due to failure of the link, and port guard is not enabled, the port goes into a down state if too many invalid FLOGI requests are received from the same host.

To enable port guard using Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Interfaces**, and then select **Port Guard** from the Physical Attributes pane. You see the interfaces listed in the Information pane. ([Figure 2-10](#))

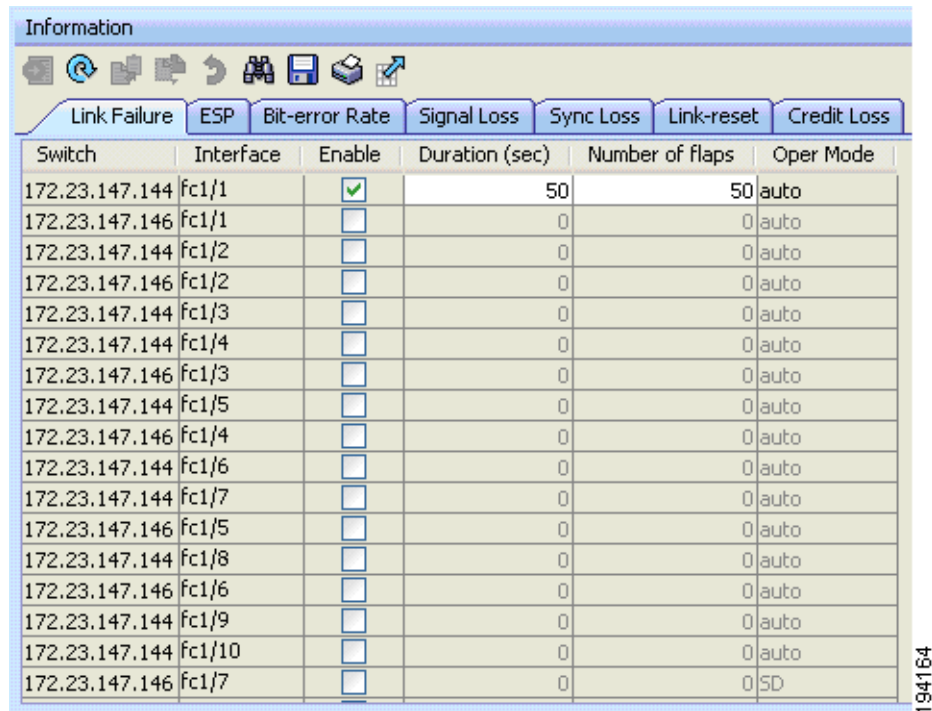
***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 2-10**      **Fabric Manager - Port Guard**



**Step 2** Click the **Link Failure** tab and then select the port (see [Figure 2-11](#)).

**Figure 2-11**      **Fabric Manager - Port Guard**



**Step 3** Check the check box in the Enable column.

**Step 4** (Optional) Enter the Duration in seconds and the number of flaps. If the values are 0, the port is brought to down state if the link flaps even once. Otherwise, the link is brought to down state if the link flaps for the number of flaps within the duration.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 5** Click **Apply** to activate the configuration.
- Step 6** Click the **ESP** tab and then select the port. (Figure 2-12)

**Figure 2-12 Fabric Manager - Port Guard**

Switch	Interface	Enable	Duration (sec)	Number of flaps	Oper Mode
172.23.147.144	fc1/1	<input checked="" type="checkbox"/>	40	40	auto
172.23.147.146	fc1/1	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/2	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/2	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/3	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/4	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/3	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/5	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/4	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/6	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/5	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/7	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/8	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/6	<input type="checkbox"/>	0	0	auto
172.23.147.144	fc1/9	<input type="checkbox"/>	0	0	auto
172.23.147.146	fc1/7	<input type="checkbox"/>	0	0	SD
172.23.147.144	fc1/10	<input type="checkbox"/>	0	0	auto

- Step 7** Check the check box in the Enable column.
- Step 8** (Optional) Enter the duration in seconds and the number of flaps. If the values are 0, the port is brought to down state if a trustsec violation occurs even once. Otherwise, the link is brought to down state if there is trustsec violation for the number of flaps within the duration.
- Step 9** Click the **Bit-error Rate**, **Signal Loss**, **Sync Loss**, **Link-reset**, and **Credit Loss** tabs and complete the port guard configuration.
- Step 10** Click **Apply** to activate the configuration.

To enable port guard for single or multiple interfaces using Device Manager, follow these steps:

- Step 1** From the menu bar, select **Interface > Port Guard**.  
You see the FC Interfaces listed.
- Step 2** Click the **Link Failure** tab and then select the port.
- Step 3** Check the check box in the Enable column.
- Step 4** (Optional) Enter the duration in seconds and the number of flaps. If the values are 0, the port goes into a down state even if the link flaps once. Otherwise, the link goes into a down state if the link flaps for the number of flaps within the duration.
- Step 5** Click **Apply** to activate the configuration.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 6** Click the **ESP** tab and then select the port.
- Step 7** Check the check box in the Enable column.
- Step 8** (Optional) Enter the Duration in seconds and the number of flaps. If the values are 0, the port is brought to down state if a trsutsec violation occurs even once. Otherwise, the link is brought to down state if a trustsec violation occurs for the number of flaps within the duration.
- Step 9** Click **Apply** to activate the configuration.

## Configuring Port Monitor

Port monitor helps to monitor the performance and the status of ports and generate alerts when problems occur. You can configure the thresholds for various counters and trigger an event when the values cross the threshold settings.

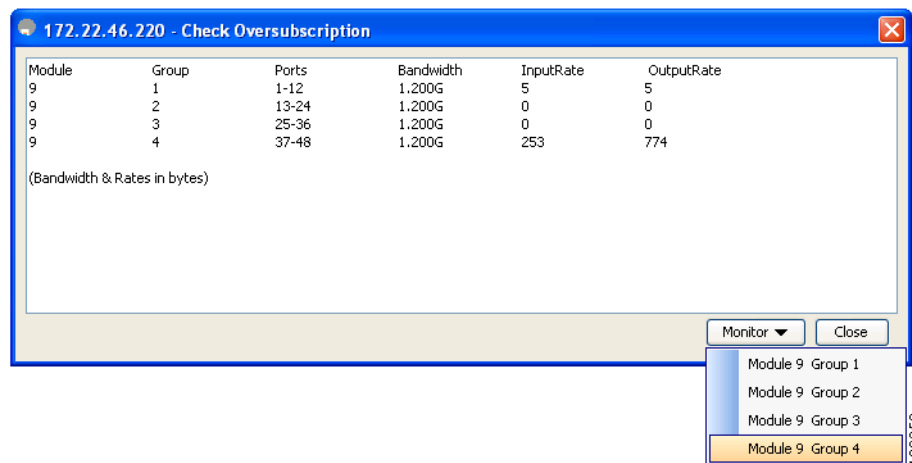
For information about configuring port monitor, refer to the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*.

## Port Group Charting

To monitor a particular group using Device Manager, follow these steps:

- Step 1** Right-click on any port group module and select **Check Oversubscription**.  
The **Check Oversubscription** table is displayed.
- Step 2** From the **Monitor** drop-down list box, select one particular group to monitor (Figure 2-13).

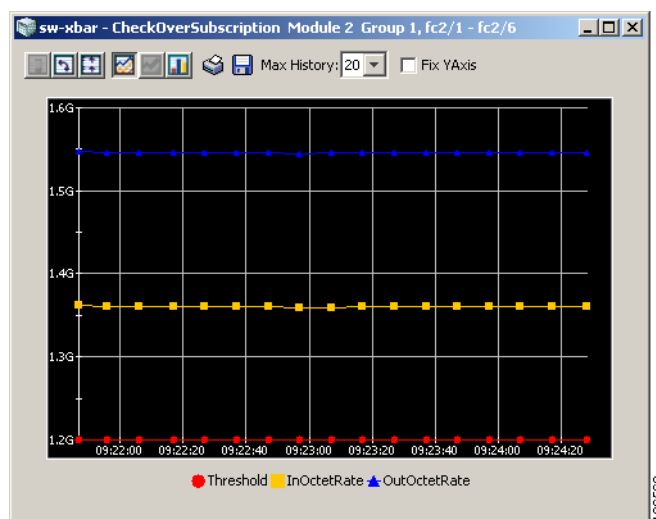
**Figure 2-13 Port Group Charting**



The Device Manager will display the monitoring table of the selected group with counters on each interval and displays the line chart automatically (see Figure 2-14). From the Monitoring table, you can also chose the **Bar chart** icon to view the selected group as Bar charts.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 2-14 Line Chart Example**



## Management Interfaces

You can remotely configure the switch through the management interface (mgmt0). To configure a connection on the mgmt0 interface, you must configure either the IP version 4 (IPv4) parameters (IP address, subnet mask, and default gateway) or the IP version 6 (IPv6) parameters so that the switch is reachable.

This section describes the management interfaces and includes the following topics:

- [About Management Interfaces, page 2-27](#)
- [Configuring Management Interfaces, page 2-27](#)

## About Management Interfaces

Before you begin to configure the management interface manually, obtain the switch's IPv4 address and subnet mask, or the IPv6 address.

The management port (mgmt0) is autosensing and operates in full-duplex mode at a speed of 10/100/1000 Mbps. Autosensing supports both the speed and the duplex mode. On a Supervisor-1 module, the default speed is 100 Mbps and the default duplex mode is auto. On a Supervisor-2 module, the default speed is auto and the default duplex mode is auto.



**Note**

You need to explicitly configure a default gateway to connect to the switch and send IP packets or add a route for each subnet.

## Configuring Management Interfaces

To configure the mgmt0 Ethernet interface using Fabric Manager, follow these steps:

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- 
- Step 1** Select a VSAN in the Logical Domains pane.
- Step 2** Expand **Switches > Interfaces** and then select **Management**.  
You see the interface configuration in the Information pane.
- Step 3** Click the **General** tab.
- Step 4** Set the IP Address/Mask field.
- Step 5** Set Admin to **up**.
- Step 6** (Optional) Set other configuration parameters using the other tabs.
- Step 7** Click **Apply Changes**.
- 

## VSAN Interfaces

VSANs apply to Fibre Channel fabrics and enable you to configure multiple isolated SAN topologies within the same physical infrastructure. You can create an IP interface on top of a VSAN and then use this interface to send frames to this VSAN. To use this feature, you must configure the IP address for this VSAN. VSAN interfaces cannot be created for nonexistent VSANs.

This section describes VSAN interfaces and includes the following topics:

- [About VSAN Interfaces, page 2-28](#)
- [Creating VSAN Interfaces, page 2-28](#)

## About VSAN Interfaces

Follow these guidelines when creating or deleting VSAN interfaces:

- Create a VSAN before creating the interface for that VSAN. If a VSAN does not exist, the interface cannot be created.
- Create the interface VSAN—it is not created automatically.
- If you delete the VSAN, the attached interface is automatically deleted.
- Configure each interface only in one VSAN.



**Tip**

After configuring the VSAN interface, you can configure an IP address or Virtual Router Redundancy Protocol (VRRP) feature. See the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*.

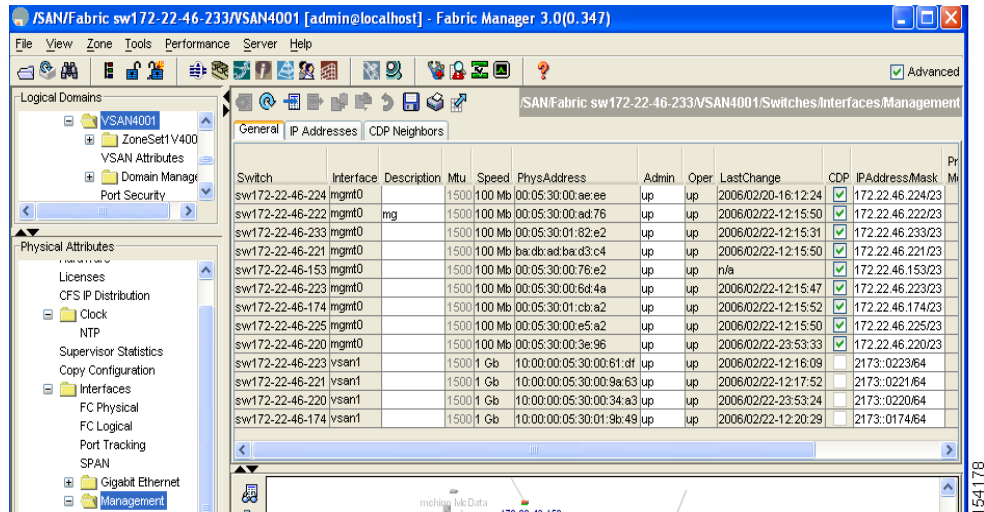
## Creating VSAN Interfaces

To create a VSAN interface using Fabric Manager, follow these steps:

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

- Step 1** Expand **Switches > Interfaces** and then select **Management** (see Figure 2-15).

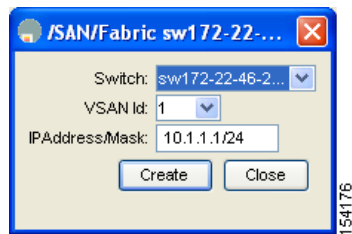
**Figure 2-15** General Management Tab



- Step 2** Click **Create Row**.

You see the Create Interface dialog box (see Figure 2-16).

**Figure 2-16** Create Interface Dialog Box



- Step 3** Select the switch and VSAN ID for which you want to configure a VSAN interface.



**Note** You can only create a VSAN interface for an existing VSAN. If the VSAN does not exist, you cannot create a VSAN interface for it.

- Step 4** Set IPAddress/Mask to the IP address and subnet mask for the new VSAN interface.

- Step 5** Click **Create** to create the VSAN interface or click **Close** to close the dialog box without creating the VSAN interface.

## Default Settings

Table 2-7 lists the default settings for interface parameters.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 2-7**      **Default Interface Parameters**

Parameters	Default
Interface mode	Auto
Interface speed	Auto
Administrative state	Shutdown (unless changed during initial setup)
Trunk mode	On (unless changed during initial setup) on non-NPV and NPIV core switches. Off on NPV switches.
Trunk-allowed VSANs or VF-IDs	1 to 4093
Interface VSAN	Default VSAN (1)
Beacon mode	Off (disabled)
EISL encapsulation	Disabled
Data field size	2112 bytes





## CHAPTER 3

# Configuring Ethernet Interfaces

---

Fabric Manager and Device Manager display configuration settings and status information about the physical Ethernet interfaces on Cisco Nexus 5000 Series switches. However, you cannot change the configuration for physical Ethernet interfaces using Fabric Manager or Device Manager.

This chapter includes the following sections:

- [About Ethernet Interfaces, page 3-1](#)
- [Displaying Interface Information, page 3-1](#)
- [Default Settings, page 3-3](#)

## About Ethernet Interfaces

The Ethernet ports can operate as standard Ethernet interfaces connected to servers or to a LAN. The Ethernet interfaces also support Fibre Channel over Ethernet (FCoE). FCoE allows the physical Ethernet link to carry both Ethernet and Fibre Channel traffic.

On a Cisco Nexus 5000 Series switch, the Ethernet interfaces are enabled by default.

## Displaying Interface Information

Fabric Manager and Device Manager display configuration settings and status information about the physical Ethernet interfaces on Cisco Nexus 5000 Series switches.

This section describes how to display the Ethernet interface status and includes the following topics:

- [Displaying Interface Information Using Fabric Manager, page 3-1](#)
- [Displaying Interface Information Using Device Manager, page 3-2](#)

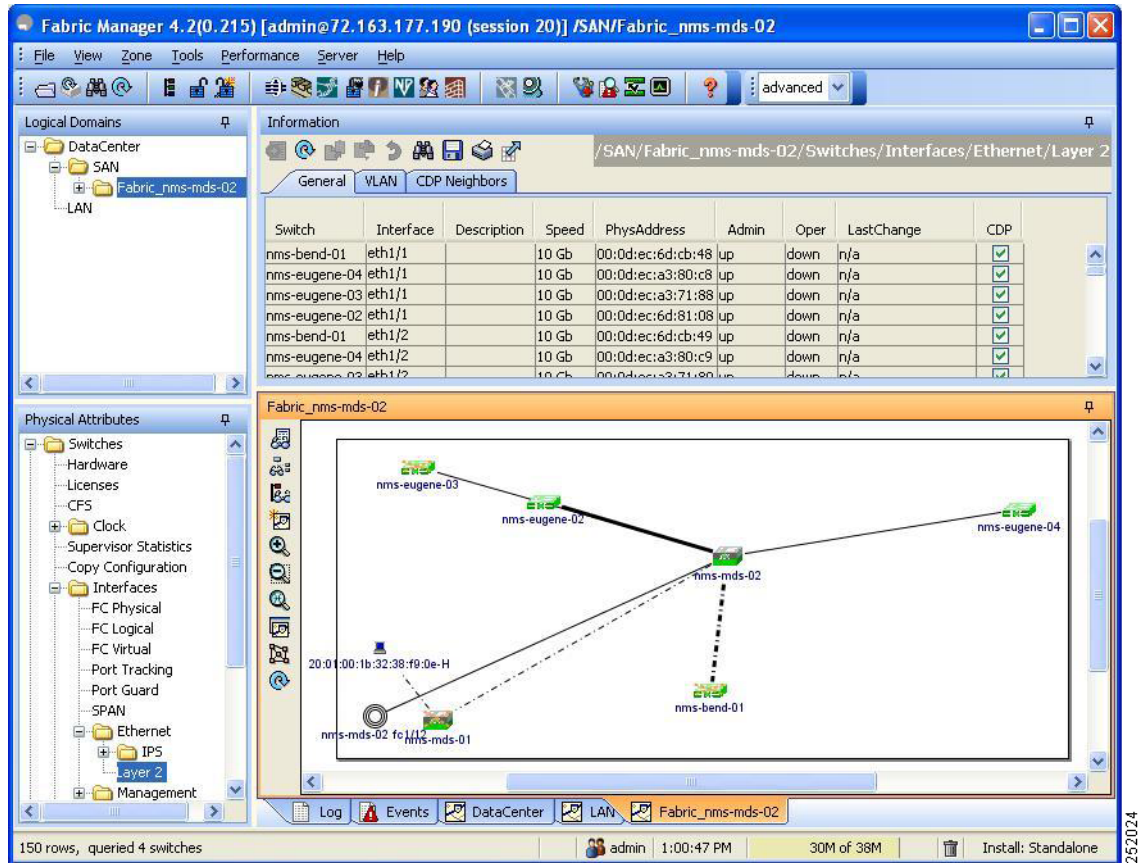
## Displaying Interface Information Using Fabric Manager

To display Ethernet interfaces using Fabric Manager, follow these steps:

- 
- Step 1** In the Physical Attributes pane, expand **Switches > Interfaces > Ethernet**, and then choose **Layer2**. You see the Ethernet interface information pane (see [Figure 3-1](#)).
- The General tab displays the description, speed, MAC address, and status for each Ethernet interface.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 3-1 Ethernet Information Pane**



- Step 2** Click the **VLAN** tab to display the VLAN assigned to each interface.
- Step 3** Click the **CDP Neighbors** tab to display the CDP neighbor assigned to each interface.

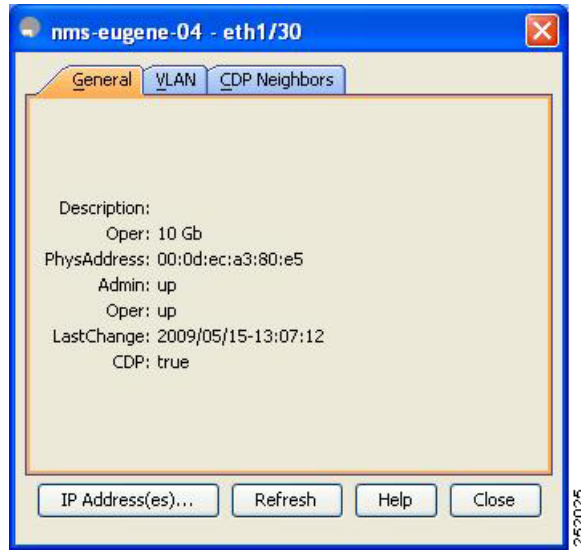
## Displaying Interface Information Using Device Manager

To display Ethernet interfaces using Device Manager, follow these steps:

- Step 1** Launch Device Manager from the Cisco Nexus 5000 Series switch.
- Step 2** Choose **Interface > Ethernet**.
- You see the Ethernet Interfaces dialog box (see [Figure 3-2](#)).
- The General tab displays the description, speed, MAC address, and status for each interface.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 3-2 Ethernet Interfaces Dialog Box**



**Step 3** Click the **VLAN** tab to display the VLAN assigned to each interface. Click the **CDP Neighbors** tab to display the CDP neighbor assigned to each interface.

## Default Settings

Table 3-1 lists the default settings for all physical Ethernet interfaces.

**Table 3-1 Default Ethernet Interface Parameters**

Parameters	Default
Oper Speed	10 GB
Admin Status	Up
CDP	True
VLAN Type	Static
VLAN List	1

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***



## CHAPTER 4

# Configuring Virtual Fibre Channel Interfaces

---

This chapter describes how to configure virtual Fibre Channel (FC) interfaces on a Cisco Nexus 5000 Series switch.



### Note

Before you configure virtual FC interfaces on a Cisco Nexus 5000 Series switch, you must enable and configure Fibre Channel over Ethernet (FCoE) on the switch. For information on enabling and configuring FCoE, refer to the *Cisco Fabric Manager Fabric Configuration Guide*.

---

This chapter includes the following sections:

- [About Virtual Fibre Channel Interfaces, page 4-1](#)
- [Guidelines and Limitations, page 4-1](#)
- [Configuring Virtual Fibre Channel Interfaces, page 4-2](#)
- [Default Settings, page 4-16](#)

## About Virtual Fibre Channel Interfaces

Cisco Nexus 5000 Series switches support FCoE, which allows Fibre Channel and Ethernet traffic to be carried on the same physical Ethernet connection between the switch and the servers.

The Fibre Channel portion of FCoE is configured as a virtual Fibre Channel interface. Logical Fibre Channel features (such as interface mode) can be configured on virtual FC interfaces. A virtual FC interface must be bound to an interface before it can be used.



### Note

Virtual FC interfaces are created with the administrative state set to down. You need to explicitly configure the administrative state to bring the virtual FC interface into operation.

---

## Guidelines and Limitations

When configuring virtual FC interfaces, note the following guidelines and limitations:

- Each virtual FC interface can be bound to one of the following interfaces:
  - An Ethernet interface.
  - An Ethernet PortChannel.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- A media access control (MAC) address of an FCoE Node (ENode) or a remote Fibre Channel Forwarder (FCF) identified by the virtual FC interface.
- An Ethernet host interface on a Cisco Nexus 2000 Series Fabric Extender.
- FCoE is supported only on 10-Gigabit Ethernet interfaces.
- FCoE is not supported on private VLANs.

## Configuring Virtual Fibre Channel Interfaces

This section describes how to configure virtual FC interfaces and includes the following topics:

- [Overview, page 4-2](#)
- [Configuring a Virtual Fibre Channel Interface, page 4-2](#)
- [Mapping VLANs to VSANs, page 4-5](#)
- [Assigning Fibre Channel VSAN Membership, page 4-8](#)
- [Creating a Virtual Fibre Channel Interface, page 4-8](#)
- [Deleting a Virtual Fibre Channel Interface, page 4-15](#)

### Overview

You can configure a virtual FC interface on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.0(1a) or later releases. You can bind a virtual FC interface to a physical Ethernet interface, an Ethernet PortChannel, or a remote MAC address.

The Ethernet interface that you bind the virtual FC interface to must be configured as follows:

- The Ethernet interface must be a trunk port (use the **switchport mode trunk** command).
- The FCoE VLAN that corresponds to the virtual Fibre Channel's VSAN must be in the allowed VLAN list.
- The FCoE VLAN must not be configured as the native VLAN of the trunk port.
- The Ethernet interface must be configured as PortFast (use the **spanning-tree port type edge trunk** command).

Following the above configuration guidelines will ensure a smooth upgrade to a T11 Fibre Channel Initialization Protocol (FIP)-based FCoE release in the future.

## Configuring a Virtual Fibre Channel Interface

This section describes how to configure a virtual FC interface and includes the following topics:

- [Configuring a Virtual Fibre Channel Interface Using Fabric Manager, page 4-2](#)
- [Configuring a Virtual Fibre Channel Interface Using Device Manager, page 4-4](#)

### Configuring a Virtual Fibre Channel Interface Using Fabric Manager

To configure virtual FC interfaces using Fabric Manager, follow these steps:

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 1** In the Physical Attributes pane, expand **Switches > Interfaces**, and then choose **VFC (FCoE)**.

You see the FC Virtual information pane shown in [Figure 4-1](#).

The General tab in the Information pane displays the description, bind type, bound interface, bound MAC address, FCF priority value, VSAN port, and status for each virtual FC interface.

**Figure 4-1 FC Virtual Information Pane**

Switch	Interface	Description	Bind Type	Bind Interface	Bind MACAddress	FCF Priority	Port VSAN	Mode Admin	Mode Oper	Status Service	Status Admin	Status Oper	FailureCause	LastChange
nms-eugene-03	vfc1		interfaceIndex	eth1/1	00:00:00:00:00:00	0	1F	auto	in	down	down	down	adminDown	n/a

**Step 2** In the Information pane, in the FC Virtual table, click a virtual FC interface row to configure, and do the following:

- a. (Optional) You can modify the bind type for the selected virtual FC interface. To do so, click the **Bind Type** column. From the drop-down list, choose **interfaceIndex** or **macAddress**.



**Note**

You cannot modify the bind type value of a virtual FC interface on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to Release 4.1(3). On such a switch, the Bind Type column will display interfaceIndex as the bind type.

- b. (Optional) Double-click the **Bind Interface** column to choose a physical Ethernet interface or Ethernet PortChannel that will be bound to the virtual FC interface.



**Note**

This column is dimmed if the Bind Type value is macAddress.

In the Bind Interface column, you can bind a virtual FC interface to one of the following:

- A physical Ethernet interface that runs at 10-Gigabit Ethernet speed.
  - An Ethernet PortChannel on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.1(3) or later releases. The Ethernet PortChannel must have only one interface that runs at 10-Gigabit Ethernet speed.
  - An Ethernet host interface on a Cisco Nexus 2000 Series Fabric Extender. However, you cannot bind the Ethernet host interface of a Cisco Nexus N2224TP Series Fabric Extender, Cisco Nexus N2232TP Series Fabric Extender, or Cisco Nexus N2232TT Series Fabric Extender.
- c. (Optional) Double-click the **Bind MAC Address** column to enter the MAC address of the ENode or the remote FCF.

This column is dimmed if the Bind Type value is interfaceIndex.

- d. (Optional) Double-click the **FCF Priority** column to enter a FCF priority value for the virtual FC interface. The value that you enter in this field will override the default FCF Priority value you configured in the FCoE Information pane. For more information on configuring FCoE, refer to the *Cisco Fabric Manager Fabric Configuration Guide*.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Note**

You cannot modify the FCF Priority value on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to Release 4.1(3).

e. In the Information pane toolbar, click the **Apply Changes** icon to save the configuration.

**Step 3** In the Information pane toolbar, click the **Create Row** icon to create a virtual FC interface. For more information, see the “[Creating a Virtual Fibre Channel Interface Using Fabric Manager](#)” section on page 4-13.

**Step 4** In the Information pane toolbar, click the **Delete Row** icon to delete a virtual FC interface. For more information, see the “[Deleting a Virtual Fibre Channel Interface](#)” section on page 4-15.

## Configuring a Virtual Fibre Channel Interface Using Device Manager

To configure virtual FC interfaces using Device Manager, follow these steps:

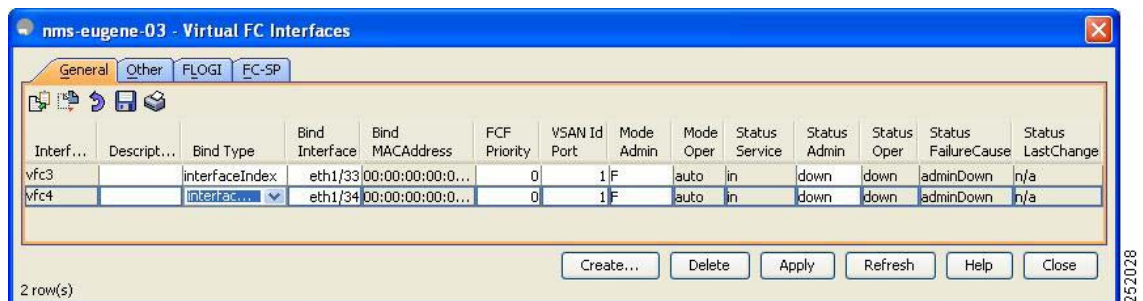
**Step 1** Launch Device Manager from the Cisco Nexus 5000 Series switch.

**Step 2** Choose **Interface > Virtual Interfaces > Fibre Channel**.

You see the Virtual FC Interfaces dialog box shown in [Figure 4-2](#).

The General tab displays the description, bind type, bound interface, bound MAC address, FCF priority value, VSAN port, and status for each virtual FC interface.

**Figure 4-2 Virtual FC Interfaces Dialog Box**



**Step 3** Click a virtual FC interface row to configure. Modify the values for the virtual FC interface.

**Note**

- In the Bind Interface column, you can bind a virtual FC interface to one of the following:
- A physical Ethernet interface that runs at 10-Gigabit Ethernet speed.
  - An Ethernet PortChannel on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.1(3) or later releases. The Ethernet PortChannel must have only one interface that runs at 10-Gigabit Ethernet speed.
  - An Ethernet host interface on a Cisco Nexus 2000 Series Fabric Extender. However, you cannot bind the Ethernet host interface of a Cisco Nexus N2224TP Series Fabric Extender, Cisco Nexus N2232TP Series Fabric Extender, or Cisco Nexus N2232TT Series Fabric Extender.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

For more information, see the “Configuring a Virtual Fibre Channel Interface Using Fabric Manager” section on page 4-2.

- Step 4** Click **Apply** to save the configuration.
  - Step 5** Click **Create** to create a virtual FC interface. For more information, see the “Creating a Virtual Fibre Channel Interface Using Device Manager” section on page 4-14.
  - Step 6** Click **Delete** to delete a virtual FC interface. For more information, see the “Deleting a Virtual Fibre Channel Interface” section on page 4-15.
- 

## Mapping VLANs to VSANs

A VLAN-VSAN mapping indicates the VLAN that is used to transport Fibre Channel traffic for a specific VSAN. Each virtual FC interface is associated with only one VSAN. Any VSAN with associated virtual FC interfaces must be mapped to a dedicated FCoE-enabled VLAN. FCoE is not supported on private VLANs.

This section provides information about how to map a VLAN to a VSAN and includes the following topics:

- [Mapping VLANs to VSANs Using Fabric Manager, page 4-5](#)
- [Mapping VLANs to VSANs Using Device Manager, page 4-7](#)

### Mapping VLANs to VSANs Using Fabric Manager

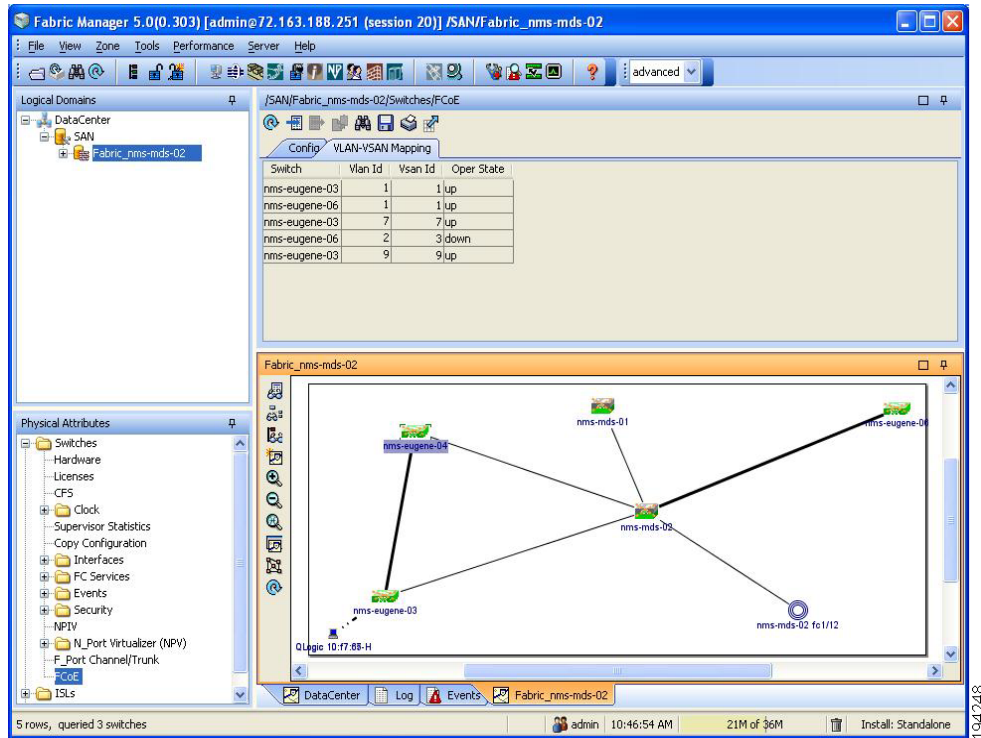
To create a mapping between a VSAN and its associated VLAN using Fabric Manager, follow these steps:

- 
- Step 1** In the Physical Attributes pane, choose **Switches > FCoE**.
  - Step 2** In the Information pane, click the **VLAN-VSAN Mapping** tab.  
You see the VLAN-VSAN Mapping information pane shown in [Figure 4-3](#).

The VLAN-VSAN Mapping tab displays the existing VLAN-VSAN mappings and the operational state of the VLAN-VSAN associations. You cannot modify an existing VLAN-VSAN mapping.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 4-3 VLAN-VSAN Mapping Information Pane**



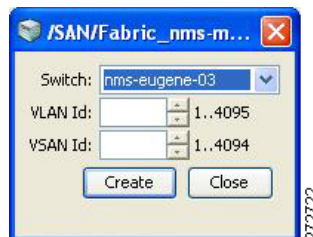
**Step 3** In the Information pane toolbar, click the **Create Row** icon to create a new mapping.



**Note** You must have a Cisco Nexus 5000 Series switch in the fabric to map a VLAN to a VSAN.

You see the Create dialog box shown in Figure 4-4.

**Figure 4-4 Create VLAN-VSAN Mapping**



**Step 4** From the Switch drop-down list, choose a Cisco Nexus 5000 Series switch.

**Step 5** In the VLAN Id and VSAN Id fields, enter the VLAN ID and the VSAN ID that will be mapped together.



**Note** The VLAN must already exist on the switch. If you enter a nonexistent VLAN ID to create the mapping, the mapping operation will fail.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 6** Click **Create** to create the mapping.

## Mapping VLANs to VSANs Using Device Manager

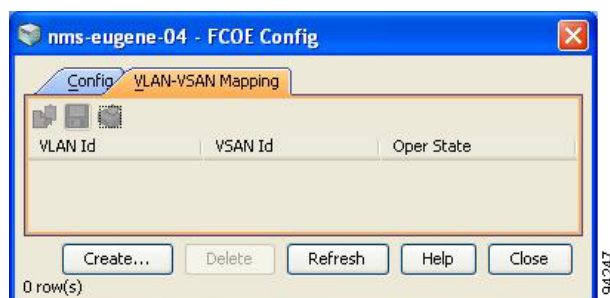
To create a mapping between a VSAN and its associated VLAN using Device Manager, follow these steps:

- Step 1** Launch Device Manager from the Cisco Nexus 5000 Series switch.

- Step 2** Choose **FCoE > Config**.

You see the FCoE Config dialog box shown in [Figure 4-5](#).

**Figure 4-5 FCoE Config Dialog Box**



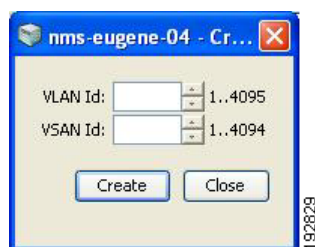
- Step 3** Click the **VLAN-VSAN Mapping** tab.

The VLAN-VSAN Mapping tab lists the existing VLAN-VSAN mappings and the operational state of the VLAN-VSAN associations. You cannot modify an existing VLAN-VSAN mapping.

- Step 4** Click **Create** to create a new mapping.

You see the Create VLAN-VSAN Mapping dialog box shown in [Figure 4-6](#).

**Figure 4-6 Create VLAN-VSAN Mapping**



- Step 5** In the VLAN Id and VSAN Id fields, enter the VLAN ID and the VSAN ID that will be mapped together.



**Note**

The VLAN must already exist on the switch. If you enter a nonexistent VLAN ID to create the mapping, the mapping operation will fail.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Step 6** Click **Create** to create the mapping.

## Assigning Fibre Channel VSAN Membership

To associate a virtual FC interface with a VSAN port using Device Manager, follow these steps:

**Step 1** Launch Device Manager from the Cisco Nexus 5000 Series switch.

**Step 2** Choose **FC > VSANs**.

You see the VSAN dialog box shown in [Figure 4-7](#).

**Figure 4-7 VSAN Dialog Box**



**Step 3** Click the **Membership** tab. This tab displays the virtual FC interfaces associated with VSAN ports.

**Step 4** For each VSAN port in the table, double-click the following VSAN parameters and choose a value to associate the virtual FC interface with the VSAN:

- **FC**—Fibre Channel ports in VSAN
- **Channels**—Ethernet PortChannels in VSAN
- **FC Virtual Interface**—Fibre Channel virtual interface to associate with the VSAN port

**Step 5** Click **Apply** to save the changes.

## Creating a Virtual Fibre Channel Interface

This section describes how to create a virtual FC interface and includes the following topics:

- [Using the FCoE Configuration Wizard, page 4-9](#)
- [Creating a Virtual Fibre Channel Interface Using Fabric Manager, page 4-13](#)
- [Creating a Virtual Fibre Channel Interface Using Device Manager, page 4-14](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Using the FCoE Configuration Wizard

To create a virtual Fibre Channel interface using the FCoE Configuration Wizard, follow these steps:

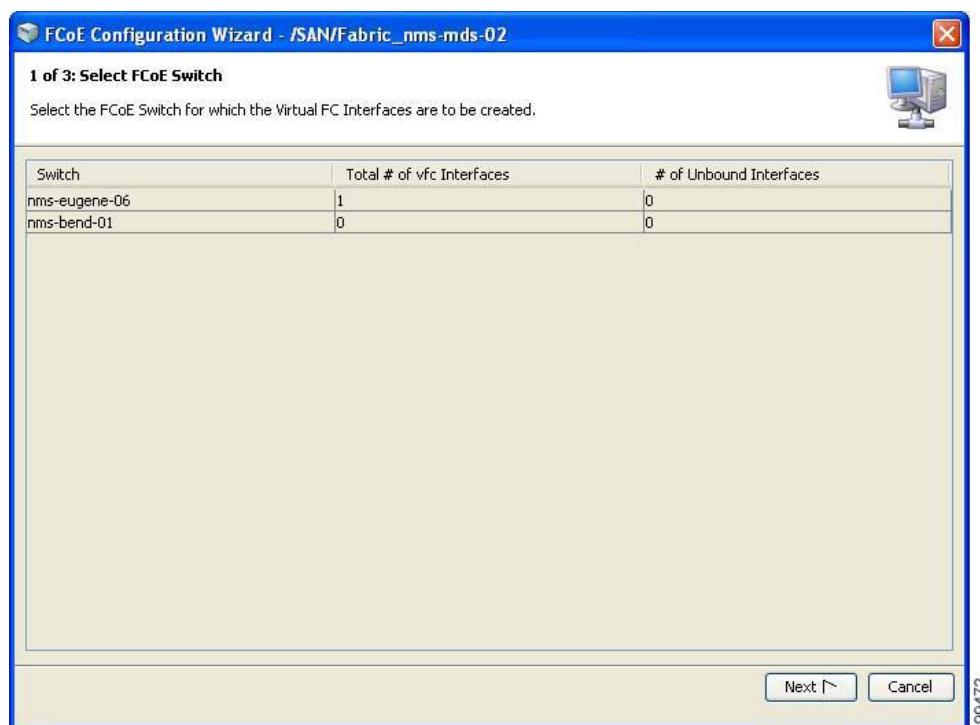
**Step 1** On the Fabric Manager toolbar, click **FCoE**, or choose **Tools > FCoE**.



**Note** The FCoE button and the Tools > FCoE menu is enabled only if the fabric includes a Cisco Nexus 5000 Series switch. A Cisco Nexus 5000 Series switch is discovered as part of the fabric only if the switch has FCoE features enabled.

You see Step 1 of the FCoE Configuration Wizard shown in [Figure 4-8](#). The wizard lists all FCoE-enabled switches in the fabric.

**Figure 4-8 FCoE Configuration Wizard - Step 1**



**Step 2** Choose a switch, and then click **Next**.

You see Step 2 of the FCoE Configuration Wizard shown in [Figure 4-9](#). The wizard shows a list of existing VLAN-VSAN mappings and the operational state of the VLAN-VSAN associations. You cannot modify an existing VLAN-VSAN mapping.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 4-9 FCoE Configuration Wizard - Step 2**

FCoE Configuration Wizard - /SAN/Fabric\_nms-mds-02

**2 of 3: Create VLAN-VSAN Mapping**

Enable FCoE on VLAN and map the VSAN to the VLAN. This step is optional if one "up" mapping already exists. (Note: Creation/Deletion of the mapping will be saved to the switch when the Next/Apply Button is clicked)

Selected Switch: **nms-bend-01**

☒ Use same VLAN Id and VSAN Id

Vlan Id	Vsan Id	Oper State
10		up
12		up
1	1	N/A

New Delete Apply Refresh

Back Next Cancel

**Step 3** Click **Next** or optionally do one of the following:



**Note**

If you choose a VLAN-VSAN mapping before clicking Next, make sure the operational state of the mapping is "up". Otherwise, an error message appears and the control remains in this step of the Wizard.

- (Optional) To delete the VLAN-VSAN mapping for the interface, choose an existing VLAN-VSAN mapping, click **Delete**, and then click **Next** to save the changes to the switch.
- (Optional) To create a new VLAN-VSAN mapping for the interface, do the following:
  - Click **New**.

A new row is added to the VLAN-VSAN mapping table.



**Note**

You must have a Cisco Nexus 5000 Series switch in the fabric to create a VLAN-VSAN mapping.

- To use the same ID for VLAN ID and VSAN ID, check the **Use same VLAN ID and VSAN ID** check box.



**Note**

The Use same VLAN ID and VSAN ID check box is checked by default.

(Optional) To automatically map a VLAN ID to a VSAN ID, you must check this check box before you create a VLAN-VSAN mapping.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Choose a VLAN ID from the drop-down list in the VLAN Id column, or type a VLAN ID in the VLAN Id field.

The VSAN ID field is automatically populated with the VLAN ID value you typed or chose in the VLAN ID field.



**Note**

If you do not check the Use same VLAN ID and VSAN ID check box, then you must choose a VSAN ID from the drop-down list in the VSAN Id column, or type a VSAN ID in the VSAN Id field.

- Click **Next** to save the changes to the switch.

You see Step 3 of the FCoE Configuration Wizard shown in [Figure 4-10](#).

**Figure 4-10 FCoE Configuration Wizard - Step 3**

**FCoE Configuration Wizard - /SAN/Fabric\_nms-mds-02**

**3 of 3: Configure Ethernet Interfaces**  
Create and Bind Virtual FC interfaces to the Ethernet interfaces/Channels. Configure the appropriate Virtual FC interfaces and Ethernet interfaces/Channels. Apply FCoE changes to the Switch.

Selected Switch: **nms-eugene-03**

☒ Show All Interfaces ☒ Auto Assign vFC Id

Interface	vFC	FCoE VLAN(VSAN)	Configure Action Status
eth1/1	<input type="checkbox"/>		
eth1/2	<input type="checkbox"/>		
eth1/3	<input type="checkbox"/>		Interface mapped to vfc1.
eth1/4	<input type="checkbox"/>		Interface mapped to vfc2.
eth1/5	<input type="checkbox"/>		
eth1/6	<input type="checkbox"/>		
eth1/7	<input type="checkbox"/>		Interface part of port-channel 2.
eth1/8	<input type="checkbox"/>		Interface part of port-channel 2.
eth1/9	<input type="checkbox"/>		Interface part of port-channel 3.
eth1/10	<input type="checkbox"/>		Interface part of port-channel 3.
eth1/11	<input type="checkbox"/>		
eth1/12	<input type="checkbox"/>		
eth1/13	<input type="checkbox"/>		
eth1/14	<input type="checkbox"/>		
eth1/15	<input type="checkbox"/>		

Refresh

Back Finish Cancel

- Step 4** Create and bind the virtual FC interface to the Ethernet interface, PortChannel, or Ethernet host interface of a Cisco Nexus 2000 Series Fabric Extender.



**Note**

You cannot bind virtual FC interfaces to Ethernet interfaces that are part of Ethernet PortChannels. The vFC column is disabled for all such interfaces; for example, eth1/7 to eth1/10.

You can do one of the following:

- To automatically bind a virtual FC interface to a specific Ethernet interface and assign the virtual FC ID to the interface, check the **Auto Assign vFC ID** check box, and then, for an Ethernet interface, check the relevant check box in the vFC column. To bind all Ethernet interfaces, check the **vFC** check box (located at the top of the vFC column).



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- To manually bind a virtual FC interface to a specific Ethernet interface and assign the virtual FC ID to the interface, uncheck the **Auto Assign vFC ID** check box. A vFC ID column appears (see [Figure 4-11](#)). In the vFC column, check the check box for the relevant Ethernet interface, and then type a virtual FC ID in the vFC ID field provided in the vFC ID column. To bind all Ethernet interfaces, check the **vFC** check box, and then type the virtual FC IDs in the vFC ID field for each Ethernet interface.

**Figure 4-11 FCoE Configuration Wizard - Step 3 (vFC ID, Show All Interfaces)**

Interface	vFC	vFC ID	FCoE VLAN(VSAN)	Configure Action Status
eth1/1	<input type="checkbox"/>			
eth1/2	<input type="checkbox"/>			
eth1/3	<input type="checkbox"/>			
eth1/4	<input type="checkbox"/>			Interface mapped to vfc1.
eth1/5	<input checked="" type="checkbox"/>	6	9(9)	Interface mapped to vfc2.
eth1/6	<input type="checkbox"/>			
eth1/7	<input type="checkbox"/>			Interface part of port-channel 2.
eth1/8	<input type="checkbox"/>			Interface part of port-channel 2.
eth1/9	<input type="checkbox"/>			Interface part of port-channel 3.
eth1/10	<input type="checkbox"/>			Interface part of port-channel 3.
eth1/11	<input type="checkbox"/>			
eth1/12	<input type="checkbox"/>			
eth1/13	<input type="checkbox"/>			
eth1/14	<input type="checkbox"/>			
eth1/15	<input type="checkbox"/>			



**Note**

Ethernet host interfaces of a Cisco Nexus N2224TP Series Fabric Extender, Cisco Nexus N2232TP Series Fabric Extender, or Cisco Nexus N2232TT Series Fabric Extender are not listed in this step of the wizard.

To view these interfaces, you must check the **Show All Interfaces** check box (see [Figure 4-11](#)). The Configure Action Status field displays the “Not FCoE Capable” status message for these interfaces. However, you cannot bind a virtual FC interface to any of these Ethernet interfaces.

The following guidelines define valid interfaces to which you can bind the virtual FC interface:

- The Ethernet interface must not have any virtual interface associated with it.
- The Ethernet PortChannel interface must contain only a single 10-Gigabit Ethernet interface.
- The Ethernet interface must not be connected to a Cisco Nexus 2000 Series Fabric Extender uplink port.
- The Ethernet interface must be a 10-Gigabit Ethernet interface.
- The Ethernet interface must not be in switchport monitor mode.



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 5** Click **Finish** to commit and distribute the change.

## Creating a Virtual Fibre Channel Interface Using Fabric Manager

To create a virtual FC interface using Fabric Manager, follow these steps:

**Step 1** In the Physical Attributes pane, expand **Switches > Interfaces**, and then choose **VFC (FCoE)**.

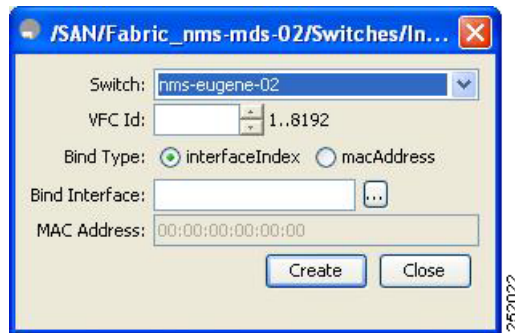


**Note** Cisco Fabric Manager 4.1(2) and later releases do not support the configuration of a virtual FC interface on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to Release 4.0(1a). Fabric Manager issues an error message if you try to configure a virtual FC interface on a Cisco Nexus 5000 Series switch that runs a Cisco NX-OS release prior to Release 4.0(1a).

**Step 2** In the Information pane toolbar, click the **Create Row** icon.

You see the Create Virtual Interface dialog box shown in [Figure 4-12](#).

**Figure 4-12** Create Virtual Interface Dialog Box



**Step 3** From the Switch drop-down list, choose the switch where the virtual FC interface will be created.

Fabric Manager preselects the next available virtual FC interface ID. Optionally, in the VFC ID field, enter a value for this ID as an integer from 1 to 8192.

**Step 4** (Optional) To bind the virtual FC interface to an Ethernet interface or an Ethernet PortChannel, do the following:

- a. Ensure that the interfaceIndex radio button is selected. The interfaceIndex radio button is selected by default.
- b. Click the button located next to the Bind Interface field, and choose the physical Ethernet interface or Ethernet PortChannel number that will be bound to this virtual FC interface. Optionally, you can enter a value for the Ethernet interface or Ethernet PortChannel in the Bind Interface field.



**Note** The interface port selector dialog box (see [Figure 4-14 on page 4-15](#)) does not display the Ethernet host interfaces of a Cisco Nexus N2224TP Series Fabric Extender, Cisco Nexus N2232TP Series Fabric Extender, or Cisco Nexus N2232TT Series Fabric Extender.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

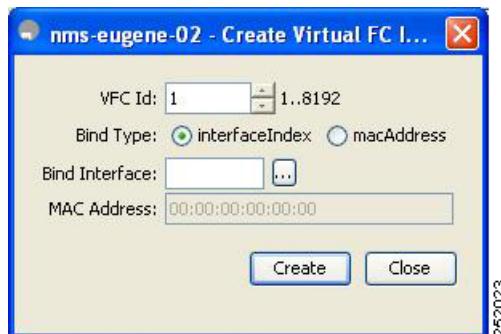
- Step 5** (Optional) To bind the virtual FC interface to the MAC address of the ENode or the remote FCF, do the following:
- Click the **macAddress** radio button.
  - In the MAC Address field, enter the MAC address of the ENode or the remote FCF identified by the virtual FC interface. For example, 00:15:60:0F:C1:D0.
- Step 6** Click **Create**.
- Step 7** (Optional) Repeat Step 3 through Step 6 to create additional virtual FC interfaces for the same switch or a different switch.
- Step 8** In the Create Virtual Interface dialog box, click **Close** when done.
- The FC Virtual information pane lists the new and existing virtual FC interfaces for the switch.

## Creating a Virtual Fibre Channel Interface Using Device Manager

To create a virtual FC interface using Device Manager, follow these steps:

- Step 1** Launch Device Manager from the Cisco Nexus 5000 Series switch.
- Step 2** Choose **Interface > Virtual Interfaces > Fibre Channel**.
- You see the Virtual FC Interfaces dialog box (see [Figure 4-2](#)).
- The General tab displays the description, bind type, bound Ethernet interface or PortChannel, bound MAC address, FCF priority value, VSAN port, and status for each virtual FC interface.
- Step 3** Click **Create**.
- You see the Create Virtual FC Interfaces General dialog box shown in [Figure 4-13](#).

**Figure 4-13 Create Virtual FC Interfaces Dialog Box**



- Step 4** In the VFC Id field, enter the virtual FC interface ID as an integer from 1 to 8192. The VFC Id field increments by 1.
- Step 5** (Optional) To bind the virtual FC interface to an Ethernet interface or an Ethernet PortChannel or an Ethernet host interface on a Cisco Nexus 2000 Series Fabric Extender, do the following:
- Ensure that the **interfaceIndex** radio button is selected. The **interfaceIndex** radio button is selected by default.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- b. Click the button located next to the Bind Interface field. In the interface selector dialog box that appears (see [Figure 4-14](#)), choose the physical Ethernet interface, Ethernet PortChannel, or Ethernet host interface on a Cisco Nexus 2000 Series Fabric Extender to bind to the virtual FC interface. Optionally, you can enter a value for the Ethernet interface, Ethernet PortChannel, or Ethernet host interface in the Bind Interface field.

**Figure 4-14 Interface Port Selector Dialog Box**



**Note**

You cannot bind a virtual FC interface to an Ethernet interface that runs at 1-Gigabit Ethernet speed or is connected to a port connecting the Cisco Nexus 5000 Series switch to a Cisco Nexus 2000 Series Fabric Extender.

The interface port selector dialog box (see [Figure 4-14](#)) does not display the Ethernet host interfaces of a Cisco Nexus N2224TP Series Fabric Extender, Cisco Nexus N2232TP Series Fabric Extender, or Cisco Nexus N2232TT Series Fabric Extender.

- Step 6** (Optional) To bind the virtual FC interface to the MAC address of the ENode or the remote FCF, do the following:
  - a. Click the **macAddress** radio button.
  - b. In the MAC Address field, enter the MAC address of the ENode or the remote FCF identified by the virtual FC interface. For example, 00:15:60:0F:C1:D0.
- Step 7** Click **Create**.  
You see the virtual FC interface in the Virtual FC Interfaces dialog box.
- Step 8** (Optional) Repeat Step 4 through Step 7 to create additional virtual FC interfaces.
- Step 9** In the Create Virtual FC Interfaces General dialog box, click **Close** when done.  
The Virtual FC Interfaces dialog box lists the new and existing virtual FC interfaces for the switch.

## Deleting a Virtual Fibre Channel Interface

You can delete a virtual FC interface using Fabric Manager or Device Manager.

To delete a virtual FC interface, follow these steps:

- Step 1** Do one of the following:

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- In Fabric Manager, in the Physical Attributes pane, expand **Switches > Interfaces**, and then choose **VFC (FCoE)**.

You see the Virtual Fibre Channel table in the Information pane.

- Launch Device Manager from the Cisco Nexus 5000 Series switch, and then choose **Interface > Virtual Interfaces > Fibre Channel**.

You see the Virtual FC Interfaces dialog box.

**Step 2** Choose a virtual FC interface that you want to delete.

**Step 3** Do one of the following:

- In Fabric Manager, in the Information pane toolbar, click the **Delete Row** icon.
- In Device Manager, in the Virtual FC Interfaces dialog box, click **Delete**.

In the confirmation dialog box that appears, confirm the deletion of the virtual FC interface.

## Default Settings

Table 4-1 lists the default settings for all virtual FC interfaces.

**Table 4-1 Default Virtual Fibre Channel Interface Parameters**

Parameters	Default
VSAN ID Port	1
Mode Admin	F
Mode Oper	Auto
Status Service	In
Status Admin	Down



## CHAPTER 5

# Configuring Fibre Channel Interfaces

---

Cisco MDS 9000 Family hardware modules and switches are categorized into generations based on the time of introduction, capabilities, features, and compatibilities:

- Generation 1—Modules and switches with a maximum port speed of 2 Gbps.
- Generation 2—Modules and switches with a maximum port speed of 4 Gbps.
- Generation 3—Modules and switches with a maximum port speed of 8 Gbps.

This chapter describes how to configure these Fibre Channel interfaces, including the following sections:

- [About Generations of Modules and Switches, page 5-1](#)
- [Port Groups and Port Rate Modes, page 5-3](#)
- [Combining Generation 1, Generation 2, and Generation 3 Modules, page 5-10](#)
- [Configuring Module Interface Shared Resources, page 5-14](#)
- [Configuring Port Speed, page 5-18](#)
- [Configuring Rate Mode, page 5-19](#)
- [Configuring Oversubscription Ratio Restrictions, page 5-20](#)
- [Configuring Bandwidth Fairness, page 5-24](#)
- [Taking Interfaces Out of Service, page 5-26](#)
- [Releasing Shared Resources in a Port Group, page 5-27](#)
- [Displaying SFP Diagnostic Information, page 5-28](#)
- [Default Settings, page 5-30](#)

## About Generations of Modules and Switches

The Cisco MDS 9500 Series switches, Cisco MDS 9222i, Cisco MDS 9216A and Cisco MDS 9216i switches support a set of modules called the Generation 2 modules. Each module or switch can have one or more ports in port groups that share common resources such as bandwidth and buffer credits.

In addition to supporting Generation 2 modules, the Cisco MDS 9500 Series switches and the Cisco MDS 9222i switch support another set of modules called Generation 3 modules. Similar to Generation 2, each Generation 3 module can have one or more ports in port groups that share common resources such as bandwidth and buffer credits.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

Generation 3 Fibre Channel modules are supported on the Cisco MDS 9506 and 9509 switches with Supervisor-2 modules. The MDS 9513 Director supports 4/44-port Host-Optimized Fibre Channel switching module with either Fabric 1 or Fabric 2 modules, but requires Fabric 2 module for support of the 48-port and the 24-port 8-Gbps Fibre Channel switching modules. The MDS 9222i switch supports the 4/44-port Host-Optimized Fibre Channel switching module. MDS NX-OS Release 4.1(1) is required to support the Generation 3 modules.

Table 5-1 identifies the Generation 2 and Generation 3 modules, as well as the Fabric switches.

**Table 5-1 Fibre Channel Modules and Fabric Switches**

Part Number	Product Name/Description
<b>Generation 3 Modules</b>	
DS-X9248-96K9	48-port 8-Gbps Fibre Channel switching module
DS-X9224-96K9	24-port 8-Gbps Fibre Channel switching module
DS-X9248-48K9	4/44-port 8-Gbps Host-Optimized Fibre Channel switching module
DS-13SLT-FAB2	Fabric 2 module that enables the 24-port and the 48-port 8-Gbps Fibre Channel switching module to use the full 96-Gbps backplane bandwidth with any-to-any connectivity.
<b>Generation 3 Fabric Switches</b>	
DS-C9148-K9	Cisco MDS 9148 Fabric switch 48-port 8-Gbps Fabric switch
<b>Generation 2 Modules</b>	
DS-X9148	48-port 4-Gbps Fibre Channel switching module
DS-X9124	24-port 4-Gbps Fibre Channel switching module
DS-X9304-18K9	18-port 4-Gbps Fibre Channel switching module with 4-Gigabit Ethernet ports
DS-X9112	12-port 4-Gbps Fibre Channel switching module
DS-X9704	4-port 10-Gbps Fibre Channel switching module
DS-X9530-SF2-K9	Supervisor-2 module for Cisco MDS 9500 Series switches.
<b>Generation 2 Fabric Switches</b>	
DS-C9134-K9	Cisco MDS 9134 Fabric switch 32-port 4-Gbps Fabric switch with 2 additional 10-Gbps ports
DS-C9124	Cisco MDS 9124 Fabric switch 24-port 4-Gbps Fabric switch
DS-C9222i-K9	Cisco MDS 9222i Multiservice Modular switch 18-port 4-Gbps switch with 4-Gigabit Ethernet IP storage services ports, and a modular expansion slot to host Cisco MDS 9000 Family switching and services modules



**Note**

Generation 2 Fibre Channel switching modules are not supported on the Cisco MDS 9216 switch; however, they are supported by both the Supervisor-1 module and the Supervisor-2 module.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

For detailed information about the installation and specifications for these modules and switches, refer to the hardware installation guide for your switch.

## Port Groups and Port Rate Modes

This section includes the following topics:

- [Port Groups, page 5-3](#)
- [Port Rate Modes, page 5-4](#)
- [Dedicated Rate Mode Configurations for the 8-Gbps Modules, page 5-7](#)
- [Reserving Bandwidth Quickly for the 8-Gbps Modules, page 5-8](#)
- [Dynamic Bandwidth Management, page 5-9](#)
- [Out-of-Service Interfaces, page 5-10](#)

## Port Groups

Each module or switch can have one or more ports in port groups that share common resources such as bandwidth and buffer credits. Port groups are defined by the hardware consisting of sequential ports. For example, ports 1 through 12, ports 13 through 24, ports 25 through 36, and ports 37 through 48 are the port groups on the 48-port 4-Gbps Fibre Channel switching modules.

[Table 5-6](#) shows the port groups for the Generation 2 and Generation 3 Fibre Channel modules, and Generation 2 and Generation 3 Fabric switches.

**Table 5-2 Bandwidth and Port Groups for the Fibre Channel Modules and Fabric Switches**

Part Number	Product Name/ Description	Number of Ports Per Port Group	Bandwidth Per Port Group (Gbps)	Maximum Bandwidth Per Port (Gbps)
<b>Generation 3 Modules</b>				
DS-X9248-96K9	48-port 8-Gbps Fibre Channel switching module	6	12.8	8 Gbps
DS-X9224-96K9	24-port 8-Gbps Fibre Channel switching module	3	12.8	8 Gbps
DS-X9248-48K9	4/44-port 8-Gbps Host-Optimized Fibre Channel switching module	12	12.8	8/4 Gbps <sup>1</sup>
<b>Generation 3 Fabric Switches</b>				
DS-C9148-K9 (Cisco MDS 9148 Fabric switch)	48-port 8-Gbps Fabric switch	4	32	8 Gbps
<b>Generation 2 Modules</b>				

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Table 5-2 Bandwidth and Port Groups for the Fibre Channel Modules and Fabric Switches**

Part Number	Product Name/ Description	Number of Ports Per Port Group	Bandwidth Per Port Group (Gbps)	Maximum Bandwidth Per Port (Gbps)
DS-X9148	48-port 4-Gbps Fibre Channel switching module	12	12.8	4 Gbps
DS-X9124	24-port 4-Gbps Fibre Channel switching module	6	12.8	4 Gbps
DS-X9304-18K9 (MSM-18/4 Multiservice module)	18-port 4-Gbps Fibre Channel switching module with 4-Gigabit Ethernet ports	6	12.8	4 Gbps
DS-X9112	12-port 4-Gbps Fibre Channel switching module	3	12.8	4 Gbps
DS-X9704	4-port 10-Gbps Fibre Channel switching module	1	10	10 Gbps
<b>Generation 2 Fabric Switches</b>				
DS-C9134-K9 (Cisco MDS 9134 Fabric switch)	32-port 4-Gbps Fabric switch	4	16	4 Gbps
	2-port 10-Gbps Fabric switch	1	10	10 Gbps
DS-C9124K9 (Cisco MDS 9124 Fabric switch)	24-port 4-Gbps Fabric switch	4	16	4 Gbps
DS-C9222i-K9 (Cisco MDS 9222i Multiservice Modular switch)	18-port 4-Gbps, 4 Gigabit Ethernet ports and a modular expansion slot.	6	12.8	4 Gbps

1. A maximum of 4 ports (one per port group) in a 4/44-port 8-Gbps switching module can operate at 8 Gbps bandwidth in dedicated or shared mode. All the other ports can operate at a maximum of 4 Gbps in shared mode or dedicated mode.

## Port Rate Modes

In Generation 2 and Generation 3 modules, you can configure the port rate modes. The *port rate mode* configuration is used to determine the bandwidth allocation for ports in a port group. Two port rate modes are supported:

- **Dedicated Rate Mode**—A port is allocated required fabric bandwidth to sustain line traffic at the maximum operating speed configured on the port. For more information, see the [“Dedicated Rate Mode” section on page 5-6](#).
- **Shared Rate Mode**—Multiple ports in a port group share data paths to the switch fabric and share bandwidth. For more information, see the [“Shared Rate Mode” section on page 5-7](#).



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Note**

In Generation 1 modules, you cannot configure the port rate modes. The mode is determined implicitly based on the port mode and line card type.

**Note**

Port rate modes are not supported on the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

Table 5-3 shows the modules that support dedicated, shared, and the default rate modes.

**Table 5-3 Port Rate Mode Support on Generation 2 and Generation 3 Modules and Switches**

Part Number	Product Name/ Description	Supports Dedicated Rate Mode	Supports Shared Rate Mode	Default Speed Mode and Rate Mode on All Ports
<b>Generation 3 Modules</b>				
DS-X9248-96K9	48-Port 8-Gbps Fibre Channel switching module	Yes	Yes <sup>1</sup>	Auto, Shared
DS-X9224-96K9	24-Port 8-Gbps Fibre Channel switching module	Yes	Yes <sup>1</sup>	Auto, Shared
DS-X9248-48K9	4/44-Port 8-Gbps Host-Optimized Fibre Channel switching module	Yes	Yes <sup>1</sup>	Auto Max 4 Gbps, Shared
<b>Generation 3 Fabric Switches</b>				
DS-C9148-K9 (Cisco MDS 9148 Fabric switch)	48-port 8-Gbps Fabric switch	Yes	No	Auto, Dedicated
<b>Generation 2 Modules</b>				
DS-X9148	48-port 4-Gbps Fibre Channel switching module <sup>2</sup>	Yes	Yes	Auto, Shared
DS-X9124	24-port 4-Gbps Fibre Channel switching module	Yes	Yes	Auto, Shared
DS-X9304-18K9 (MSM-18/4 Multiservice module)	18-port 4-Gbps Fibre Channel switching module with 4-Gigabit Ethernet ports	Yes	Yes	Auto, Shared
DS-X9112	12-port 4-Gbps Fibre Channel switching module	Yes	No	Auto, Dedicated
DS-X9704	4-port 10-Gbps Fibre Channel switching module	Yes	No	Auto, Dedicated
<b>Generation 2 Fabric Switches</b>				
DS-C9134-K9 (Cisco MDS 9134 Fabric switch)	32-port 4-Gbps Fabric switch	Yes	Yes	Auto, Shared
	2-port 10-Gbps Fabric switch	Yes	No	Auto, Dedicated

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 5-3 Port Rate Mode Support on Generation 2 and Generation 3 Modules and Switches**

Part Number	Product Name/ Description	Supports Dedicated Rate Mode	Supports Shared Rate Mode	Default Speed Mode and Rate Mode on All Ports
DS-C9124 (Cisco MDS 9124 Fabric switch)	24-port 4-Gbps Fabric switch <sup>3</sup>	Yes	No	Auto, Dedicated
DS-C9222i-K9 (Cisco MDS 9222i Multiservice Modular switch)	18-port 4-Gbps Fibre Channel switch with 4-Gigabit Ethernet IP storage services ports, and a modular expansion slot to host Cisco MDS 9000 Family Switching and Services Modules	Yes	Yes	Auto, Shared

1. Shared rate mode is supported on Fx ports only and no ISLs.
2. All ports in a 48-port 4-Gbps switching module can operate in dedicated rate mode with a 1-Gbps operating speed. However, if you configure one or more ports to operate in 2-Gbps or 4-Gbps dedicated rate mode, some of the other ports in the port group would have to operate in shared mode.
3. All ports in a 24-port 4-Gbps switching module can operate in dedicated rate mode with a 2-Gbps operating speed. However, if you configure one or more ports to operate in 4-Gbps dedicated rate mode, some of the other ports in the port group would have to operate in shared mode.

## Dedicated Rate Mode

When port rate mode is configured as dedicated, a port is allocated required fabric bandwidth and related resources to sustain line rate traffic at the maximum operating speed configured for the port. In this mode, ports do not use local buffering and all receive buffers are allocated from a global buffer pool (see the “[Buffer Pools](#)” section on page 6-3).

Table 5-4 shows the bandwidth provided by the various port speed configurations on the 8-Gbps Fibre Channel switching modules.

**Table 5-4 Bandwidth Reserved for the Port Speeds on Generation 3 Switching Modules**

Configured Speed	Reserved Bandwidth
Auto	8 Gbps
8-Gbps	
Auto with 4-Gbps maximum	4 Gbps
4-Gbps	
Auto with 2-Gbps maximum	2 Gbps
2-Gbps	
1-Gbps	1 Gbps

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Table 5-5 shows the amount of bandwidth reserved for a configured port speed on 4-Gbps switching modules.

**Table 5-5 Bandwidth Reserved for the Port Speeds on Generation 2 Switching Modules**

Configured Speed	Reserved Bandwidth
Auto	4 Gbps
4-Gbps	
Auto with 2-Gbps maximum	2 Gbps
2-Gbps	
1-Gbps	1 Gbps



**Note**

The 4-Port 10-Gbps Fibre Channel module ports in auto mode only support auto speed mode at 10 Gbps.

## Shared Rate Mode

When port rate mode is configured as shared, multiple ports within a port group share data paths to the switch fabric so that fabric bandwidth and related resources are shared. Often, the available bandwidth to the switch fabric may be less than the negotiated operating speed of a port. Ports in this mode use local buffering for the BB\_credit buffers.

All ports in 4-Gbps Fibre Channel switching modules where bandwidth is shared support 1-Gbps, 2-Gbps, or 4-Gbps traffic. However, it is possible to configure one or more ports in a port group to operate in dedicated rate mode with 1-Gbps, 2-Gbps or 4-Gbps operating speed.

All ports in the 48-Port and 24-Port 8-Gbps Fibre Channel switching modules where bandwidth is shared support 1-Gbps, 2-Gbps, 4-Gbps, or 8-Gbps traffic.

In the 4/44-Port 8-Gbps Host-Optimized Fibre Channel switching module, all the ports where bandwidth is shared support 1-Gbps, 2-Gbps, 4-Gbps in a maximum of 44 ports, or 8 Gbps in a maximum of 4 ports.

## Dedicated Rate Mode Configurations for the 8-Gbps Modules

Table 5-6 shows the maximum possible dedicated rate mode configuration scenarios for the Generation 3 Fibre Channel modules.

**Table 5-6 Dedicated Rate Mode Bandwidth Reservation for Generation 3 Fibre Channel Modules**

Part Number	Product Name/Description	Dedicated Bandwidth per Port	Maximum Allowed Ports that can come up	Ports in Shared Mode
DS-X9248-96K9	48-port 8-Gbps Fibre Channel switching module	8 Gbps	8 Ports	All the remaining ports are 8 Gbps shared.
		4 Gbps	24 Ports	
		2 Gbps	48 Ports	
DS-X9224-96K9	24-port 8-Gbps Fibre Channel switching module	8 Gbps	8 Ports	All the remaining ports are 8 Gbps shared.
		4 Gbps	24 Ports	

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Table 5-6 Dedicated Rate Mode Bandwidth Reservation for Generation 3 Fibre Channel Modules (continued)**

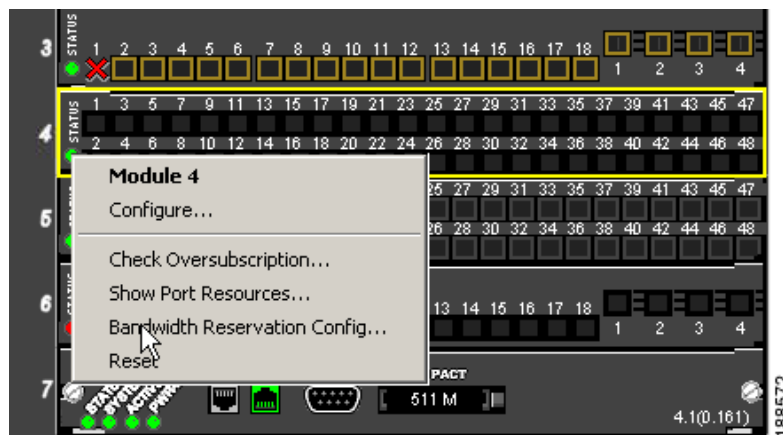
Part Number	Product Name/ Description	Dedicated Bandwidth per Port	Maximum Allowed Ports that can come up	Ports in Shared Mode
DS-X9248-48K9	4/44-port 8-Gbps Host-Optimized Fibre Channel switching module	8 Gbps	4 Ports	All the remaining ports are 4 Gbps shared (8 Gbps of bandwidth can be provided only to one port per port group in Dedicated or Shared rate mode).
		4 Gbps	12 Ports	
		2 Gbps	24 Ports	
		1 Gbps	48 Ports	

## Reserving Bandwidth Quickly for the 8-Gbps Modules

To quickly reserve bandwidth for all the ports in the port groups on the Generation 3 Fibre Channel modules using the Device Manager, follow these steps:

- Step 1** On the Device Manager window, right-click the 8-Gbps Fibre Channel module.

**Figure 5-1 Device Manager - 8 Gbps Module - Pop-Up Menu**



- Step 2** From the pop up menu, select **Bandwidth Reservation Config...**

- Step 3** In the Bandwidth Reservation Configuration dialog box that is displayed, choose a bandwidth reservation scheme. (Figure 5-2).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 5-2 RateMode Configuration Dialog Box**



Table 5-7 describes the default RateMode configuration schemes available in the Bandwidth Reservation Configuration dialog box for the 8-Gbps modules.

**Table 5-7 RateMode Configuration Schemes**

Module	Available RateMode Config Macros
DS-X9248-96K9 48-Port 8-Gbps Fibre Channel module	<ul style="list-style-type: none"> <li>Dedicated 4 Gbps on the first port of each group and the remaining ports 8 Gbps shared</li> <li>Dedicated 8 Gbps on the first port of each group and the remaining ports 8 Gbps shared</li> <li>Shared 8 Gbps on all ports (initial &amp; default settings)</li> </ul>
DS-X9224-96K9 24-Port 8-Gbps Fibre Channel module	<ul style="list-style-type: none"> <li>Dedicated 8 Gbps on the first port of each group and the remaining ports 8G shared</li> <li>Shared Auto<sup>1</sup> on all ports (initial &amp; default settings)</li> </ul>
DS-X9248-48K9 4/44-Port 8-Gbps Host-Optimized Fibre Channel module	<ul style="list-style-type: none"> <li>Dedicated 2 Gbps on the first port of each group and the remaining ports 4 Gbps shared</li> <li>Dedicated 8 Gbps on the first port of each group and the remaining ports 4 Gbps shared</li> <li>Shared Auto with Maximumu of 4 Gbps on all ports (initial &amp; default settings)</li> </ul>

1. Auto is 8 Gbps.

**Step 4** Click **Apply**.

## Dynamic Bandwidth Management

On port switching modules where bandwidth is shared, the bandwidth available to each port within a port group can be configured based on the port rate mode and speed configurations. Within a port group, some ports can be configured in dedicated rate mode while others operate in shared mode.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Ports configured in dedicated rate mode are allocated the required bandwidth to sustain a line rate of traffic at the maximum configured operating speed, and ports configured in shared mode share the available remaining bandwidth within the port group. Bandwidth allocation among the shared mode ports is based on the operational speed of the ports. For example, if four ports operating at speeds 1 Gbps, 1 Gbps, 2 Gbps, and 4 Gbps share bandwidth of 8 Gbps, the ratio of allocation would be 1:1:2:4.

Unutilized bandwidth from the dedicated ports is shared among only the shared ports in a port group as per the ratio of the configured operating speed. A port cannot be brought up unless the reserved bandwidth is guaranteed for the shared ports (see [Table 5-10](#)). For dedicated ports, configured bandwidth is taken into consideration while calculating available bandwidth for the port group. This behavior can be changed using bandwidth fairness by using the **rate-mode bandwidth-fairness module number** command.

For example, consider a 48-port 8-Gbps module. This module has 6 ports per port group with 12.8 Gbps bandwidth. Ports three to six are configured at 4 Gbps. If the first port is configured at 8 Gbps dedicated rate mode, and the second port is configured at 4-Gbps dedicated rate mode, then no other ports can be configured at 4 Gbps or 8 Gbps because the left over bandwidth of 0.8 Gbps (12.8-(8+4)) cannot meet the required 0.96 Gbps for the remaining four ports. A minimum of 0.24 Gbps reserved bandwidth is required for the for the rest of the four ports. However, if the two ports (for example, 5 and 6) are taken out of service (note that it is not same as shut-down), required reserved bandwidth for the two ports (3 and 4) is 0.48 and port 2 can be configured at 4 Gbps in dedicated rate mode. Note this behavior can be overridden by bandwidth fairness command in which case reserved bandwidth is not enforced. Once the port is up, ports 3 and 4 can share the unutilized bandwidth from ports 1 and 2.

## Out-of-Service Interfaces

On supported modules and fabric switches, you might need to allocate all the shared resources for one or more interfaces to another interface in the port group or module. You can take interfaces out of service to release shared resources that are needed for dedicated bandwidth. When an interface is taken out of service, all shared resources are released and made available to the other interface in the port group or module. These shared resources include bandwidth for the shared mode port, rate mode, BB\_credits, and extended BB\_credits. All shared resource configurations are returned to their default values when the interface is brought back into service. Corresponding resources must be made available in order for the port to be successfully returned to service.



**Caution**

If you need to bring an interface back into service, you might disrupt traffic if you need to release shared resources from other interfaces in the same port group.

## Combining Generation 1, Generation 2, and Generation 3 Modules

Cisco MDS NX-OS Release 4.1(1) and later supports combining Generation 1, Generation 2, and Generation 3 modules and switches with the following considerations:

- MDS NX-OS Release 4.1(1) and later features are not supported on Generation 1 switches and modules.
- Generation 3 modules do not support the following Generation 1 hardware:
  - Supervisor 1 module

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- 4-Port IP Storage Services module
- 8-Port IP Storage Services module
- MDS 9216 Switch
- MDS 9216A switch
- MDS 9020 switch
- MDS 9120 switch
- MDS 9140 switch
- Supervisor-1 modules must be upgraded to Supervisor-2 modules on the MDS 9506 and MDS 9509 Directors.
- IPS-4 and IPS-8 modules must be upgraded to the MSM-18/4 Multiservice modules.
- Fabric 1 modules must be upgraded to Fabric 2 modules on the MDS 9513 Director to use the 48-port or the 24-port 8-Gbps module.
- MDS Fabric Manager Release 4.x supports MDS SAN-OS Release 3.x and NX-OS 4.x in mixed mode through Interswitch Link (ISL) connectivity.

**Note**

When a Cisco or another vendor switch port is connected to a Generation 1 module port (ISL connection), the receive buffer-to-buffer credits of the port connected to the Generation 1 module port should not exceed 255.

## Port Indexes

Cisco MDS 9000 switches allocate index identifiers for the ports on the modules. These port indexes cannot be configured. You can combine Generation 1, Generation 2, and Generation 3 switching modules, with either Supervisor-1 modules or Supervisor-2 modules. However, combining switching modules and supervisor modules has the following port index limitations:

- Supervisor-1 modules only support a maximum of 252 port indexes, regardless of the type of switching modules.
- Supervisor-2 modules support a maximum of 1020 port indexes when all switching modules in the chassis are Generation 2 or Generation 3.
- Supervisor-2 modules only support a maximum of 252 port indexes when only Generation 1 switching modules, or a combination of Generation 1, Generation 2, or Generation 3 switching modules, are installed in the chassis.

**Note**

On a switch with the maximum limit of 252 port index maximum limit, any new module that exceeds the limit when installed does not power up.

Generation 1 switching modules have specific numbering requirements. If these requirements are not met, the module does not power up. The port index numbering requirements include the following:

- If port indexes in the range of 256 to 1020 are assigned to operational ports, Generation 1 switching modules do not power up.
- A block of contiguous port indexes is available. If this block of port indexes is not available, Generation 1 modules do not power up. [Table 5-8](#) shows the port index requirements for the Generation 1 modules.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Note**

If the switch has Supervisor-1 modules, the block of 32 contiguous port indexes must begin on the slot boundary. The slot boundary for slot 1 is 0, for slot 2 is 32, and so on. For Supervisor-2 modules, the contiguous block can start anywhere.

**Table 5-8 Port Index Requirements for Generation 1 Modules**

Generation 1 Module	Number of Port Indexes Required	
	Supervisor-1 Module	Supervisor-2 Module
16-port 2-Gbps Fibre Channel module	16	16
32-port 2-Gbps Fibre Channel module	32	32
8-port Gigabit Ethernet IP Storage Services module	32	32
4-port Gigabit Ethernet IP Storage Services module	32	16
32-port 2-Gbps Fibre Channel Storage Services Module (SSM).	32	32
14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module	32	22

The allowed mix of Generation 1 and Generation 2 switching modules in a chassis is determined at run-time, either when booting up the switch or when installing the modules. In some cases, the sequence in which switching modules are inserted into the chassis determines if one or more modules is powered up.

When a module does not power up because of a resource limitation, you can see the reason by viewing the module information in the Information pane.

For information on recovering a module powered-down because port indexes are not available, refer to the *Cisco MDS 9000 Family Troubleshooting Guide*.

**Tip**

Whenever using mixed Generation 1 and Generation 2 modules, power up the Generation 1 modules first. During a reboot of the entire switch, the Generation 1 modules power up first (default behavior).

## PortChannels

PortChannels have the following restrictions:

- The maximum number of PortChannels allowed is 256 if all switching modules are Generation 2 or Generation 3, or both.
- The maximum number of PortChannels allowed is 128 whenever there is a Generation 1 switching module in use with a Generation 2 or Generation 3 switching module.
- Ports need to be configured in dedicated rate mode on the Generation 2 and Generation 3 switching module interfaces to be used in the PortChannel.

**Note**

The number of PortChannels allowed does not depend on the type of supervisor module. However, Generation 3 modules require the Supervisor 2 module on the MDS 9506 and 9509 switches.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

The Generation 1, Generation 2, and Generation 3 modules have the following restrictions for PortChannel configuration:

- Generation 1 switching module interfaces do not support auto speed with a maximum of 2 Gbps.
- Generation 1 and Generation 2 module interfaces do not support auto speed with maximum of 4 Gbps.
- Generation 2 and Generation 3 switching module interfaces cannot be forcefully added to a PortChannel if sufficient resources are not available.

When configuring PortChannels on switches with Generation 1, Generation 2, and Generation 3 switching modules, follow one of these procedures:

- Configure the PortChannel, and then configure the Generation 2 and Generation 3 interfaces to auto with a maximum of 2 Gbps.
- Configure the Generation 1 switching modules followed by the Generation 2 switching modules, and then the Generation 3 switching modules, and then configure the PortChannel.

When configuring PortChannels on switches with only Generation 2 and Generation 3 switching modules, follow one of these procedures:

- Configure the PortChannel, and then configure the Generation 3 interfaces to auto with a maximum of 4 Gbps.
- Configure the Generation 2 switching modules, followed by the Generation 3 switching modules, and then configure the PortChannel.

Table 5-9 describes the results of adding a member to a PortChannel for various configurations.

**Table 5-9 PortChannel Configuration and Addition Results**

PortChannel Members	Configured Speed		New Member Type	Addition Type	Result
	PortChannel	New Member			
No members	Any	Any	Generation 1 or Generation 2 or Generation 3	Force	Pass
	Auto	Auto	Generation 1 or Generation 2 or Generation 3	Normal or force	Pass
	Auto	Auto max 2000	Generation 2 or Generation 3	Normal	Fail
				Force	Pass or fail <sup>1</sup>
	Auto	Auto max 4000	Generation 3		
	Auto max 2000	Auto	Generation 2 or Generation 3	Normal	Fail
				Force	Pass
	Auto max 2000	Auto max 4000	Generation 3		
	Auto max 4000	Auto	Generation 2 or Generation 3		
	Auto max 4000	Auto max 2000	Generation 2 or Generation 3		

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 5-9 PortChannel Configuration and Addition Results (continued)**

PortChannel Members	Configured Speed		New Member Type	Addition Type	Result
	PortChannel	New Member			
Generation 1 interfaces	Auto	Auto	Generation 2 or Generation 3	Normal	Fail
				Force	Pass
	Auto max 2000	Auto	Generation 1	Normal or force	Pass
	Auto max 2000	Auto	Generation 2 or Generation 3	Normal	Fail
				Force	Pass or fail <sup>1</sup>
	Auto max 4000	Auto	Generation 1 or Generation 2		
Generation 2 interfaces	Auto	Auto	Generation 1	Normal or force	Fail
				Force	Pass
	Auto max 2000	Auto	Generation 1	Normal or force	Pass
	Auto max 2000	Auto	Generation 2 or Generation 3	Normal	Fail
				Force	Pass
	Auto	Auto max 2000	Generation 2 or Generation 3	Normal	Fail
Generation 3 interfaces	Auto	Auto	Generation 1	Normal or force	Fail
				Force	Pass
	Auto max 2000	Auto	Generation 1	Normal or force	Pass
	Auto max 2000	Auto	Generation 2	Normal	Fail
				Force	Pass
	Auto	Auto max 2000	Generation 2	Normal	Fail
				Force	Pass
	Auto max 2000	Auto	Generation 3	Normal	Fail
	Auto	Auto max 2000	Generation 3	Normal	Fail
				Force	Pass

1. If resources are not available.

## Configuring Module Interface Shared Resources

This section describes how to configure Generation 2 and Generation 3 module interface shared resources and contains the following sections:

- [Configuration Guidelines for 48-Port, 24-Port, and 4/44-Port 8-Gbps Fibre Channel Switching Modules, page 5-15](#)
- [Configuration Guidelines for 48-Port and 24-Port 4-Gbps Fibre Channel Switching Modules, page 5-16](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- [Configuration Guidelines for 12-Port 4-Gbps Switching Module Interfaces, page 5-17](#)
- [Configuration Guidelines for 4-Port 10-Gbps Switching Module Interfaces, page 5-18](#)
- [Configuring Port Speed, page 5-18](#)
- [Configuring Rate Mode, page 5-19](#)
- [Configuring Oversubscription Ratio Restrictions, page 5-20](#)
- [Configuring Bandwidth Fairness, page 5-24](#)
- [Taking Interfaces Out of Service, page 5-26](#)
- [Releasing Shared Resources in a Port Group, page 5-27](#)

## Configuration Guidelines for 48-Port, 24-Port, and 4/44-Port 8-Gbps Fibre Channel Switching Modules

The 48-Port, 24-Port, and 4/44-Port 8-Gbps Fibre Channel switching modules support the following features:

- 1-Gbps, 2-Gbps, 4-Gbps, and 8-Gbps speed traffic
- Shared and dedicated rate mode
- ISL and Fx port modes
- Extended BB\_credits

### Migrating from Shared Mode to Dedicated Mode

To configure 48-port, 24-port, 4/44-port 8-Gbps Fibre Channel switching modules when starting with the default configuration or when migrating from shared rate mode to dedicated rate mode, follow these guidelines:

1. Take unused interfaces out of service to release resources for other interfaces, if necessary.  
See the [“Taking Interfaces Out of Service” section on page 5-26](#).
2. Configure the traffic speed to use (1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, or autosensing with a maximum of 2 Gbps or 4 Gbps).  
See the [“Configuring Port Speed” section on page 5-18](#).
3. Configure the rate mode (dedicated or shared).  
See the [“Configuring Rate Mode” section on page 5-19](#).
4. Configure the port mode.  
See the [“About Interface Modes” section on page 2-3](#).



---

**Note** ISL ports cannot operate in shared rate mode.

---

5. Configure the BB\_credits and extended BB\_credits, as necessary.  
See the [“About Extended BB\\_Credits” section on page 6-16](#).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Migrating from Dedicated Mode to Shared Mode

To configure 48-port, 24-port, 4/44-port 8-Gbps Fibre Channel switching modules migrating from dedicated rate mode to shared rate mode, follow these guidelines:

1. Take unused interfaces out of service to release resources for other interfaces, if necessary.  
See the [“Taking Interfaces Out of Service” section on page 5-26](#).
2. Configure the BB\_credits and extended BB\_credits, as necessary.  
See the [“BB\\_Credit Buffers for Switching Modules” section on page 6-5](#), [“BB\\_Credit Buffers for Switching Modules” section on page 6-5](#), and the [“About Extended BB\\_Credits” section on page 6-16](#).
3. Configure the port mode.  
See the [“About Interface Modes” section on page 2-3](#).




---

**Note** ISL ports cannot operate in shared rate mode.

---

4. Configure the rate mode (dedicated or shared) to use.  
See the [“Configuring Rate Mode” section on page 5-19](#).
5. Configure the traffic speed (1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, or autosensing with a maximum of 2 Gbps or 4 Gbps) to use.  
See the [“Configuring Port Speed” section on page 5-18](#).

## Configuration Guidelines for 48-Port and 24-Port 4-Gbps Fibre Channel Switching Modules

The 48-port and 24-port 4-Gbps Fibre Channel switching modules support the following features:

- 1-Gbps, 2-Gbps, and 4-Gbps speed traffic
- Shared and dedicated rate mode
- ISL (E or TE) and Fx (F or FL) port modes
- Extended BB\_credits

## Migrating from Shared Mode to Dedicated Mode

To configure 48-port and 24-port 4-Gbps Fibre Channel switching modules when starting with the default configuration or when migrating from shared rate mode to dedicated rate mode, follow these guidelines:

1. Take unused interfaces out of service to release resources for other interfaces, if necessary.  
See the [“Taking Interfaces Out of Service” section on page 5-26](#).
2. Configure the traffic speed to use (1 Gbps, 2 Gbps, 4 Gbps, or autosensing with a maximum of 2 Gbps or 4 Gbps).  
See the [“Configuring Port Speed” section on page 5-18](#).
3. Configure the rate mode (dedicated or shared) to use.  
See the [“Configuring Rate Mode” section on page 5-19](#).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

4. Configure the port mode.



---

**Note** ISL ports cannot operate in shared rate mode.

---

5. Configure the BB\_credits and extended BB\_credits, as necessary.

See the [“About Extended BB\\_Credits” section on page 6-16](#).

## Migrating from Dedicated Mode to Shared Mode

To configure 48-port and 24-port 4-Gbps Fibre Channel switching modules migrating from dedicated rate mode to shared rate mode, follow these guidelines:

1. Take unused interfaces out of service to release resources for other interfaces, if necessary.

See the [“Taking Interfaces Out of Service” section on page 5-26](#).

2. Configure the BB\_credits and extended BB\_credits, as necessary.

See the [“BB\\_Credit Buffers for Switching Modules” section on page 6-5](#), [“BB\\_Credit Buffers for Fabric Switches” section on page 6-14](#), and the [“About Extended BB\\_Credits” section on page 6-16](#).

3. Configure the port mode.

See the [“About Interface Modes” section on page 2-3](#).



---

**Note** ISL ports cannot operate in shared rate mode.

---

4. Configure the rate mode (dedicated or shared) to use.

See the [“Configuring Rate Mode” section on page 5-19](#).

5. Configure the traffic speed (1 Gbps, 2 Gbps, 4 Gbps, or autosensing with a maximum of 2 Gbps or 4 Gbps) to use.

See the [“Configuring Port Speed” section on page 5-18](#).

## Configuration Guidelines for 12-Port 4-Gbps Switching Module Interfaces

The 12-port 4-Gbps switching modules support the following features:

- 1-Gbps, 2-Gbps, and 4-Gbps speed traffic
- Only dedicated rate mode
- ISL (E or TE) and Fx (F or FL) port modes
- Extended BB\_credits
- Performance buffers

To configure 4-port 10-Gbps switching modules when starting with the default configuration, follow these guidelines:

1. Configure the traffic speed (1 Gbps, 2 Gbps, 4 Gbps, or autosensing with a maximum of 2 Gbps or 4 Gbps) to use.

See the [“Configuring Port Speed” section on page 5-18](#).

2. Configure the port mode.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

3. Configure the BB\_credits, performance buffers, and extended BB\_credits, as necessary.

See the “BB\_Credit Buffers for Switching Modules” section on page 6-5, “BB\_Credit Buffers for Fabric Switches” section on page 6-14, and the “About Extended BB\_Credits” section on page 6-16.


**Note**

If you change the port bandwidth reservation parameters on a 48-port or 24-port module, the change affects only the changed port. No other ports in the port group are affected.

## Configuration Guidelines for 4-Port 10-Gbps Switching Module Interfaces

The 4-port 10-Gbps switching modules support the following features:

- Only 10-Gbps speed traffic
- Only dedicated rate mode
- ISL (E or TE) and F port modes
- Extended BB\_credits
- Performance buffers

Use the following guidelines to configure 4-port 10-Gbps switching modules when starting with the default configuration:

1. Configure the port mode.

See the “About Interface Modes” section on page 2-3.

2. Configure the BB\_credits, performance buffers, and extended BB\_credits, as necessary.

See the “BB\_Credit Buffers for Switching Modules” section on page 6-5, “BB\_Credit Buffers for Fabric Switches” section on page 6-14, and the “About Extended BB\_Credits” section on page 6-16.

## Configuring Port Speed

The port speed on an interface, combined with the rate mode, determines the amount of shared resources available to the ports in the port group on a 48-port, 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching module. Especially in the case of dedicated rate mode, the port group resources are reserved even though the bandwidth is not used. For example, on Generation 2 modules, if an interface is configured for autosensing (auto) and dedicated rate mode, then 4 Gbps of bandwidth is reserved even though the maximum operating speed is 2 Gbps. For the same interface, if autosensing with a maximum speed of 2 Gbps (auto max 2000) is configured, then only 2 Gbps of bandwidth is reserved and the unused 2 Gbps is shared with the other interface in the port group.


**Note**

- The Generation 2, 4-port 10-Gbps switching module supports 10-Gbps traffic only.
- On Generation 3, 8-Gbps modules, setting the port speed to auto enables autosensing, which negotiates to a maximum speed of 8 Gbps.
- On Generation 2, 4-Gbps modules, setting the port speed to auto enables autosensing, which negotiates to a maximum speed of 4 Gbps.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**



### Caution

Changing port speed and rate mode disrupts traffic on the port. Traffic on other ports in the port group is not affected.

To configure dedicated bandwidth on an interface using Fabric Manager, follow these steps:

- Step 1** Select a switch from the Fabric pane, or select a group of switches (SAN, fabric, VSAN) from the Logical Domains pane.
- Step 2** Expand **Switches**, expand **Interfaces** and select **FC Physical** from the Physical Attributes pane. You see the **FC Physical > General** tab in the Interfaces pane.
- Step 3** Scroll until you see the row containing the switch and port you want to configure.
- Step 4** Select **auto**, **1Gb**, **4Gb**, or **autoMax2G** from the Speed Admin column (see [Figure 5-3](#)).



### Note

The Generation 3, 8-Gbps Fibre Channel switching modules support the following **speed** configurations: **1G**, **2G**, **4G**, **8G**, **autoMax2G**, **autoMax4G** and the **auto** speed configuration configures autosensing for the interface with 8 Gbps of bandwidth reserved.

**Figure 5-3 Speed Admin Column in Port Configuration**

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	FailureCause
sw-isola-220	fc9/7	FX	auto	300	n/a		auto	n/a	shared	in	up	down	linkFailure
sw-isola-220	fc9/34	FX	auto	300	n/a		auto	n/a	shared	in	up	down	linkFailure
sw-isola-220	fc13/12	FX	auto	300	n/a		auto	n/a	shared	in	up	down	linkFailure
sw-isola-220	fc9/33	FX	auto	300	n/a		1Gb	n/a	shared	in	up	down	linkFailure
sw-isola-220	fc9/1	FX	auto	300	n/a		2Gb	n/a	shared	in	up	down	linkFailure
							4Gb						
							autoMax2G						

The auto parameter enables autosensing on the interface. The autoMax2G parameter enables autosensing on the interface with a maximum speed of 2 Gbps.



### Note

If you change the port bandwidth reservation parameters on a 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching module, the change affects only the changed port. No other ports in the port group are affected.

- Step 5** Click the **Apply Changes** icon.

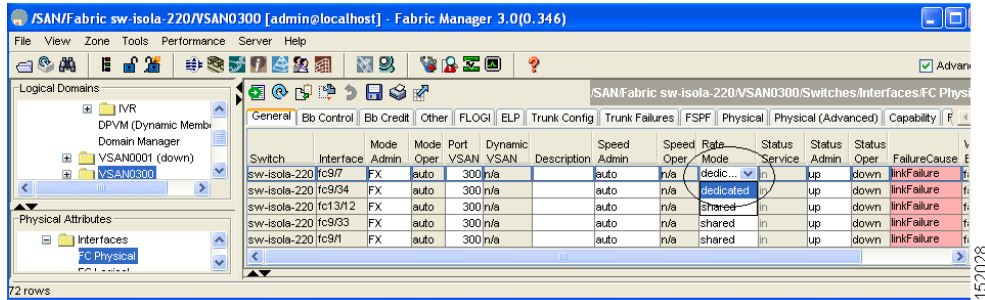
## Configuring Rate Mode

To configure the rate mode (dedicated or shared) on an interface on a 4-Gbps or 8-Gbps Fibre Channel switching module using Fabric Manager, follow these steps:

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 1** Select a switch from the Fabric pane, or select a group of switches (SAN, fabric, VSAN) from the Logical Domains pane.
- Step 2** Expand **Switches > Interfaces** and then select **FC Physical** from the Physical Attributes pane. You see the **FC Physical > General** tab in the Interfaces pane.
- Step 3** Scroll until you see the row containing the switch and port you want to configure.
- Step 4** Select **dedicated** or **shared** from the Rate Mode column (see [Figure 5-4](#)).

**Figure 5-4 Rate Mode Port Configuration**



- Step 5** Click the **Apply Changes** icon.



**Caution**

Changing port speed and rate mode disrupts traffic on the port.

## Configuring Oversubscription Ratio Restrictions

The 48-port and 24-port 4-Gbps, and all 8-Gbps Fibre Channel switching modules support oversubscription on switches with shared rate mode configurations. By default, all 48-port and 24-port 4-Gbps, and 8-Gbps Fibre Channel switching modules have restrictions on oversubscription ratios enabled. As of Cisco SAN-OS Release 3.1(1) and NX-OS Release 4.1(1), you can disable restrictions on oversubscription ratios.

[Table 5-10](#) describes the bandwidth allocation for oversubscribed interfaces configured in shared mode on the 4-Gbps and 8-Gbps modules.

**Table 5-10 Bandwidth Allocation for Oversubscribed Interfaces**

Switching Module	Configured Speed	Reserved Bandwidth (Gbps)		Maximum Bandwidth (Gbps)
		Ratios enabled	Ratios disabled	
48-Port 8-Gbps Fibre Channel Module	Auto 8 Gbps	0.36	0.2	8
	Auto Max 4 Gbps	0.24	0.1	4
	Auto Max 2 Gbps	0.12	0.05	2



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Table 5-10 Bandwidth Allocation for Oversubscribed Interfaces (continued)**

Switching Module	Configured Speed	Reserved Bandwidth (Gbps)		Maximum Bandwidth (Gbps)
		Ratios enabled	Ratios disabled	
24-Port 8-Gbps Fibre Channel Module	Auto 8 Gbps	0.8	0.8	8
	Auto Max 4 Gbps	0.4	0.4	4
	Auto Max 2 Gbps	0.2	0.2	2
4/44-Port 8-Gbps Host-Optimized Fibre Channel Module	8 Gbps	0.87	0.16	8
	Auto Max 4 Gbps	0.436	0.08	4
	Auto Max 2 Gbps	0.218	0.04	2
	1 Gbps	0.109	0.02	1
48-port 4-Gbps Fibre Channel switching module	Auto 4 Gbps	0.8	0.09	4
	Auto Max 2 Gbps	0.4	0.045	2
	1 Gbps	0.2	0.0225	1
24-port 4-Gbps Fibre Channel switching module	Auto 4 Gbps	1	0.27	4
	Auto Max 2 Gbps	0.5	0.135	2
	1 Gbps	0.25	0.067	1

All ports in the 48-port and 24-port 4-Gbps modules can be configured to operate at 4 Gbps in shared mode even if other ports in the port group are configured in dedicated mode, regardless of available bandwidth. However, when oversubscription ratio restrictions are enabled, you may not have all shared 4-Gbps module ports operating at 4 Gbps.

All ports in the 48-port and 24-port 8-Gbps modules can be configured to operate at 8 Gbps in shared mode even if other ports in the port group are configured in dedicated mode, regardless of available bandwidth. However, when oversubscription ratio restrictions are enabled you may not have all shared 8-Gbps module ports operating at 8 Gbps.

On the 48-port and 24-port 8-Gbps modules, if you have configured one 8-Gbps dedicated port in one port group, no other ports in the same port group can be configured to operate at 8-Gbps dedicated mode. You can have any number of 8-Gbps shared and 4-Gbps dedicated or shared ports. On the 4/44-port 8-Gbps module, only one port per port group can be configured in 8-Gbps dedicated or shared mode.

In the following example, a 24-port 4-Gbps module has oversubscription ratios enabled and three dedicated ports in one port group operating at 4-Gbps. No other ports in the same port group can be configured to operate at 4 Gbps.

For dedicated ports, oversubscription ratio restrictions do not apply to the shared pool in port groups. So if oversubscription ratio restrictions are disabled, and you have configured three 4-Gbps dedicated ports in one port group, then you can configure all other ports in the same port group to operate at a shared rate of 4 Gbps.

When disabling restrictions on oversubscription ratios, all ports in shared mode on 48-port and 24-port 4-Gbps or any 8-Gbps Fibre Channel switching modules must be shut down. When applying restrictions on oversubscription ratios, you must take shared ports out of service.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**



#### Note

When restrictions on oversubscription ratios are disabled, the bandwidth allocation among the shared ports is proportionate to the configured speed. If the configured speed is auto on Generation 2 modules, then bandwidth is allocated assuming a speed of 4 Gbps. For example, if you have three shared ports configured at 1, 2, and 4 Gbps, then the allocated bandwidth ratio is 1:2:4.

As of Cisco SAN-OS Release 3.0 and NX-OS Release 4.1(1) or when restrictions on oversubscription ratios are enabled, the port bandwidths are allocated in equal proportions, regardless of port speed, so, the bandwidth allocation for the same three ports mentioned in the example would be 1:1:1.

## Disabling Restrictions on Oversubscription Ratios

Before disabling restrictions on oversubscription ratios, ensure that you have explicitly shut down shared ports.

To disable restrictions on oversubscription ratios on multiple 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching modules using Fabric Manager, follow these steps:

**Step 1** Choose **Physical > Modules**.

You see the Module dialog box (see [Figure 5-5](#)).

**Figure 5-5**      **Module Dialog Box**

Module	Name	Model	Oper Status	Reset?	RateModeOversubsc...	BandwidthFairness...	Power Admin	Power Oper	Status	LastChangeTime	AdminStatus	OperStatus	Current
1	2x1GE IPS, 14x1/2Gbps FC Module	DS-X9302-14K9	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	25229.4W / 600.7A
3	1/2/4 Gbps FC Module	DS-X9148	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	184.8W / 4.4A
5	IP Storage Services Module	DS-X9308-SMIP	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	200.34W / 4.77A
6	IP Storage Services Module	DS-X9304-SMIP	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	160.02W / 3.81A
7	Supervisor/Fabric-2	DS-X9530-SF2-K9	ha-standby	<input type="checkbox"/>	enabled	enable	enabled	Reset triggered due ...		2007/01/26-07:39:13	on	ok	126.0W / 3.0A
8	Supervisor/Fabric-2	DS-X9530-SF2-K9	active	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/25-20:59:57	on	ok	126.0W / 3.0A
11	1/2/4 Gbps FC Module	DS-X9124	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	168.0W / 4.0A
13	1/2 Gbps FC Module	DS-X9016	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	210.0W / 5.0A
14	Fabric card module	DS-13SLT-FAB1	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	84.0W / 2.0A
15	Fabric card module	DS-13SLT-FAB1	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown		2007/01/26-07:37:27	on	ok	84.0W / 2.0A



#### Caution

This feature is only supported on 48-port and 24-port 4-Gbps, and 8-Gbps Fibre Channel switching modules.

**Step 2** Select **disabled** from the RateModeOversubscriptionLimit drop-down list for each module for which you want to disable restrictions on oversubscription ratios.

**Step 3** Click **Apply** to save the changes.

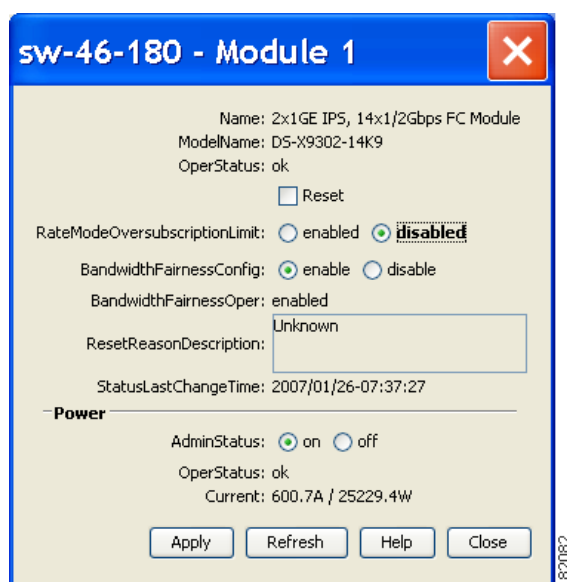
To disable restrictions on oversubscription ratios on a single 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching module using Device Manager, follow these steps:

**Step 1** Right-click a module and select **Configure**.

You see the Module dialog box (see [Figure 5-6](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 5-6**      **Module Dialog Box**



**Step 2** Click the **disabled** radio button to disable restrictions on oversubscription ratios.

**Step 3** Click **Apply** to save the changes.

## Enabling Restrictions on Oversubscription Ratios



### Caution

You must enable restrictions on oversubscription ratios before you can downgrade modules to a previous release.

Before enabling restrictions on oversubscription ratios, ensure that you have explicitly configured shared ports to out-of-service mode.

To enable restrictions on oversubscription ratios on multiple 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching modules using Fabric Manager, follow these steps:

**Step 1** Choose **Physical > Modules**.

You see the Module dialog box (see [Figure 5-5](#)).

**Step 2** Select **enabled** from the RateModeOversubscriptionLimit drop-down list for each module for which you want to enable restrictions on oversubscription ratios.

**Step 3** Click **Apply** to save the changes.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

To enable restrictions on oversubscription ratios on a single 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching module using Device Manager, follow these steps:

- 
- Step 1** Right-click a module and select **Configure**.  
You see the Module dialog box (see [Figure 5-6](#)).
- Step 2** Click the **enabled** radio button to enable restrictions on oversubscription ratios.
- Step 3** Click **Apply** to save the changes.
- 

## Configuring Bandwidth Fairness

This feature improves fairness of bandwidth allocation among all ports and provides better throughput average to individual data streams. Bandwidth fairness can be configured per module.

As of Cisco SAN-OS Release 3.1(2), all 48-port and 24-port 4-Gbps Fibre Channel switching modules, as well as 18-port Fibre Channel/4-port Gigabit Ethernet Multiservice modules, have bandwidth fairness enabled by default. As of Cisco NX-OS Release 4.1(1), all the 8-Gbps Fibre Channel switching modules have bandwidth fairness enabled by default.



### Caution

When you disable or enable bandwidth fairness, the change does not take effect until you reload the module.

---

This section includes the following topics:

- [Enabling Bandwidth Fairness, page 5-24](#)
- [Disabling Bandwidth Fairness, page 5-26](#)
- [Upgrade or Downgrade Scenario, page 5-26](#)



### Note

This feature is supported only on the 48-port and 24-port 4-Gbps modules, the 8-Gbps modules, and the 18/4-port Multiservice Module (MSM).

---

## Enabling Bandwidth Fairness

To enable bandwidth fairness on multiple 48-port or 24-port 4-Gbps, or any 8-Gbps Fibre Channel switching modules using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Physical > Modules**.  
You see the Module dialog box (see [Figure 5-7](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 5-7 Module Dialog Box**

Module	Name	Model	Oper Status	Reset?	RateModeOverSubsc...	BandwidthFairness...	Power Admin	Power Oper	StatusLastChangeTime	AdminStatus	OperStatus	Current
1	2x1GE IPS, 14x1/2Gbps FC Module	DS-X9302-14K9	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	25229.4W / 600.7A
3	1/2 1/4 Gbps FC Module	DS-X9148	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	184.8W / 4.4A
5	IP Storage Services Module	DS-X9308-SMP	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	200.34W / 4.77A
6	IP Storage Services Module	DS-X9304-SMP	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	160.02W / 3.81A
7	Supervisor/Fabric-2	DS-X9530-SF2-K9	ha-standby	<input type="checkbox"/>	enabled	enable	enabled	Reset triggered due ...	2007/01/26-07:39:13	on	ok	126.0W / 3.0A
8	Supervisor/Fabric-2	DS-X9530-SF2-K9	active	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/25-20:59:57	on	ok	126.0W / 3.0A
11	1/2 1/4 Gbps FC Module	DS-X9124	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	168.0W / 4.0A
13	1/2 Gbps FC Module	DS-X9016	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	210.0W / 5.0A
14	Fabric card module	DS-13SLT-FAB1	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	84.0W / 2.0A
15	Fabric card module	DS-13SLT-FAB1	ok	<input type="checkbox"/>	enabled	enable	enabled	Unknown	2007/01/26-07:37:27	on	ok	84.0W / 2.0A

10 row(s)

Buttons: Apply Refresh Help Close

- Step 2** Select **enable** from the BandwidthFairnessConfig drop-down list for each module for which you want to enable bandwidth fairness.
- Step 3** Click **Apply** to save the changes.

To enable bandwidth fairness on a single 48-port or 24-port 4-Gbps Fibre Channel switching module using Device Manager, follow these steps:

- Step 1** Right-click a module and select **Configure**.  
You see the Module dialog box (see Figure 5-8).

**Figure 5-8 Module Dialog Box**

**sw-46-180 - Module 1**

Name: 2x1GE IPS, 14x1/2Gbps FC Module  
ModelName: DS-X9302-14K9  
OperStatus: ok

☐ Reset

RateModeOverSubscriptionLimit: ☒ enabled ☐ disabled

BandwidthFairnessConfig: ☐ enable ☒ **disable**

BandwidthFairnessOper: enabled

ResetReasonDescription:

StatusLastChangeTime: 2007/01/26-07:37:27

**Power**

AdminStatus: ☒ on ☐ off

OperStatus: ok

Current: 600.7A / 25229.4W

Buttons: Apply Refresh Help Close

- Step 2** Click the **enable** radio button to enable bandwidth fairness.
- Step 3** Click **Apply** to save the changes.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Disabling Bandwidth Fairness



### Note

If you disable bandwidth fairness, up to a 20 percent increase in internal bandwidth allocation is possible for each port group; however, bandwidth fairness is not guaranteed when there is a mix of shared and full-rate ports in the same port group.

To disable bandwidth fairness on multiple 48-port or 24-port 4-Gbps, or 8-Gbps Fibre Channel switching modules using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Physical > Modules**.  
You see the Module dialog box (see [Figure 5-7](#)).
  - Step 2** Select **disable** from the BandwidthFairnessConfig drop-down list for each module for which you want to disable bandwidth fairness.
  - Step 3** Click **Apply** to save the changes.
- 

To disable bandwidth fairness on a single 48-port or 24-port 4-Gbps, or 8-Gbps Fibre Channel switching module using Device Manager, follow these steps:

- 
- Step 1** Right-click a module and select **Configure**.  
You see the Module dialog box (see [Figure 5-8](#)).
  - Step 2** Click the **disable** radio button to disable bandwidth fairness.
  - Step 3** Click **Apply** to save the changes.
- 

## Upgrade or Downgrade Scenario

When you are upgrading from a release earlier than Cisco SAN-OS Release 3.1(2), all modules operate with bandwidth fairness disabled until the next module reload. After the upgrade, any new module that is inserted has bandwidth fairness enabled.

When you are downgrading to a release earlier than Cisco SAN-OS Release 3.1(2), all modules keep operating in the same bandwidth fairness configuration prior to the downgrade. After the downgrade, any new module that is inserted has bandwidth fairness disabled.



### Note

After the downgrade, any insertion of a module or module reload will have bandwidth fairness disabled.

## Taking Interfaces Out of Service

You can take interfaces out of service on Generation 2 and Generation 3 switching modules. When an interface is out of service, all the shared resources for the interface are released as well as the configuration associated with those resources.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Note**

The interface must be disabled before it can be taken out of service.

**Caution**

Taking interfaces out of service releases all the shared resources to ensure that they are available to other interfaces. This causes the configuration in the shared resources to revert to default when the interface is brought back into service. Also, an interface cannot come back into service unless the default shared resources for the port are available. The operation to free up shared resources from another port is disruptive.

**Note**

The interface cannot be a member of a PortChannel.

To take an interface out of service using Fabric Manager, follow these steps:

- Step 1** Select a switch from the Fabric pane, or select a group of switches (SAN, fabric, VSAN) from the Logical Domains pane.
- Step 2** Expand **Switches**, expand **Interfaces** and select **FC Physical** in the Physical Attributes pane. You see the **FC Physical > General** tab in the Information pane.
- Step 3** Scroll down until you see the row containing the switch and port you want to configure.
- Step 4** Scroll right (if necessary) until you see the **Status Service** column.
- Step 5** Select **in** or **out** from the Status Service column.
- Step 6** Click the **Apply Changes** icon.

## Releasing Shared Resources in a Port Group

When you want to reconfigure the interfaces in a port group on a Generation 2 or Generation 3 module, you can return the port group to the default configuration to avoid problems with allocating shared resources.

**Note**

The interface cannot be a member of a PortChannel.

**Caution**

Releasing shared resources disrupts traffic on the port. Traffic on other ports in the port group is not affected.

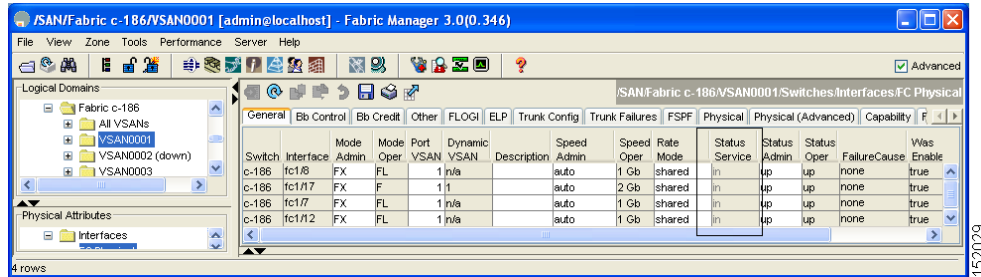
To release the shared resources for a port group using Fabric Manager, follow these steps:

- Step 1** Select a switch from the Fabric pane, or select a group of switches (SAN, fabric, VSAN) from the Logical Domains pane.
- Step 2** Expand **Switches > Interfaces** and then select **FC Physical** from the Physical Attributes pane. You see the **FC Physical > General** tab in the Information pane.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 3** Scroll down until you see the row containing the switch and port you want to configure.
- Step 4** Scroll right (if necessary) until you see the **Status Service** column (see [Figure 5-9](#)).

**Figure 5-9 Status Service Column for FC Physical**



- Step 5** Select the **out** status from the **Status Service** column.
- Step 6** Click the **Apply Changes** icon.
- Step 7** Select the **in** status from the **Status Service** column.
- Step 8** Click the **Apply Changes** icon.

## Displaying SFP Diagnostic Information

To view diagnostic information for multiple ports using Device Manager, follow these steps:

- Step 1** Choose **Interface > FC All** and click the **Diagnostics** tab or hold down the **Control** key, and then click each port for which you want to view diagnostic information.
- Step 2** Right-click the selected ports, select **Configure**, and click the **Diagnostics** tab.
- You see the FC Interfaces dialog box (see [Figure 5-10](#)).



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 5-10 FC Interfaces Dialog Box**

Interface, Sensor	Value/Units	High Alarm	Low Alarm	High Warning	Low Warning
fc1/13, Voltage	3.2819 V	3.63	2.97	3.58	3.02
fc1/13, Current	7.118 mA	16	2	15	3
fc1/13, Temperature	29.347 C	95	-5	90	0
fc1/13, Rx Power	-2.873 dBm	1	0.05	0.794	0.063
fc1/13, Tx Power	-3.788 dBm	0.794	0.112	0.631	0.125
fc1/14, Voltage	3.2816 V	3.63	2.97	3.58	3.02
fc1/14, Current	7.336 mA	16	2	15	3
fc1/14, Temperature	29.375 C	95	-5	90	0
fc1/14, Rx Power	-3.089 dBm	1	0.05	0.794	0.063
fc1/14, Tx Power	-3.496 dBm	0.794	0.112	0.631	0.125
fc1/20, Voltage	3.2816 V	3.63	2.97	3.58	3.02
fc1/20, Current	5.548 mA	16	2	15	3
fc1/20, Temperature	29.406 C	95	-5	90	0
fc1/20, Rx Power	-3.269 dBm	1	0.05	0.794	0.063
fc1/20, Tx Power	-3.695 dBm	0.794	0.112	0.631	0.125
fc1/22, Voltage	3.2887 V	3.9	2.7	3.7	2.9
fc1/22, Current	8.08 mA	17	1	14	2
fc1/22, Temperature	27.671 C	95	-25	90	-20
fc1/22, Rx Power	-4.659 dBm	1.259	0.01	0.794	0.015
fc1/22, Tx Power	-4.236 dBm	0.631	0.067	0.631	0.079

20 row(s) (Note: ++ high-alarm + high-warning; -- low-alarm; - low-warning)

**Step 3** Click **Refresh** to view the latest diagnostic information.

To view diagnostic information for a single port using Device Manager, follow these steps:

**Step 1** Right-click a port, select **Configure**, and click the **Diagnostics** tab.  
You see the port licensing options for the selected port (see Figure 5-11).

**Figure 5-11 Diagnostics Tab for Selected Port**

Interface, Sensor	Value/Units	High Alarm	Low Alarm	High Warning	Low Warning
fc1/13, Voltage	3.2819 V	3.63	2.97	3.58	3.02
fc1/13, Current	7.118 mA	16	2	15	3
fc1/13, Temperature	29.347 C	95	-5	90	0
fc1/13, Rx Power	-2.865 dBm	1	0.05	0.794	0.063
fc1/13, Tx Power	-3.798 dBm	0.794	0.112	0.631	0.125

5 row(s) (Note: ++ high-alarm + high-warning; -- low-alarm; - low-warning)

**Step 2** Click **Refresh** to view the latest diagnostic information.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Default Settings

Table 5-11 lists the default settings for Generation 2 interface parameters.

**Table 5-11 Default Generation 2 Interface Parameters**

Parameter	Default			
	48-Port 4-Gbps Switching Module	24-Port 4-Gbps Switching Module	12-Port 4-Gbps Switching Module	4-Port 10-Gbps Switching Module
Speed mode	auto <sup>1</sup>	auto <sup>1</sup>	auto <sup>1</sup>	auto <sup>2</sup>
Rate mode	shared	shared	dedicated	dedicated
Port mode	Fx	Fx	auto <sup>3</sup>	auto <sup>4</sup>
BB_credit buffers	16	16	250	250
Performance buffers	—	—	145 <sup>5</sup>	145 <sup>5</sup>

1. Auto speed mode on the 4-Gbps switching modules enables autosensing and negotiates to a maximum speed of 4 Gbps.
2. The 4-port 10-Gbps switching module only supports 10-Gbps traffic.
3. Auto port mode on the 12-port 4-Gbps switching module interfaces can operate in E port mode, TE port mode, and Fx port mode.
4. Auto port mode on the 4-port 10-Gbps switching module interfaces can operate in E port mode, TE port mode, and F port mode.
5. Performance buffers are shared among all ports on the module.

Table 5-12 lists the default settings for Generation 3 interface parameters.

**Table 5-12 Default Generation 3 Interface Parameters**

Parameter	Default		
	48-Port 8-Gbps Switching Module	24-Port 8-Gbps Switching Module	4/44-Port 8-Gbps Host-Optimized Switching Module
Speed mode	auto <sup>1</sup>	auto <sup>1</sup>	auto_max_4G <sup>2</sup>
Rate mode	shared	shared	shared
Port mode	Fx	Fx	Fx
BB_credit buffers	32	32	32

1. Auto speed mode on the 8-Gbps switching modules enables autosensing and negotiates to a maximum speed of 8 Gbps.
2. Auto\_max\_4G speed mode on the 4/44-port 8-Gbps switching module negotiates to a maximum speed of 4 Gbps.



## CHAPTER 6

# Configuring Interface Buffers

---

Fibre Channel interfaces use buffer credits to ensure all packets are delivered to their destination. This chapter describes the different buffer credits available on the Cisco MDS 9000 Family switches and modules, and includes the following topics:

- [About Buffer-to-Buffer Credits, page 6-1](#)
- [Configuring Buffer-to-Buffer Credits, page 6-2](#)
- [About Performance Buffers, page 6-2](#)
- [Configuring Performance Buffers, page 6-2](#)
- [Buffer Pools, page 6-3](#)
- [BB\\_Credit Buffers for Switching Modules, page 6-5](#)
- [BB\\_Credit Buffers for Fabric Switches, page 6-14](#)
- [About Extended BB\\_Credits, page 6-16](#)
- [Configuring Extended BB\\_credits, page 6-18](#)
- [Enabling Buffer-to-Buffer Credit Recovery, page 6-19](#)
- [About Receive Data Field Size, page 6-19](#)
- [Configuring Receive Data Field Size, page 6-19](#)

## About Buffer-to-Buffer Credits

Buffer-to-buffer credits (BB\_credits) are a flow-control mechanism to ensure that Fibre Channel switches do not run out of buffers, so that switches do not drop frames. BB\_credits are negotiated on a per-hop basis.

The receive BB\_credit (fcrxbbcredit) value may be configured for each Fibre Channel interface. In most cases, you do not need to modify the default configuration.

The receive BB\_credit values depend on the module type and the port mode, as follows:

- For 16-port switching modules and full rate ports, the default value is 16 for Fx mode and 255 for E or TE modes. The maximum value is 255 in all modes. This value can be changed as required.
- For 32-port switching modules and host-optimized ports, the default value is 12 for Fx, E, and TE modes. These values cannot be changed.
- For Generation 2 and Generation 3 switching modules, see the [“Buffer Pools” section on page 6-3](#).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Note**

In the Cisco MDS 9100 Series switches, the groups of ports on the left outlined in white are in dedicated rate mode. The other ports are host-optimized. Each group of 4 host-optimized ports have the same features as for the 32-port switching module.

## Configuring Buffer-to-Buffer Credits

To configure BB\_credits for a Fibre Channel interface using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
  - Step 2** Click the **Bb Credit** tab.  
You see the buffer credits.
  - Step 3** Set any of the buffer-to-buffer credits for an interface.
  - Step 4** Click **Apply Changes**.
- 

## About Performance Buffers

Regardless of the configured receive BB\_credit value, additional buffers, called performance buffers, improve switch port performance. Instead of relying on the built-in switch algorithm, you can manually configure the performance buffer value for specific applications (for example, forwarding frames over FCIP interfaces).

**Note**

Performance buffers are not supported on the Cisco MDS 9148 Fabric Switch, Cisco MDS 9124 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

For each physical Fibre Channel interface in any switch in the Cisco MDS 9000 Family, you can specify the amount of performance buffers allocated in addition to the configured receive BB\_credit value.

The default performance buffer value is 0. If you set the performance buffer value to 0, the built-in algorithm is used. If you do not specify the performance buffer value, 0 is automatically used.

## Configuring Performance Buffers

To configure performance buffers for a Fibre Channel interface using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**.  
You see the interface configuration in the Information pane.
  - Step 2** Click the **BB Credit** tab.  
You see performance buffer information in the Perf Bufs Admin and Perf Bufs Oper columns.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 3** Set the performance buffers for an interface.

**Step 4** Click **Apply Changes**.

## Buffer Pools

In the architecture of Generation 2 and Generation 3 modules, receive buffers shared by a set of ports are called *buffer groups*. The receive buffer groups are organized into *global* and *local* buffer pools.

The receive buffers allocated from the global buffer pool to be shared by a port group are called a *global receive buffer pool*. Global receive buffer pools include the following buffer groups:

- Reserved internal buffers
- Allocated BB\_credit buffers for each Fibre Channel interface (user configured or assigned by default)
- Common unallocated buffer pool for BB\_credits, if any, to be used for additional BB\_credits as needed
- Performance buffers (only used on 12-port 4-Gbps and 4-port 10-Gbps switching modules)

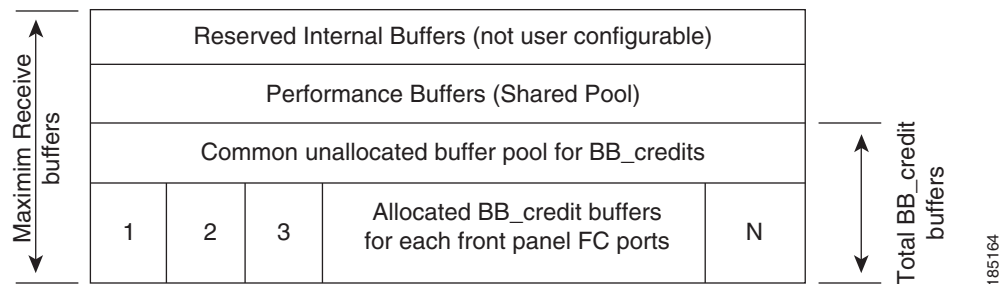


### Note

The 48-port and 24-port 8-Gbps modules have *dual global buffer pools*. Each buffer pool in the 48-port modules support 24 ports and in the 24-port modules each buffer pool supports 12 ports.

Figure 6-1 shows the allocation of BB\_credit buffers on line cards (24-port and 48-port 4-Gbps line cards).

**Figure 6-1 Receive Buffers for Fibre Channel Ports in a Global Buffer Pool**



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Figure 6-2 shows the default BB\_credit buffer allocation model for 48-port 8-Gbps switching modules. The minimum BB\_credits required to bring up a port is two buffers.

**Figure 6-2 BB\_Credit Buffer Allocation in 48-Port 8-Gbps Switching Modules**

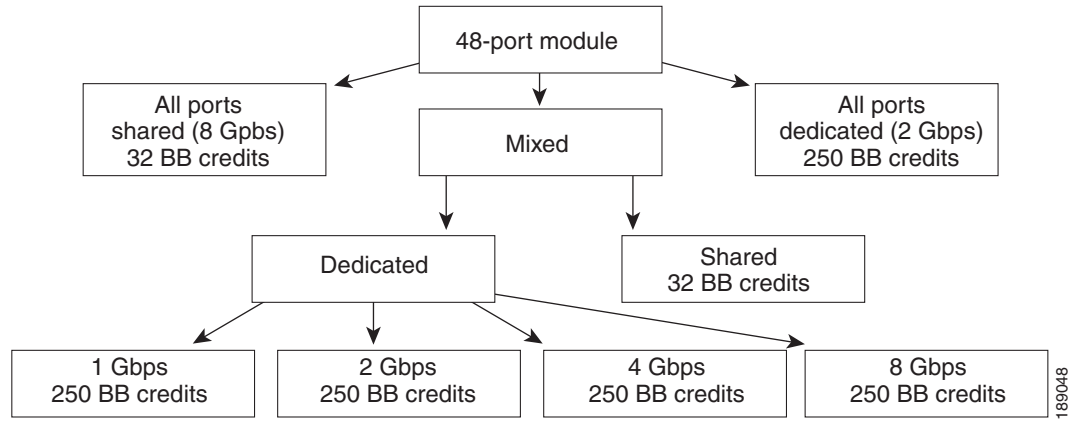
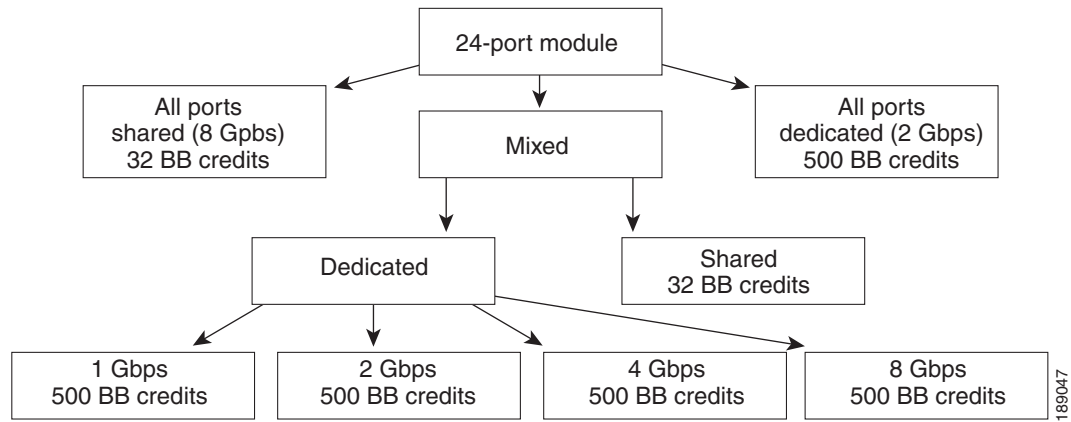


Figure 6-3 shows the default BB\_credit buffer allocation model for 24-port 8-Gbps switching modules. The minimum BB\_credits required to bring up a port is two buffers.

**Figure 6-3 BB\_Credit Buffer Allocation in 24-Port 8-Gbps Switching Modules**



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

Figure 6-4 shows the default BB\_credit buffer allocation model for 4/44-port 8-Gbps host-optimized switching modules. The minimum BB\_credits required to bring up a port is two buffers.

**Figure 6-4 BB\_Credit Buffer Allocation in 4/44-Port 8-Gbps Switching Modules**

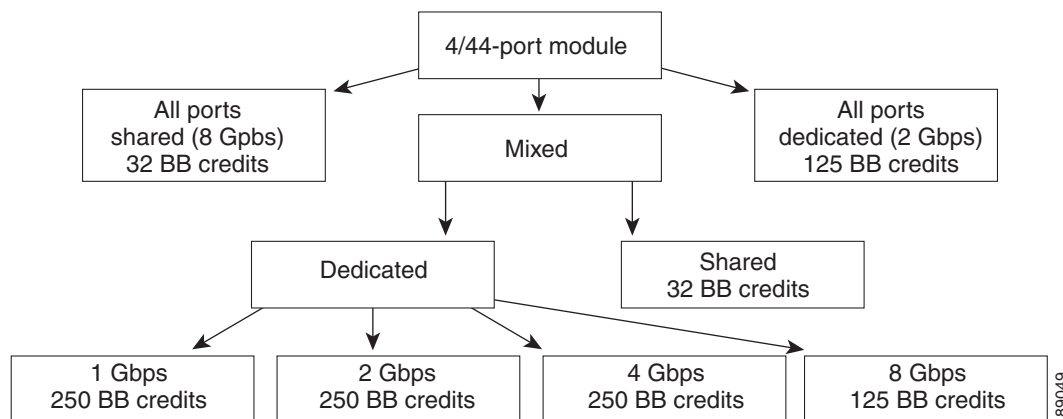
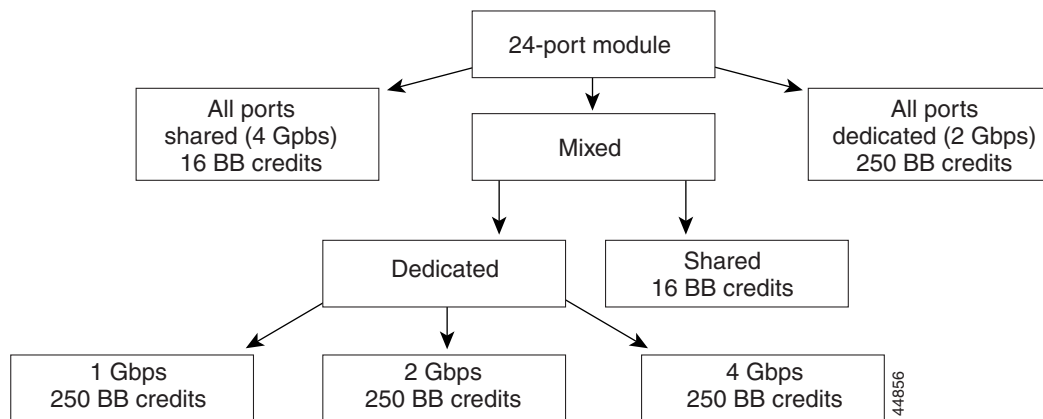


Figure 6-5 shows the default BB\_credit buffer allocation model for 24-port 4-Gbps switching modules. The minimum BB\_credits required to bring up a port is two buffers.

**Figure 6-5 BB\_Credit Buffer Allocation in 24-Port 4-Gbps Switching Modules**



**Note**

The default BB\_credit buffer allocation is the same for all port speeds.

## BB\_Credit Buffers for Switching Modules

This section describes how buffer credits are allocated to Cisco MDS 9000 switching modules, and includes the following topics:

- [48-Port 8-Gbps Fibre Channel Module BB\\_Credit Buffers, page 6-6](#)
- [24-Port 8-Gbps Fibre Channel Module BB\\_Credit Buffers, page 6-7](#)
- [4/44-Port 8-Gbps Host-Optimized Fibre Channel Module BB\\_Credit Buffers, page 6-8](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- [48-Port 4-Gbps Fibre Channel Module BB\\_Credit Buffers, page 6-9](#)
- [24-Port 4-Gbps Fibre Channel Module BB\\_Credit Buffers, page 6-10](#)
- [18-Port Fibre Channel/4-Port Gigabit Ethernet Multiservice Module BB\\_Credit Buffers, page 6-11](#)
- [4-Port 10-Gbps Switching Module BB\\_Credit Buffers, page 6-13](#)

## 48-Port 8-Gbps Fibre Channel Module BB\_Credit Buffers

Table 6-1 lists the BB\_credit buffer allocation for the 48-port 8-Gbps Fibre Channel switching module.

**Table 6-1 48-Port 8-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 8-Gbps Speed		Shared Rate Mode 8-Gbps Speed
	ISL	Fx Port	Fx Port
Default BB_credit buffers	250	32	32
Maximum BB_credit buffers	500	500	32
<b>Total Number of BB_Credit Buffers per Module</b>			
Ports 1 through 24	6000		
Ports 25 through 48	6000		

The following guidelines apply to BB\_credit buffers on 48-port 8-Gbps Fibre Channel switching modules:

- BB\_credit buffers allocated for ports 1 through 24 and 25 through 48 can be a maximum of 6000 each so that the load is distributed.
- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 500 buffers for dedicated rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 500 buffers for dedicated rate mode or 32 buffers for shared rate mode.
- Performance buffers are not supported on this module.

Each port group on the 48-port 8-Gbps Fibre Channel switching module consists of six ports. The ports in shared rate mode in a port group can have a maximum bandwidth oversubscription of 10:1 considering that each port group has 12.8-Gbps bandwidth.

The following example configurations are supported by the 48-port 8-Gbps Fibre Channel switching modules:

- Six ports with shared rate mode and 8-Gbps speed (4:1 oversubscription) (default)
- One port with dedicated rate mode and 8-Gbps speed plus five ports with shared rate mode and 8-Gbps speed (10:1 oversubscription)
- Two ports with dedicated rate mode and 4-Gbps speed plus four ports with shared rate mode and 4-Gbps speed (4:1 oversubscription)
- One port with dedicated rate mode and 4-Gbps speed plus three ports with dedicated rate mode and 2-Gbps speed plus two ports with shared rate mode and 4-Gbps speed (4:1 oversubscription)



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- Six ports with dedicated rate mode and 2-Gbps speed

## 24-Port 8-Gbps Fibre Channel Module BB\_Credit Buffers

Table 6-2 lists the BB\_credit buffer allocation for the 24-port 8-Gbps Fibre Channel switching module.

**Table 6-2 24-Port 8-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 8-Gbps Speed		Shared Rate Mode 8-Gbps Speed
	ISL	Fx Port	Fx Port
Default BB_credit buffers	500	32	32
Maximum BB_credit buffers	500 <sup>1</sup>	500 <sup>1</sup>	32
<b>Total Number of BB_Credit Buffers per Module</b>			
Ports 1 through 12	6000		
Ports 13 through 24	6000		

1. When connected to Generation 1 modules, reduce the maximum BB\_credit allocation to 250.

The following guidelines apply to BB\_credit buffers on 24-port 8-Gbps Fibre Channel switching modules:

- BB\_credit buffers allocated for ports 1 through 12 and 13 through 24 can be a maximum of 6000 each so that the load is distributed.
- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 500 buffers for dedicated rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 500 buffers for dedicated rate mode or 32 buffers for shared rate mode.
- Performance buffers are not supported on this module.

Each port group on the 24-port 8-Gbps Fibre Channel switching module consists of three ports. The ports in shared rate mode in a port group can have a maximum bandwidth oversubscription of 10:1 considering that each port group has 12.8-Gbps bandwidth.

The following example configurations are supported by the 24-port 8-Gbps Fibre Channel switching modules:

- Three ports with shared rate mode and 8-Gbps speed (2:1 oversubscription) (default)
- One port with dedicated rate mode and 8-Gbps speed plus two ports with shared rate mode and 8-Gbps speed (4:1 oversubscription)
- One port with dedicated rate mode and 8-Gbps speed plus one port with dedicated rate mode and 4-Gbps speed plus one port with shared rate mode and 8-Gbps speed (10:1 oversubscription)
- Two ports with dedicated rate mode and 4-Gbps speed plus one port with shared rate mode and 8-Gbps speed (2:1 oversubscription)
- Three ports with dedicated rate mode and 4-Gbps speed

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## 4/44-Port 8-Gbps Host-Optimized Fibre Channel Module BB\_Credit Buffers

Table 6-3 lists the BB\_credit buffer allocation for the 4/44-port 8-Gbps Fibre Channel switching module.

**Table 6-3 4/44-Port 8-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 8-Gbps Speed		Shared Rate Mode 8-Gbps Speed
	ISL	Fx Port	Fx Port
Default BB_credit buffers	125	32	32
Maximum BB_credit buffers	250	250	32
Total number of BB_credit buffers per module	6000		

The following guidelines apply to BB\_credit buffers on 4/44-port 8-Gbps Fibre Channel switching modules:

- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 500 buffers for dedicated rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 250 buffers for dedicated rate mode or 32 buffers for shared rate mode.
- Performance buffers are not supported on this module.

Each port group on the 24-port 8-Gbps Fibre Channel switching module consists of 12 ports. The ports in shared rate mode in a port group can have a maximum bandwidth oversubscription of 10:1 considering that each port group has 12.8-Gbps bandwidth.

The following example configurations are supported by the 4/44-port 8-Gbps Fibre Channel switching modules:

- Twelve ports with shared rate mode and 4-Gbps speed (5:1 oversubscription) (default)
- One port with dedicated rate mode and 8-Gbps speed plus eleven ports with shared rate mode and 4-Gbps speed (10:1 oversubscription)
- One port with dedicated rate mode and 4-Gbps speed plus three ports with dedicated rate mode and 3-Gbps speed plus eight ports with shared rate mode and 4-Gbps speed (2:1 oversubscription)
- Twelve ports with dedicated rate mode and 1-Gbps speed

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## 48-Port 4-Gbps Fibre Channel Module BB\_Credit Buffers

Table 6-4 lists the BB\_credit buffer allocation for 48-port 4-Gbps Fibre Channel switching modules.

**Table 6-4 48-Port 4-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 4-Gbps Speed		Shared Rate Mode 4-Gbps Speed
	ISL <sup>1</sup>	Fx Port	Fx Port
Default BB_credit buffers	125	16	16
Maximum BB_credit buffers	250	250	16
Total number of BB_credit buffers per module	6000		

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 48-port 4-Gbps Fibre Channel switching modules:

- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- Performance buffers are not supported on this module.

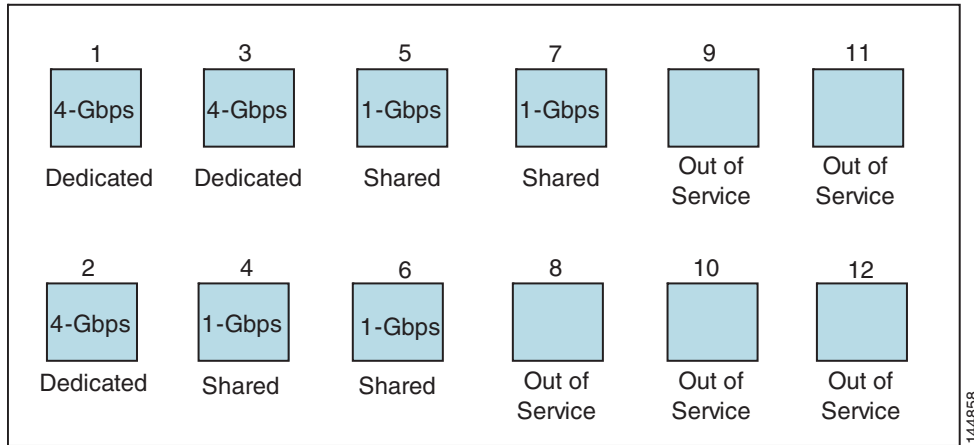
Each port group on the 48-port 4-Gbps Fibre Channel switching module consists of 12 ports. The ports in shared rate mode have bandwidth oversubscription of 2:1 by default. However, some configurations of the shared ports in a port group can have maximum bandwidth oversubscription of 4:1 (considering that each port group has 12.8-Gbps bandwidth).

The following example configurations are supported by the 48-port 4-Gbps Fibre Channel switching modules:

- Twelve ports with shared rate mode and 4-Gbps speed (4:1 oversubscription) (default)
- One port with dedicated rate mode and 4-Gbps speed plus  
11 ports with shared rate mode and 4-Gbps speed (5:1 oversubscription)
- One port with dedicated rate mode and 4-Gbps speed plus  
11 ports with shared rate mode and 2-Gbps speed (2.5:1 oversubscription)
- Two ports with dedicated rate mode and 2-Gbps speed plus  
10 ports with shared rate mode and 4-Gbps speed (5:1 oversubscription)
- Two ports with dedicated rate mode and 2-Gbps speed plus  
10 ports with shared rate mode and 2-Gbps speed (2.5:1 oversubscription)
- Twelve ports with dedicated rate mode and 1-Gbps speed
- Three ports with dedicated rate mode and 4-Gbps speed plus  
four ports with shared rate mode and 1-Gbps speed plus  
five ports put out-of-service (see Figure 6-6)

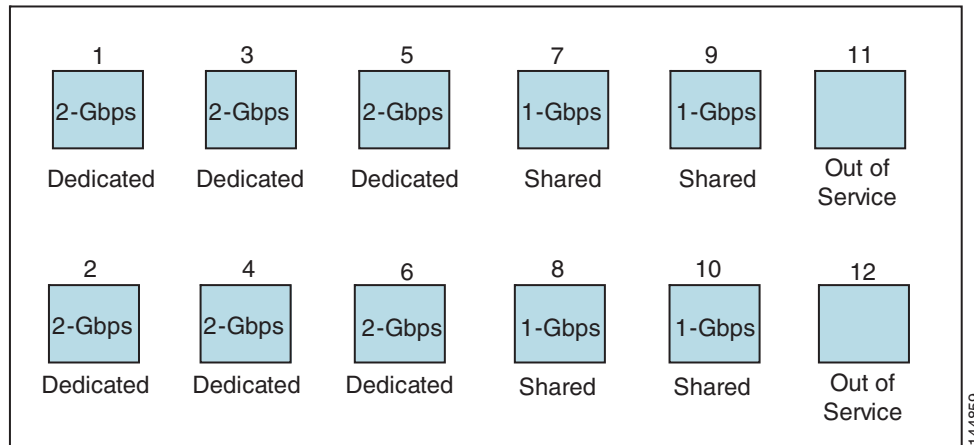
**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 6-6 Example Speed and Rate Configuration on a 48-Port 4-Gbps Switching Module**



- Six ports with dedicated rate mode and 2-Gbps speed plus four ports with shared rate mode and 1-Gbps speed plus two ports put out-of-service (see Figure 6-7)

**Figure 6-7 Example Speed and Rate Configuration on a 48-Port 4-Gbps Switching Module**



## 24-Port 4-Gbps Fibre Channel Module BB\_Credit Buffers

Table 6-5 lists the BB\_credit buffer allocation for 24-port 4-Gbps Fibre Channel switching modules.

**Table 6-5 24-Port 4-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 4-Gbps Speed		Shared Rate Mode 4-Gbps Speed
	ISL <sup>1</sup>	Fx Port	Fx Port
Default BB_credit buffers	250	16	16

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Table 6-5 24-Port 4-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port		
	Dedicated Rate Mode 4-Gbps Speed		Shared Rate Mode 4-Gbps Speed
	ISL <sup>1</sup>	Fx Port	Fx Port
Maximum BB_credit buffers	250	250	16
Total number of BB_credits buffers per module	6000		

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 24-port 4-Gbps Fibre Channel switching modules:

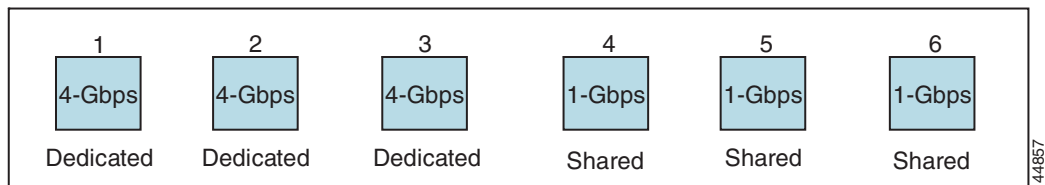
- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- Performance buffers are not supported on this module.

Each port group on the 24-port 4-Gbps Fibre Channel switching module consists of six ports. The ports in shared rate mode have a bandwidth oversubscription of 2:1 by default. However, some configurations of the shared ports in a port group can have a maximum bandwidth oversubscription of 4:1 (considering that each port group has 12.8-Gbps bandwidth).

The following example configurations are supported by the 24-port 4-Gbps Fibre Channel switching modules:

- Six ports with shared rate mode and 4-Gbps speed (2:1 oversubscription) (default)
- Two ports with dedicated rate mode and 4-Gbps speed plus four ports with shared rate mode and 4-Gbps speed (with 4:1 oversubscription)
- One port with dedicated rate mode and 4-Gbps speed plus three ports with dedicated rate mode and 2-Gbps speed plus two ports with shared rate mode and 4-Gbps speed (4:1 oversubscription)
- Six ports with dedicated rate mode and 2-Gbps speed
- Three ports with dedicated rate mode and 4-Gbps speed plus three ports with shared rate mode and 1-Gbps speed (see [Figure 6-8](#))

**Figure 6-8 Example Speed and Rate Configuration on a 24-Port 4-Gbps Switching Module**



## 18-Port Fibre Channel/4-Port Gigabit Ethernet Multiservice Module BB\_Credit Buffers

[Table 6-5](#) lists the BB\_credit buffer allocation for 18-port 4-Gbps multiservice modules.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 6-6 18-Port 4-Gbps Multiservice Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation	BB_Credit Buffers Per Port			
	Dedicated Rate Mode 4-Gbps Speed		Shared Rate Mode 4-Gbps Speed	
	ISL <sup>1</sup>	Fx Port	ISL <sup>1</sup>	Fx Port
Default BB_credit buffers	250	16	16	16
Maximum BB_credit buffers	250	250	16	16
Total number of BB_credit buffers per module	4509			

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 18-port 4-Gbps Fibre Channel switching modules:

- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- BB\_credit buffers for Fx port mode connections can be configured. The minimum is 2 buffers and the maximum of 250 buffers for dedicated rate mode or 16 buffers for shared rate mode.
- Performance buffers are not supported on this module.

## 12-Port 4-Gbps Switching Module BB\_Credit Buffers

Table 6-7 lists the BB\_credit buffer allocation for 12-port 4-Gbps switching modules.

**Table 6-7 12-Port 4-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port	
	Dedicated Rate Mode 4-Gbps Speed	
	ISL <sup>1</sup>	Fx Port
Default BB_credit buffers	250	16
Maximum BB_credit buffers	250	16
Default Performance buffers	145	12
Total number of BB_credit buffers per module	5488	
Total number of performance buffers per module	512 (shared)	

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 12-port 4-Gbps switching modules:

- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 250 buffers.
- BB\_credit buffers for Fx port mode connections can be configured from a minimum of 2 buffers to a maximum of 250 buffers.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- By default, 512 performance buffers are preallocated and are shared by all the ports. These buffers are configurable and the buffers are assigned to the port based on the availability of the buffers in the shared pool.
- There are 2488 extra buffers available as extended BB\_credit buffers after allocating all the default BB\_credit buffers for all the ports in ISL mode (5488 - (250 \* 12)).



**Note**

Extended BB\_credits are allocated across all ports on the switch. That is, they are not allocated by port group.



**Note**

By default, the ports in the 12-port 4-Gbps switching modules come up in 4-Gbps dedicated rate mode but can be configured as 1-Gbps and 2-Gbps dedicated rate mode. Shared mode is not supported.

## 4-Port 10-Gbps Switching Module BB\_Credit Buffers

Table 6-8 lists the BB\_credit buffer allocation for 4-port 10-Gbps switching modules.

**Table 6-8 4-Port 10-Gbps Switching Module BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port	
	Dedicated Rate Mode	
	10-Gbps Speed	
	ISL <sup>1</sup>	F port <sup>2</sup>
Default BB_credit buffers	250	16
Maximum BB_credit buffers	750	16
Maximum BB_credit buffers on one of the ports with Enterprise license	4095	
Total number of BB_credit buffers per module	5488	
Default Performance buffers	145	12
Total number of performance buffers per module	512 (shared)	

1. ISL = E port or TE port.

2. Ports on the 4-port 10-Gbps cannot operate in FL port mode.



**Note**

The ports in the 4-port 10-Gbps switching module only support 10-Gbps dedicated rate mode. FL port mode and shared rate mode are not supported.

The following considerations apply to BB\_credit buffers on 4-port 10-Gbps switching modules:

- BB\_credit buffers for ISL connections can be configured from a minimum of 2 buffers to a maximum of 750 buffers.
- BB\_credit buffers for Fx port mode connections can be configured from a minimum of 2 buffers to a maximum of 750 buffers.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- By default, 512 performance buffers are preallocated and are shared by all the ports. These buffers are configurable and the buffers are assigned to the port based on the availability of the buffers in the shared pool.
- There are 2488 extra buffers available as extended BB\_credits after allocating all the default BB\_credit buffers for all the ports in ISL mode ( $5488 - (750 * 4)$ ).


**Note**

Extended BB\_credits are allocated across all ports on the switch. That is, they are not allocated by port group.

## BB\_Credit Buffers for Fabric Switches

This section describes how buffer credits are allocated to Cisco MDS 9000 Fabric switches, and includes the following topics:

- [Cisco MDS 9148 Fabric Switch BB\\_Credit Buffers, page 6-14](#)
- [Cisco MDS 9148 Fabric Switch BB\\_Credit Buffers, page 6-14](#)
- [Cisco MDS 9124 Fabric Switch BB\\_Credit Buffers, page 6-15](#)
- [Cisco MDS 9222i Multiservice Modular Switch BB\\_Credit Buffers, page 6-15](#)

### Cisco MDS 9148 Fabric Switch BB\_Credit Buffers

[Table 6-9](#) lists the BB\_credit buffer allocation for 48-port 8-Gbps Fibre Channel switches.

**Table 6-9 48-Port 8-Gbps Fabric Switch BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port Group	BB_Credit Buffers Per Port	
		ISL <sup>1</sup>	Fx Port
Default BB_credit buffers	128	32	32
Maximum configurable BB_credit buffers on 8-Gbps mode	128	125	125

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 48-port 8-Gbps Fabric Switches:

- BB\_credit buffers can be configured from a minimum of 1 buffer to a maximum of 32 buffers per port when the ports are in F or FL mode.
- BB\_credit buffers can be configured from a minimum of 2 buffers to a maximum of 32 buffers per port when the ports are in E or TE mode.

### Cisco MDS 9134 Fabric Switch BB\_Credit Buffers

[Table 6-10](#) lists the BB\_credit buffer allocation for 32-port 4-Gbps Fibre Channel switches.



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Table 6-10 32-Port 4-Gbps Fabric Switch BB\_Credit Buffer Allocation**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port Group	BB_Credit Buffers Per Port	
		ISL <sup>1</sup>	Fx Port
User-configurable BB_credit buffers	64	64	64
Default BB_credit buffers on 10-Gbps mode	64	64	64
Default BB_credit buffers on 4-Gbps mode	64	16	16

1. ISL = E port or TE port.

The following considerations apply to BB\_credit buffers on 32-port 4-Gbps switches:

- BB\_credit buffers can be configured from a minimum of 1 buffer to a maximum of 61 buffers per port when the ports are in F mode and in 4-Gbps speed mode.
- BB\_credit buffers can be configured from a minimum of 2 buffers to a maximum of 64 buffers per port when the ports are in auto or E mode and in 4-Gbps speed mode.
- BB\_credit buffers can be configured from a minimum of 64 buffers to a maximum of 64 buffers per port when a port is in 10-Gbps speed mode. There can be only one port per port group configured in 10-Gbps mode. The rest of the three ports must be in down state.
- BB\_credit buffers for Fx port mode connections can be configured from a minimum of 2 buffers to a maximum of 64 buffers.

## Cisco MDS 9124 Fabric Switch BB\_Credit Buffers

Table 6-11 lists the BB\_credit buffer allocation for 24-port 4-Gbps Fibre Channel switches.

**Table 6-11 24-Port 4-Gbps Fabric Switch BB\_Credit Buffer Allocation Defaults**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port Group	BB_Credit Buffers Per Port Defaults	
		ISL <sup>1</sup>	Fx Port
User-configurable BB_credit buffers	64	16	16

1. ISL = E port or TE port.

## Cisco MDS 9222i Multiservice Modular Switch BB\_Credit Buffers

Table 6-12 lists the BB\_credit buffer allocation for 18-port 4-Gbps Multiservice Modular switches.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 6-12 18-Port 4-Gbps Fabric Switch BB\_Credit Buffer Allocation Defaults**

BB_Credit Buffer Allocation Type	BB_Credit Buffers Per Port Group	BB_Credit Buffers Per Port Defaults	
		ISL <sup>1</sup>	Fx Port
User-configurable BB_credit buffers	4509	250	16

1. ISL = E port or TE port.

## About Extended BB\_Credits

To facilitate BB\_credits for long-haul links, the extended BB\_credits feature allows you to configure the receive buffers above the maximum value on all Generation 2 and Generation 3 switching modules. When necessary, you can reduce the buffers on one port and assign them to another port, exceeding the default maximum. The minimum extended BB\_credits per port is 256 and the maximum is 4095.



### Note

Extended BB\_credits are not supported on the Cisco MDS 9148 Fabric Switch, Cisco MDS 9134 Fabric Switch, Cisco MDS 9124 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

In general, you can configure any port in a port group to dedicated rate mode. To do this, you must first release the buffers from the other ports before configuring larger extended BB\_credits for a port.



### Note

The ENTERPRISE\_PKG license is required to use extended BB\_credits on Generation 2 and Generation 3 switching modules. Also, extended BB\_credits are not supported by ports in shared rate mode.

All ports on the Generation 2 and Generation 3 switching modules support extended BB\_credits. There are no limitations for how many extended BB\_credits you can assign to a port (except for the maximum and minimum limits). If necessary, you can take interfaces out of service to make more extended BB\_credits available to other ports.

You can use the extended BB\_credits flow control mechanism in addition to BB\_credits for long-haul links.

This section includes the following topics:

- [Extended BB\\_credits on Generation 1 Switching Modules, page 6-16](#)
- [Extended BB\\_credits on Generation 2 and Generation 3 Switching Modules, page 6-17](#)

## Extended BB\_credits on Generation 1 Switching Modules

The BB\_credits feature allows you to configure up to 255 receive buffers on Generation 1 switching modules. To facilitate BB\_credits for long haul links, you can configure up to 3,500 receive BB\_credits on a Fibre Channel port on a Generation 1 switching module.

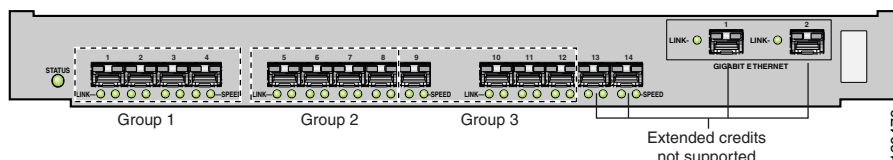
To use this feature on Generation 1 switching modules, you must meet the following requirements:

- Obtain the ENTERPRISE\_PKG license. See the *Cisco MDS 9000 Family NX-OS Licensing Guide*.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Configure this feature in any port of the full-rate 4-port group in either the Cisco MDS 9216i Switch or in the MPS-14/2 module (see Figure 6-9).

**Figure 6-9 Port Group Support for the Extended BB\_Credits Feature**



The port groups that support extended credit configurations are as follows:

- Any one port in ports 1 to 4 (identified as Group 1).
- Any one port in ports 5 to 8 (identified as Group 2).
- Any one port in ports 9 to 12 (identified as Group 3).



**Note** The last two Fibre Channel ports (port 13 and port 14) and the two Gigabit Ethernet ports do not support the extended BB\_credits feature.

- Explicitly enable this feature in the required Cisco MDS switch.
- Disable the remaining three ports in the 4-port group if you need to assign more than 2,400 BB\_credits to the first port in the port group.
  - If you assign less than 2,400 extended BB\_credits to any one port in a port group, the remaining three ports in that port group can retain up to 255 BB\_credits based on the port mode.



**Note** The receive BB\_credit value for the remaining three ports depends on the port mode. The default value is 16 for the Fx mode and 255 for E or TE modes. The maximum value is 255 in all modes. This value can be changed as required without exceeding the maximum value of 255 BB\_credits.

- If you assign more than 2,400 (up to a maximum of 3,500) extended BB\_credits to the port in a port group, you must disable the other three ports.
- Be aware that changing the BB\_credit value results in the port being disabled and then reenabled.
- Disable (explicitly) this feature if you need to nondisruptively downgrade to Cisco SAN-OS Release 1.3 or earlier. When you disable this feature, the existing extended BB\_credit configuration is completely erased.



**Note**

The extended BB\_credit configuration takes precedence over the receive BB\_credit and performance buffer configurations.

## Extended BB\_credits on Generation 2 and Generation 3 Switching Modules

To use this feature on Generation 2 or Generation 3 switching modules, you must meet the following requirements:

- Display the interface configuration in the Information pane.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- Obtain the Enterprise package (ENTERPRISE\_PKG) license (see the *NX-OS Family Licensing Guide*).
- Configure this feature in any port on a Generation 2 switch module. See the “[About Extended BB\\_Credits](#)” section on page 6-16 for more information on extended BB\_credits on Generation 2 switching modules.

**Note**

Extended BB\_credits are not supported on the Cisco MDS 9124 Fabric Switch, Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

## Configuring Extended BB\_credits

To configure extended BB\_credits for an MDS-14/2 interface, for a Generation 2 switching module interface, or for an interface in a Cisco MDS 9216i switch using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
- Step 2** Click the **BB Credit** tab.
- Step 3** In the **Extended** column, set the extended BB\_credits for the selected interface.
- Step 4** Click **Apply Changes**.
-

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Enabling Buffer-to-Buffer Credit Recovery

Although the Fibre Channel standards require low bit error rates, bit errors do occur. Over time, the corruption of receiver-ready messages, known as R\_RDY primitives, can lead to a loss of credits, which can eventually cause a link to stop transmitting in one direction. The Fibre Channel standards provide a feature for two attached ports to detect and correct this situation. This feature is called buffer-to-buffer credit recovery.

Buffer-to-buffer credit recovery functions as follows: the sender and the receiver agree to send checkpoint primitives to each other, starting from the time that the link comes up. The sender sends a checkpoint every time it has sent the specified number of frames, and the receiver sends a checkpoint every time it has sent the specified number of R\_RDY primitives. If the receiver detects lost credits, it can retransmit them and restore the credit count on the sender.

The buffer-to-buffer credit recovery feature can be used on any nonarbitrated loop link. This feature is most useful on unreliable links, such as MANs or WANs, but can also help on shorter, high-loss links, such as a link with a faulty fiber connection.



### Note

The buffer-to-buffer credit recovery feature is not compatible with distance extension (DE) feature, also known as buffer-to-buffer credit spoofing. If you use intermediate optical equipment, such as DWDM transceivers or Fibre Channel bridges, on ISLs between switches that use DE, then buffer-to-buffer credit recovery on both sides of the ISL needs to be disabled.

Buffer-to-buffer credit recovery on ISLs (E or TE ports) is enabled by default.

## About Receive Data Field Size

You can also configure the receive data field size for Fibre Channel interfaces. If the default data field size is 2112 bytes, the frame length will be 2148 bytes.

## Configuring Receive Data Field Size

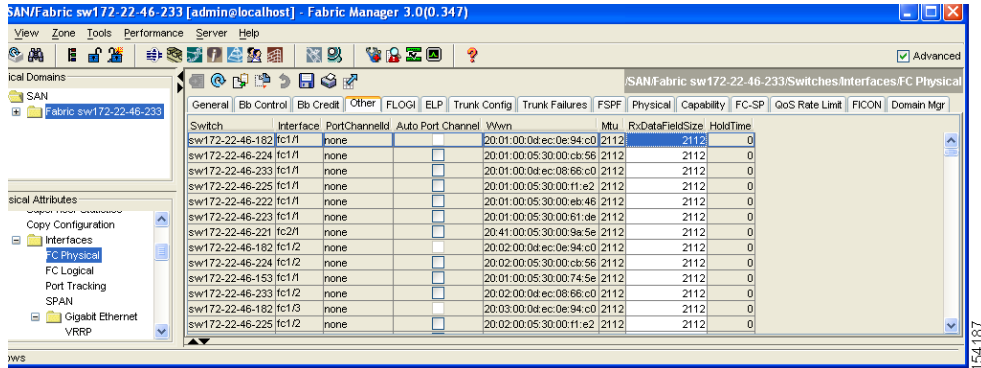
You can also configure the receive data field size for Fibre Channel interfaces. If the default data field size is 2112 bytes, the frame length will be 2148 bytes.

To configure the receive data field size using Fabric Manager, follow these steps:

- 
- Step 1** Expand **Switches > Interfaces** and then select **FC Physical**.  
You see the interface configuration in the Information pane.
  - Step 2** Click the **Other** tab and set the RxDataFieldSize field (see [Figure 6-10](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 6-10 Changing Rx Data Size**



**Step 3** (Optional) Set other configuration parameters using the other tabs.

**Step 4** Click **Apply Changes**.



## CHAPTER 7

# Configuring Trunking

---

This chapter describes the trunking feature provided in Cisco MDS 9000 switches. It includes the following sections:

- [About Trunking, page 7-1](#)
- [Trunking Guidelines and Restrictions, page 7-3](#)
- [Configuring Trunk Mode and VSAN List, page 7-7](#)
- [Default Settings, page 7-11](#)

## About Trunking

Trunking, also known as VSAN trunking, is a feature specific to switches in the Cisco MDS 9000 Family. Trunking enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link. Trunking is supported on E ports and F ports (See [Figure 7-1](#) and [Figure 7-2](#)).

This section includes the following topics:

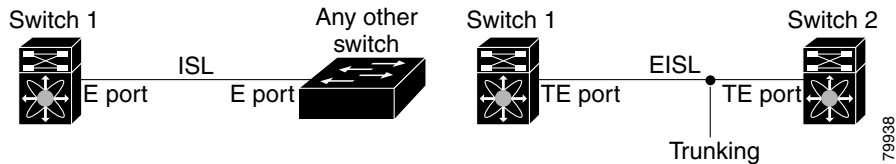
- [Trunking E Ports, page 7-2](#)
- [Trunking F Ports, page 7-2](#)
- [Key Concepts, page 7-3](#)
- [Trunking Misconfiguration Examples, page 7-4](#)
- [Upgrade and Downgrade Restrictions, page 7-5](#)
- [Difference Between TE Ports and TF-TNP Ports, page 7-5](#)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

## Trunking E Ports

Trunking the E ports enables interconnect ports to transmit and receive frames in more than one VSAN, over the same physical link, using enhanced ISL (EISL) frame format.

**Figure 7-1 Trunking E Ports**



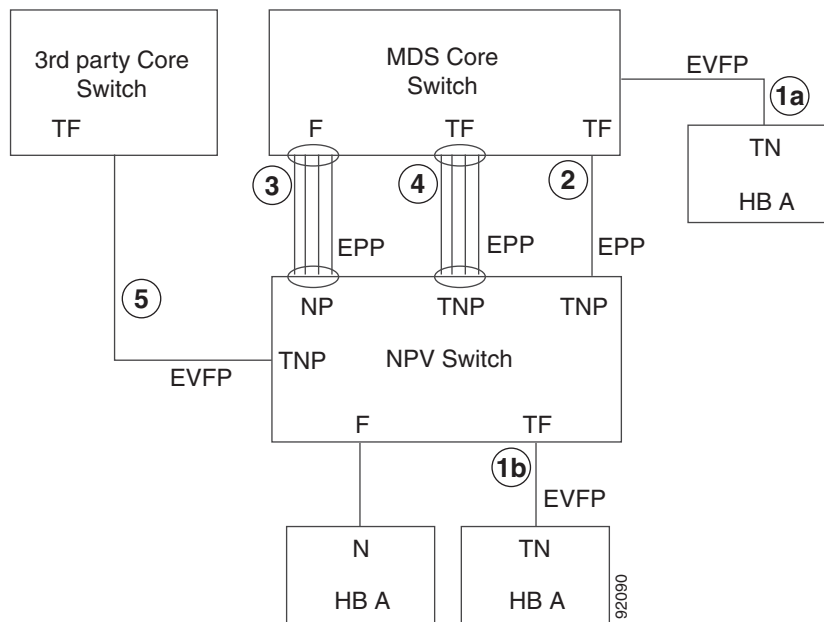
### Note

Trunking is not supported by internal ports on both the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter.

## Trunking F Ports

Trunking F ports allows interconnected ports to transmit and receive tagged frames in more than one VSAN, over the same physical link. Figure 7-2 represents the possible trunking scenarios in a SAN with MDS core switches, NPV switches, third-party core switches, and HBAs.

**Figure 7-2 Trunking F Ports**





***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Link Number	Link Description
1a and 1b	F port trunk with N port. <sup>1</sup>
2	F port trunk with NP port.
3	F PortChannel with NP port.
4	Trunked F PortChannel with NP port.
5	Trunking NP port with third-party core switch F port. <sup>1</sup>

1. These features are not supported currently.

## Key Concepts

The trunking feature includes the following key concepts:

- **TE port**—If trunk mode is enabled in an E port and that port becomes operational as a trunking E port, it is referred to as a TE port.
- **TF port**—If trunk mode is enabled in an F port (see the link 2 in [Figure 7-2](#)) and that port becomes operational as a trunking F port, it is referred to as a TF port.
- **TN port**—If trunk mode is enabled (not currently supported) in an N port (see the link 1b in [Figure 7-2](#)) and that port becomes operational as a trunking N port, it is referred to as a TN port.
- **TNP port**—If trunk mode is enabled in an NP port (see the link 2 in [Figure 7-2](#)) and that port becomes operational as a trunking NP port, it is referred to as a TNP port.
- **TF PortChannel**—If trunk mode is enabled in an F PortChannel (see the link 4 in [Figure 7-2](#)) and that PortChannel becomes operational as a trunking F PortChannel, it is referred to as TF PortChannel. Cisco Port Trunking Protocol (PTP) is used to carry tagged frames.
- **TF-TN port link**—A single link can be established to connect an F port to an HBA to carry tagged frames (see the link 1a and 1b in [Figure 7-2](#)) using Exchange Virtual Fabrics Protocol (EVFP). A server can reach multiple VSANs through a TF port without inter-VSAN routing (IVR).
- **TF-TNP port link**—A single link can be established to connect an TF port to an TNP port using the PTP protocol to carry tagged frames (see the link 2 in [Figure 7-2](#)). PTP is used because PTP also supports trunking PortChannels.



**Note** The TF-TNP port link between a third-party NPV core and a Cisco NPV switch is established using the EVFP protocol.

- A Fibre Channel VSAN is called Virtual Fabric and uses a VF\_ID in place of the VSAN ID. By default, the VF\_ID is 1 for all ports. When an N port supports trunking, a PWWN is defined for each VSAN and called as logical PWWN. In the case of MDS core switches, the PWWNs for which the N port requests additional FC\_IDs are called virtual PWWNs.

## Trunking Guidelines and Restrictions

The trunking feature includes the following guidelines and restrictions:

- F ports support trunking in Fx mode.

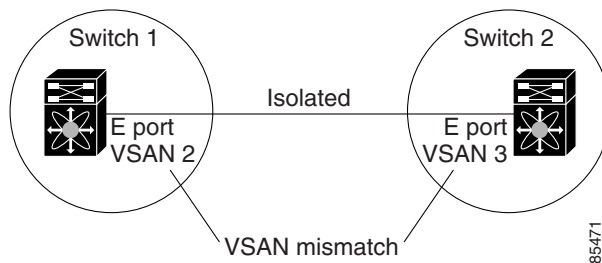
***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- The trunk-allowed VSANs configured for TE, TF, and TNP links are used by the trunking protocol to determine the allowed active VSANs in which frames can be received or transmitted.
- If a trunking enabled E port is connected to a third-party switch, the trunking protocol ensures seamless operation as an E port.
- Trunking F ports and trunking F PortChannels are not supported on the following hardware:
  - 91x4 switches, if NPIV is enabled and used as the NPIV core switch.
  - Generation 1 2-Gbps Fibre Channel switching modules.
- On core switches, the FC-SP authentication will be supported only for the physical FLOGI from the physical PWWN.
- No FC-SP authentication is supported by the NPV switch on the server F ports.
- MDS does not enforce the uniqueness of logical PWWNs across VSANs.
- DPVM is not supported on trunked F port logins.
- The DPVM feature is limited to the control of the port VSAN, since the EVFP protocol does not allow changing the VSAN on which a logical PWWN has done FLOGI.
- The port security configuration will be applied to both the first physical FLOGI and the per VSAN FLOGIs.
- Trunking is not supported on F ports that have FlexAttach enabled.
- On MDS 91x4 core switches, hard zoning can be done only on F ports that are doing either NPIV or trunking. However, in NPV mode, this restriction does not apply since zoning is enforced on the core F port.

## Trunking Misconfiguration Examples

If you do not configure the VSANs correctly, issues with the connection may occur. For example, if you merge the traffic in two VSANs, both VSANs will be mismatched. The trunking protocol validates the VSAN interfaces at both ends of a link to avoid merging VSANs (see [Figure 7-3](#)).

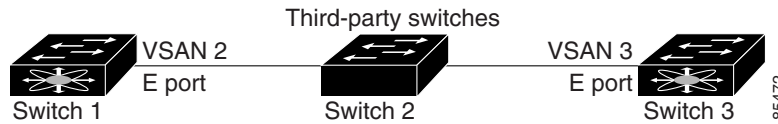
**Figure 7-3 VSAN Mismatch**



The trunking protocol detects potential VSAN merging and isolates the ports involved (see [Figure 7-3](#)). The trunking protocol cannot detect merging of VSANs when a third-party switch is placed in between two Cisco MDS 9000 Family switches (see [Figure 7-4](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 7-4 Third-Party Switch VSAN Mismatch**



VSAN 2 and VSAN 3 are effectively merged with overlapping entries in the name server and the zone applications. The Cisco MDS 9000 Fabric Manager helps detect such topologies.

## Upgrade and Downgrade Restrictions

The trunking and channeling feature includes the following upgrade and downgrade restrictions:

- When F port trunking or channeling is configured on a link, the switch cannot be downgraded to Cisco MDS SAN-OS Release 3.x and NX-OS Release 4.1(1b), or earlier.
- If you are upgrading from a SAN-OS Release 3.x to NX-OS Release 5.0(1), and you have not created VSAN 4079, the NX-OS software will automatically create VSAN 4079 and reserve it for EVFP use.

If you have created VSAN 4079, the upgrade to NX-OS Release 5.0(1) will have no affect on VSAN 4079.

If you downgrade after NX-OS Release 5.0(1) creates VSAN 4079 and reserves it for EVFP use, the VSAN will no longer be reserved.

## Difference Between TE Ports and TF-TNP Ports

In case of TE ports, the VSAN will in be initializing state when VSAN is coming up on that interface and when peers are in negotiating phase. Once the handshake is done, VSAN will be moved to up state in the successful case, and isolated state in the case of failure. Device Manager will show the port status as amber during initializing state and it will be green once VSANs are up.

In case of TF ports, after the handshake, one of the allowed VSAN will be moved to up state. And all other VSAN will be in initializing state even though the handshake with the peer is completed and successful. Each VSAN will be moved from initializing state to up state when a server or target logs in through the trunked F or NP ports in the corresponding VSAN.



### Note

In case of TF or TNP ports, the Device Manager will show the port status as amber even after port is up and there is no failure. It will be changed to green once all the VSAN has successful logins.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Enabling the Trunking Protocols

This section explains how to enable or disable the required trunking and channeling protocols represented in [Figure 7-2](#) and includes the following topics:

- [About Trunking Protocols, page 7-6](#)
- [Enabling the F Port Trunking and Channeling Protocol, page 7-7](#)

## About Trunking Protocols

The trunking protocol is important for trunking operations on the ports. The protocols enable the following activities:

- Dynamic negotiation of operational trunk mode.
- Selection of a common set of trunk-allowed VSANs.
- Detection of a VSAN mismatch across an ISL.

[Table 7-1](#) specifies the protocols used for trunking and channeling.

**Table 7-1 Supported Trunking Protocols**

Trunk Link	Default
TE-TE port link	Cisco EPP (PTP)
TF-TN port link <sup>1</sup>	FC-LS Rev 1.62 EVFP
TF-TNP port link	Cisco EPP (PTP)
E or F PortChannel	Cisco EPP (PCP)
TF Port Channel	Cisco EPP (PTP and PCP)
Third-party TF-TNP port link <sup>1</sup>	FC-LS Rev 1.62 EVFP

1. These features are not currently supported.

By default, the trunking protocol is enabled on E ports and disabled on F ports. If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected. The TE port continues to function in trunk mode, but only supports traffic in VSANs that it negotiated with previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, disable the trunking protocol.



### Note

We recommend that both ends of a trunking link belong to the same port VSAN. On certain switches or fabric switches where the port VSANs are different, one end returns an error and the other end is not connected.



### Tip

To avoid inconsistent configurations, shut all ports before enabling or disabling the trunking protocols.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Enabling the F Port Trunking and Channeling Protocol



### Note

The trunking protocols must be enabled to support trunking, and NPIV must be enabled on the core switch to activate a TF-TNP link. To enable NPIV, use the **feature npiv** command.

To enable or disable the F port trunking and channeling protocols using the Fabric Manager, follow these steps:

- 
- Step 1** From the Physical Interfaces panel, expand **Switches** and then select **F\_Port\_Channel/Trunk**.  
You see the list of switches in the Fabric with F port trunking and channeling enabled.
- Step 2** From the Status column, select **enable** or **disable**.
- 

## Configuring Trunk Mode and VSAN List

This section includes the following topics:

- [About Trunk Modes, page 7-7](#)
- [Configuring Trunk Mode, page 7-8](#)
- [About Trunk-Allowed VSAN Lists and VF\\_IDs, page 7-9](#)
- [Configuring an Allowed-Active List of VSANs, page 7-11](#)

## About Trunk Modes

By default, trunk mode is enabled on all Fibre Channel interfaces (Mode: E, F, FL, Fx, ST, and SD) on non-NPV switches. On NPV switches, by default, trunk mode is disabled. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The trunk mode configuration at the two ends of an ISL, between two switches, determine the trunking state of the link and the port modes at both ends (see [Table 7-2](#)).

**Table 7-2 Trunk Mode Status Between Switches**

Your Trunk Mode Configuration			Resulting State and Port Mode	
Port Type	Switch 1	Switch 2	Trunking State	Port Mode
E ports	On	Auto or on	Trunking (EISL)	TE port
	Off	Auto, on, or off	No trunking (ISL)	E port
	Auto	Auto	No trunking (ISL)	E port
Port Type	Core Switch	NPV Switch	Trunking State	Link Mode
F and NP ports	On	Auto or on	Trunking	TF-TNP link
	Auto	On	Trunking	TF-TNP link
	Off	Auto, on, or off	No trunking	F-NP link

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Tip**

The preferred configuration on the Cisco MDS 9000 Family switches is one side of the trunk set to auto and the other side set to on.

**Note**

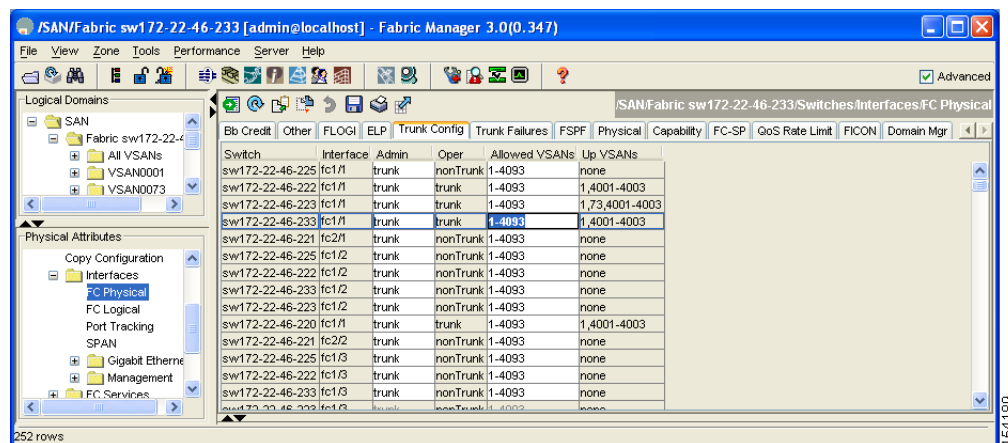
When connected to a third-party switch, the trunk mode configuration on E ports has no effect. The ISL is always in a trunking disabled state. In the case of F ports, if the third-party core switch ACC's physical FLOGI with the EVFP bit is configured, then EVFP protocol enables trunking on the link.

## Configuring Trunk Mode

To configure trunk mode using Fabric Manager, follow these steps:

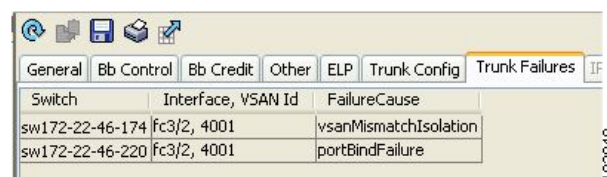
- Step 1** Expand **Interfaces** and then select **FC Physical**. You see the interface configuration in the Information pane.
- Step 2** Click the **Trunk Config** tab to modify the trunking mode for the selected interface. You see the information shown in [Figure 7-5](#).

**Figure 7-5 Trunking Configuration**



- Step 3** Make changes to the Admin and Allowed VSANs values.
- Step 4** Click the **Trunk Failures** tab to check if a link did not come up. You see the reason listed in the FailureCause column (see [Figure 7-6](#)).

**Figure 7-6 Trunk Failures Tab**



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 5** Click the **Apply Changes** icon.

## About Trunk-Allowed VSAN Lists and VF\_IDs

Each Fibre Channel interface has an associated trunk-allowed VSAN list. In TE-port mode, frames are transmitted and received in one or more VSANs specified in this list. By default, the VSAN range (1 through 4093) is included in the trunk-allowed list.

The common set of VSANs that are configured and active in the switch are included in the trunk-allowed VSAN list for an interface, and they are called *allowed-active* VSANs. The trunking protocol uses the list of allowed-active VSANs at the two ends of an ISL to determine the list of operational VSANs in which traffic is allowed.

Switch 1 (see [Figure 7-7](#)) has VSANs 1 through 5, switch 2 has VSANs 1 through 3, and switch 3 has VSANs 1, 2, 4, and 5 with a default configuration of trunk-allowed VSANs. All VSANs configured in all three switches are allowed-active. However, only the common set of allowed-active VSANs at the ends of the ISL become operational (see [Figure 7-7](#)).

For all F, N, and NP ports, the default VF\_ID is 1 when there is no VF\_ID configured. The trunk-allowed VF\_ID list on a port is same as the list of trunk-allowed VSANs. VF\_ID 4094 is called the control VF\_ID and it is used to define the list of trunk-allowed VF-IDs when trunking is enabled on the link.

If F port trunking and channeling is enabled, or if **switchport trunk mode on** is configured in NPV mode for any interface, or if NP PortChannel is configured, the VSAN and VF-ID ranges available for the configuration are as described in [Table 7-3](#).

**Table 7-3 VSAN and VF-ID Reservations**

VSAN or VF-ID	Description
000h	Cannot be used as virtual fabric identifier.
001h(1) to EFFh(3839)	This VSAN range is available for user configuration.
F00h(3840) to FEEh(4078)	Reserved VSANs and they are not available for user configuration.
FEFh(4079)	EVFP isolated VSAN.
FF0h(4080) to FFEh(4094)	Used for vendor-specific VSANs.
FFFh	Cannot be used as virtual fabric identifier.

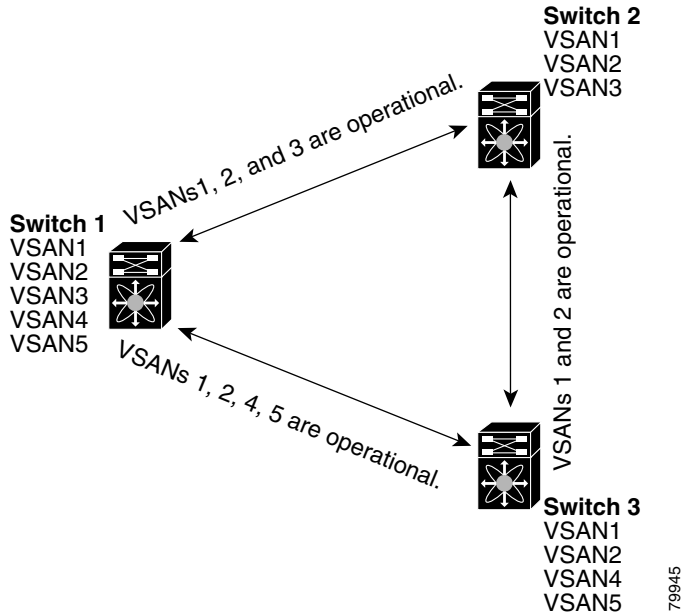


**Note**

If the VF\_ID of the F port and the N port do not match, then no tagged frames can be exchanged.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 7-7 Default Allowed-Active VSAN Configuration**



You can configure a select set of VSANs (from the allowed-active list) to control access to the VSANs specified in a trunking ISL.

Using [Figure 7-7](#) as an example, you can configure the list of allowed VSANs on a per-interface basis (see [Figure 7-8](#)). For example, if VSANs 2 and 4 are removed from the allowed VSAN list of ISLs connecting to switch 1, the operational allowed list of VSANs for each ISL would be as follows:

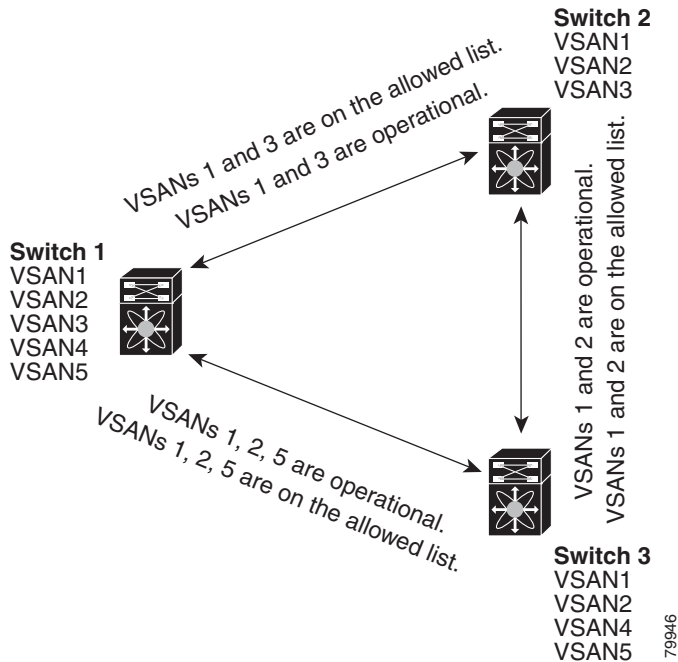
- The ISL between switch 1 and switch 2 includes VSAN 1 and VSAN 3.
- The ISL between switch 2 and switch 3 includes VSAN 1 and VSAN 2.
- The ISL between switch 3 and switch 1 includes VSAN 1, 2, and 5.

Consequently, VSAN 2 can only be routed from switch 1 through switch 3 to switch 2.



[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

**Figure 7-8** Operational and Allowed VSAN Configuration



## Configuring an Allowed-Active List of VSANs

To configure an allowed-active list of VSANs for an interface using Fabric Manager, follow these steps:

- Step 1** Expand **Interfaces** and then select **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** Click the **Trunk Config** tab.  
You see the current trunk configuration.
- Step 3** Set Allowed VSANs to the list of allowed VSANs for each interface that you want to configure.
- Step 4** Click **Apply Changes** to save these changes or click **Undo Changes** to discard any unsaved changes.

## Default Settings

Table 7-4 lists the default settings for trunking parameters.

**Table 7-4** Default Trunk Configuration Parameters

Parameters	Default
Switch port trunk mode	ON on non-NPV and MDS core switches. OFF on NPV switches.
Allowed VSAN list	1 to 4093 user-defined VSAN IDs.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 7-4**      ***Default Trunk Configuration Parameters (continued)***

Parameters	Default
Allowed VF-ID list	1 to 4093 user-defined VF-IDs.
Trunking protocol on E ports	Enabled.
Trunking protocol on F ports	Disabled.



## CHAPTER 8

# Configuring PortChannels

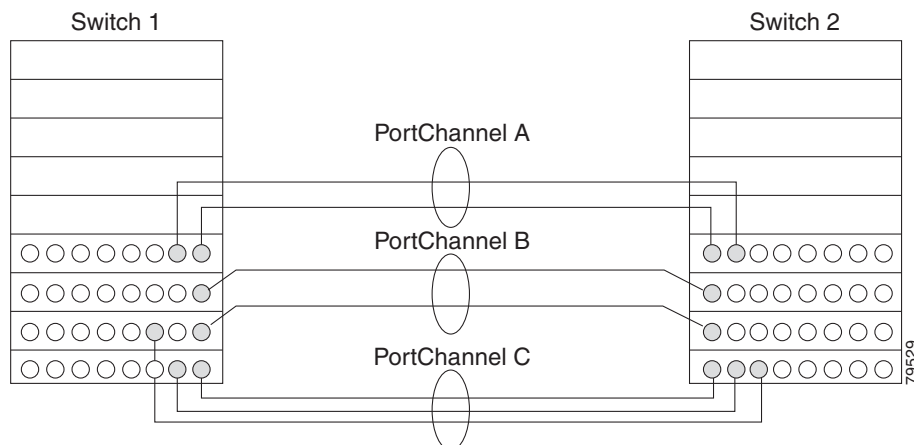
This chapter discusses the PortChannel feature provided in the switch and includes the following sections:

- [About PortChannels, page 8-1](#)
- [PortChannel Configuration, page 8-9](#)
- [Interfaces in a PortChannel, page 8-17](#)
- [PortChannel Protocols, page 8-20](#)
- [Verifying the PortChannel Configuration, page 8-24](#)
- [Default Settings, page 8-25](#)

## About PortChannels

PortChannels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy (See [Figure 8-1](#)). PortChannels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the PortChannel link.

**Figure 8-1** PortChannel Flexibility



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

PortChannels on Cisco MDS 9000 Family switches allow flexibility in configuration. This illustrates three possible PortChannel configurations:

- PortChannel A aggregates two links on two interfaces on the same switching module at each end of a connection.
- PortChannel B also aggregates two links, but each link is connected to a different switching module. If the switching module goes down, traffic is not affected.
- PortChannel C aggregates three links. Two links are on the same switching module at each end, while one is connected to a different switching module on switch 2.

This section contains the following topics:

- [About E PortChannels, page 8-2](#)
- [About F and TF PortChannels, page 8-3](#)
- [About PortChanneling and Trunking, page 8-3](#)
- [About Load Balancing, page 8-4](#)
- [About PortChannel Modes, page 8-6](#)
- [Configuration Guidelines and Restrictions, page 8-7](#)

## About E PortChannels

An E PortChannel refers to the aggregation of multiple E ports into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. PortChannels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the PortChannel link.

A PortChannel has the following features and restrictions:

- Provides a point-to-point connection over ISL (E ports) or EISL (TE ports). Multiple links can be combined into a PortChannel.
- Increases the aggregate bandwidth on an ISL by distributing traffic among all functional links in the channel.
- Load balances across multiple links and maintains optimum bandwidth utilization. Load balancing is based on the source ID, destination ID, and exchange ID (OX ID).
- Provides high availability on an ISL. If one link fails, traffic previously carried on this link is switched to the remaining links. If a link goes down in a PortChannel, the upper protocol is not aware of it. To the upper protocol, the link is still there, although the bandwidth is diminished. The routing tables are not affected by link failure. PortChannels may contain up to 16 physical links and may span multiple modules for added high availability.



### Note

See the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide* for information about failover scenarios for PortChannels and FSPF links.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

## About F and TF PortChannels

An F PortChannel is also a logical interface that combines a set of F ports connected to the same Fibre Channel node and operates as one link between the F ports and the NP ports. The F port channels support bandwidth utilization and availability like the E port channels. F PortChannels are mainly used to connect MDS core and NPV switches to provide optimal bandwidth utilization and transparent failover between the uplinks of a VSAN.

An F PortChannel trunk combines the functionality and advantages of a TF port and an F PortChannel. This logical link uses the Cisco PTP and PCP protocols over Cisco EPP (ELS).



### Note

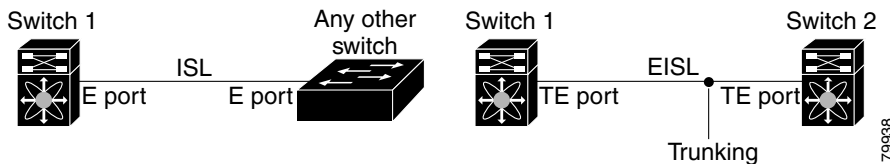
If a Cisco MDS 9124 or 9134 switch is used as a core switch, only a nontrunking F PortChannel is supported. Trunking is not supported on this platform when NPIV enabled.

## About PortChanneling and Trunking

Trunking is a commonly used storage industry term. However, the Cisco NX-OS software and switches in the Cisco MDS 9000 Family implement trunking and PortChanneling as follows:

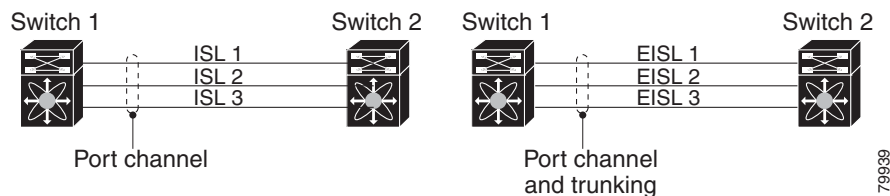
- PortChanneling enables several physical links to be combined into one aggregated logical link.
- Trunking enables a link transmitting frames in the EISL format to carry (trunk) multiple VSAN traffic. For example, when trunking is operational on an E port, that E port becomes a TE port. A TE port is specific to switches in the Cisco MDS 9000 Family. An industry standard E port can link to other vendor switches and is referred to as a nontrunking interface (See [Figure 8-2](#) and [Figure 8-3](#)). See [Chapter 7, “Configuring Trunking,”](#) for information on trunked interfaces.

**Figure 8-2 Trunking Only**



PortChanneling and trunking are used separately across an ISL:

**Figure 8-3 PortChanneling and Trunking**



- PortChanneling—Interfaces can be channelled between the following sets of ports:
  - E ports and TE ports
  - F ports and NP ports

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- TF ports and TNP ports
- Trunking—Trunking permits carrying traffic on multiple VSANs between switches. See the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.
- Both PortChanneling and trunking can be used between TE ports over EISLs.

## About Load Balancing

Two mechanisms support the load balancing functionality:

- Flow based—All frames between source and destination follow the same links for a given flow. That is, whichever link is selected for the first exchange of the flow is used for all subsequent exchanges.
- Exchange based—The first frame in an exchange picks a link and subsequent frames in the exchange follow the same link. However, subsequent exchanges can use a different link. This provides more granular load balancing while preserving the order of frames for each exchange.

Figure 8-4 illustrates how source ID 1 (SID1) and destination ID1 (DID1) based load balancing works. When the first frame in a flow is received on an interface for forwarding, link 1 is selected. Each subsequent frame in that flow is sent over the same link. No frame in SID1 and DID1 utilizes link 2.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-4 SID1 and DID1 Based Load Balancing**

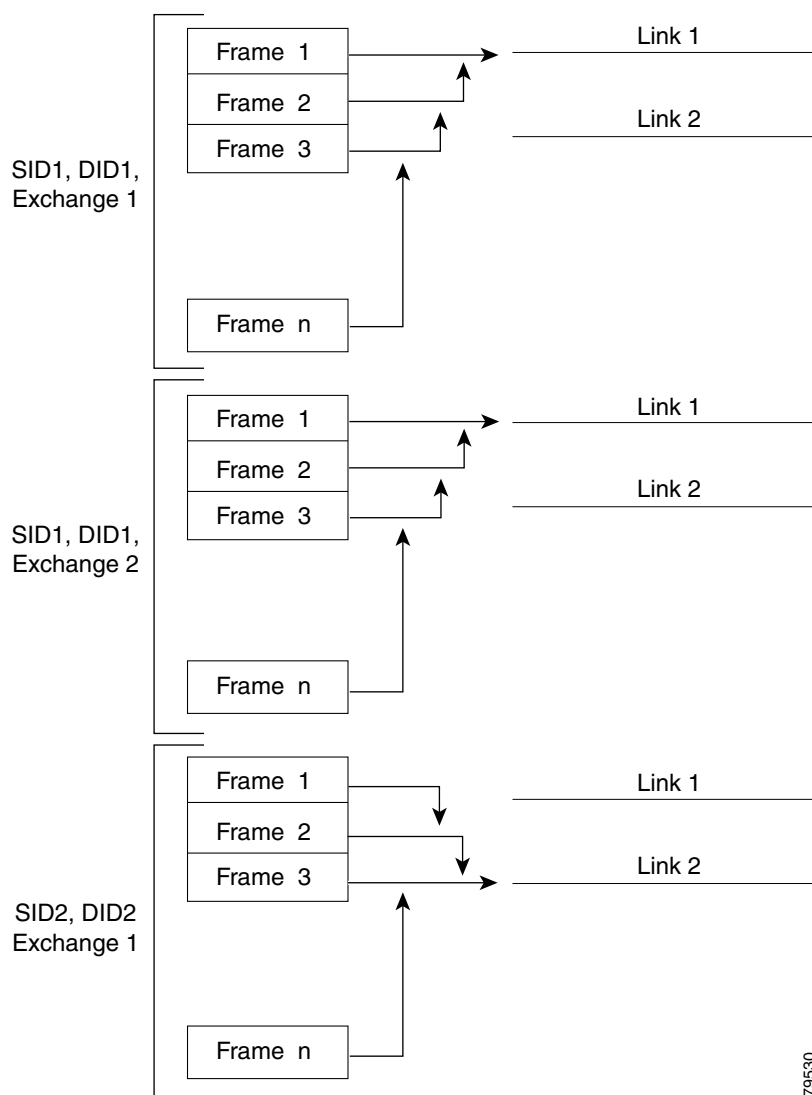
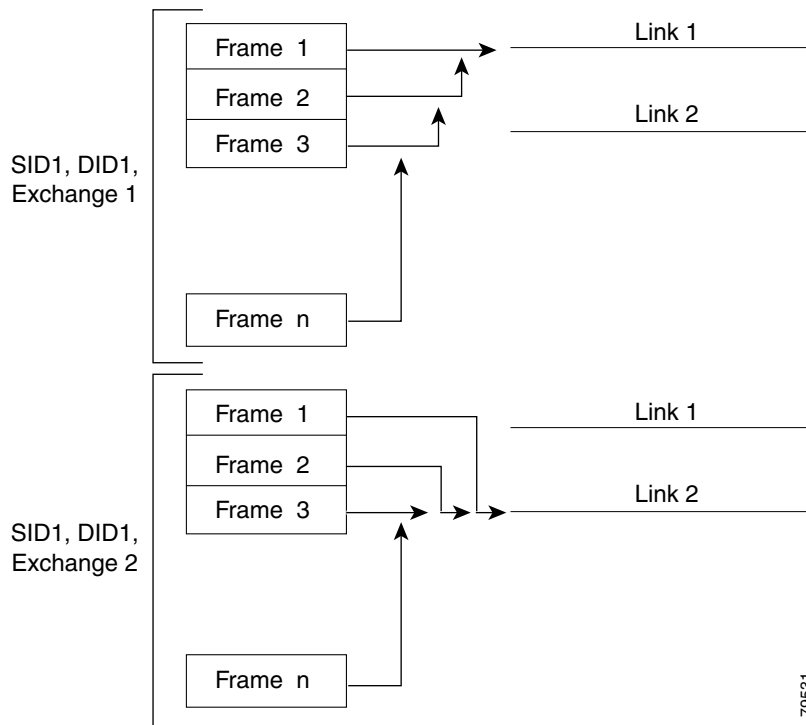


Figure 8-5 illustrates how exchange-based load balancing works. When the first frame in an exchange is received for forwarding on an interface, link 1 is chosen by a hash algorithm. All remaining frames in that particular exchange are sent on the same link. For exchange 1, no frame uses link 2. For the next exchange, link 2 is chosen by the hash algorithm. Now all frames in exchange 2 use link 2.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-5 SID1, DID1, and Exchange Based Load Balancing**



For more information on configuring load balancing and in-order delivery features, see the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.

## About PortChannel Modes

You can configure each PortChannel with a channel group mode parameter to determine the PortChannel protocol behavior for all member ports in this channel group. The possible values for a channel group mode are as follows:

- **ON (default)**—The member ports only operate as part of a PortChannel or remain inactive. In this mode, the PortChannel protocol is not initiated. However, if a PortChannel protocol frame is received from a peer port, the software indicates its nonnegotiable status. This mode is backward compatible with the existing implementation of PortChannels in releases prior to Release 2.0(1b), where the channel group mode is implicitly assumed to be ON. In Cisco MDS SAN-OS Releases 1.3 and earlier, the only available PortChannel mode was the ON mode. PortChannels configured in the ON mode require you to explicitly enable and disable the PortChannel member ports at either end if you add or remove ports from the PortChannel configuration. You must physically verify that the local and remote ports are connected to each other.
- **ACTIVE**—The member ports initiate PortChannel protocol negotiation with the peer port(s) regardless of the channel group mode of the peer port. If the peer port, while configured in a channel group, does not support the PortChannel protocol, or responds with a nonnegotiable status, it will default to the ON mode behavior. The ACTIVE PortChannel mode allows automatic recovery without explicitly enabling and disabling the PortChannel member ports at either end.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Table 8-1 compares ON and ACTIVE modes.

**Table 8-1 Channel Group Configuration Differences**

<b>ON Mode</b>	<b>ACTIVE Mode</b>
No protocol is exchanged.	A PortChannel protocol negotiation is performed with the peer ports.
Moves interfaces to the suspended state if its operational values are incompatible with the PortChannel.	Moves interfaces to the isolated state if its operational values are incompatible with the PortChannel.
When you add or modify a PortChannel member port configuration, you must explicitly disable (shut) and enable (no shut) the PortChannel member ports at either end.	When you add or modify a PortChannel interface, the PortChannel automatically recovers.
Port initialization is not synchronized.	There is synchronized startup of all ports in a channel across peer switches.
All misconfigurations are not detected as no protocol is exchanged.	Consistently detect misconfigurations using a PortChannel protocol.
Transitions misconfigured ports to the suspended state. You must explicitly disable (shut) and enable (no shut) the member ports at either end.	Transitions misconfigured ports to the isolated state to correct the misconfiguration. Once you correct the misconfiguration, the protocol ensures automatic recovery.
This is the default mode.	You must explicitly configure this mode.

## Configuration Guidelines and Restrictions

Cisco MDS 9000 Family switches support the following number of PortChannels per switch:

- Switches with only Generation 1 switching modules do not support F and TF PortChannels.
- Switches with Generation 1 switching modules, or a combination of Generation 1 and Generation 2 switching modules, support a maximum of 128 PortChannels. Only Generation 2 ports can be included in the PortChannels.
- Switches with only Generation 2 switching modules or Generation 2 and Generation 3 modules support a maximum of 256 PortChannels with 16 interfaces per PortChannel.
- A PortChannel number refers to the unique identifier for each channel group. This number ranges from of 1 to 256.

### Generation 1 PortChannel Restrictions

This section includes the restrictions on creation and addition of PortChannel members to a PortChannel on Generation 1 hardware:

- 32-port 2-Gbps or 1-Gbps switching module
- MDS 9140 switches

When configuring the host-optimized ports on Generation 1 hardware, the following PortChannel guidelines apply:

## ***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- If you execute the **write erase** command on a 32-port switching module, and then copy a saved configuration to the switch from a text file that contains the **no system default switchport shutdown** command, you need to copy the text file to the switch again for the E ports to come up without manual configuration.
- Any (or all) full line rate port(s) in the Cisco MDS 9100 Series can be included in a PortChannel.
- The host-optimized ports in the Cisco MDS 9100 Series are subject to the same PortChannel rules as 32-port switching modules; only the first port of each group of 4 ports is included in a PortChannel.
  - You can configure only the first port in each 4-port group as an E port (for example, the first port in ports 1–4, the fifth port in ports 5–8, and so on). If the first port in the group is configured as a PortChannel, the other three ports in each group (ports 2–4, 6–8, and so on) are not usable and remain in the shutdown state.
  - If any of the other three ports are configured in a no shutdown state, you cannot configure the first port to be a PortChannel. The other three ports continue to remain in a no shutdown state.

## **F and TF PortChannel Restrictions**

The following guidelines and restrictions are applicable for F and TF PortChannels:

- The ports must be in F mode.
- Automatic creation is not supported.
- The PortChannel interface must be in ACTIVE mode when multiple FCIP interfaces are grouped with WA.
- ON mode is not supported. Only ACTIVE-ACTIVE mode is supported. By default, the mode is ACTIVE on the NPV switches.
- Devices logged in through F PortChannel on an MDS switch are not supported in IVR non-NAT configuration. The devices are supported only in IVR NAT configuration.
- Port security rules are enforced only on physical PWWNs at the single link level.
- FC-SP authenticates only the first physical FLOGI of every PortChannel member.
- Since the FLOGI payload carries only the VF bits to trigger the use of a protocol after the FLOGI exchange, those bits will be overridden. In the case of the NPV switches, the core has a Cisco WWN and will try to initiate the PCP protocol.
- The name server registration of the N ports logging in through an F PortChannel will use the FWWN of the PortChannel interface.
- DPVM configuration is not supported.
- The PortChannel port VSAN cannot be configured using DPVM.
- The Dynamic Port VSAN Management (DPVM) database will be queried only for the first physical FLOGI of each member, so that the port VSAN can be configured automatically.
- DPVM does not bind FC\_IDs to VSANs, but PWWNs to VSANs. It will be queried only for the physical FLOGI.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## PortChannel Configuration

PortChannels are created with default values. You can change the default configuration just like any other physical interface.

Figure 8-6 provides examples of valid PortChannel configurations.

**Figure 8-6 Valid PortChannel Configurations**

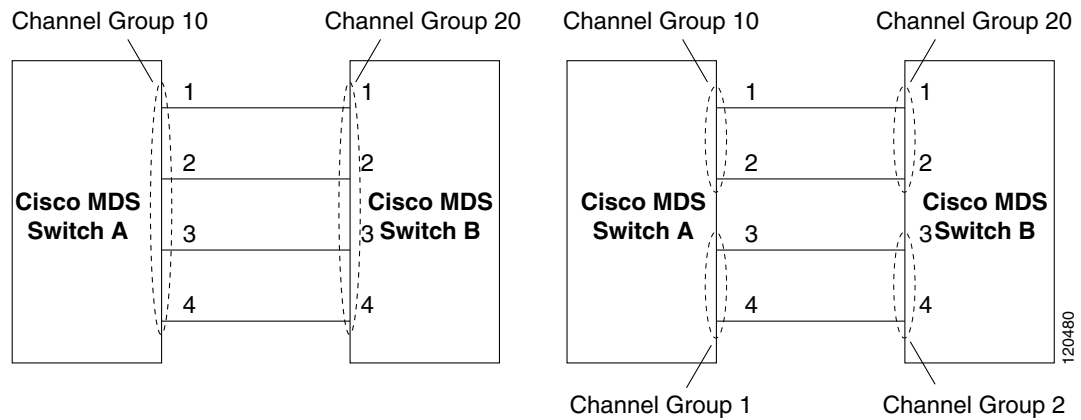
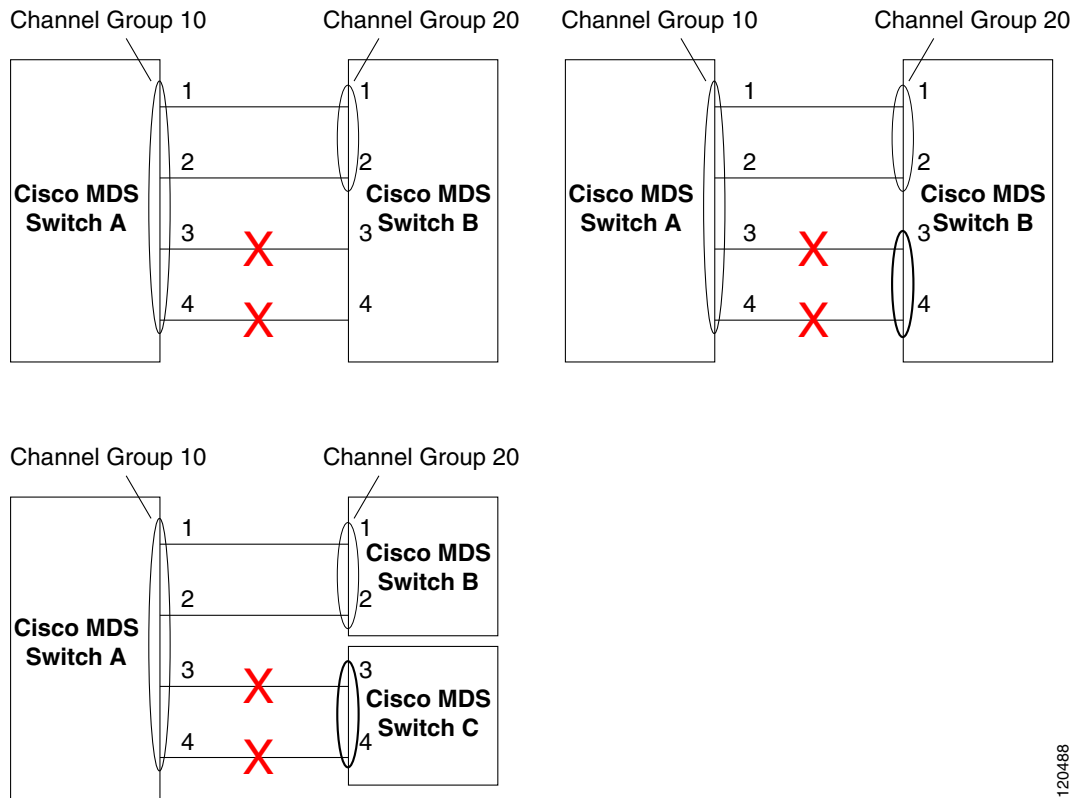


Figure 8-7 provides examples of invalid configurations. Assuming that the links are brought up in the 1, 2, 3, 4 sequence, links 3 and 4 will be operationally down as the fabric is misconfigured.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-7 Misconfigured Configurations**



120488

This section shows how to configure and modify PortChannels and contains the following topics:

- [About PortChannel Configuration, page 8-10](#)
- [Configuring PortChannels Using the Wizard, page 8-11](#)
- [About PortChannel Modes, page 8-6](#)
- [About PortChannel Deletion, page 8-16](#)
- [Deleting PortChannels, page 8-16](#)

## About PortChannel Configuration

Before configuring a PortChannel, consider the following guidelines:

- Configure the PortChannel across switching modules to implement redundancy on switching module reboots or upgrades.
- Ensure that one PortChannel is not connected to different sets of switches. PortChannels require point-to-point connections between the same set of switches.



### Note

On switches with Generation 1 switching modules, or a combination of Generation 1 and Generation 2 switching modules, you can configure a maximum of 128 PortChannels. On switches with only Generation 2 switching modules, or Generation 2 and Generation 3 switching modules, you can configure a maximum of 256 PortChannels.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

If you misconfigure PortChannels, you may receive a misconfiguration message. If you receive this message, the PortChannel's physical links are disabled because an error has been detected.

A PortChannel error is detected if the following requirements are not met:

- Each switch on either side of a PortChannel must be connected to the same number of interfaces.
- Each interface must be connected to a corresponding interface on the other side (see [Figure 8-7](#) for an example of an invalid configuration).
- Links in a PortChannel cannot be changed after the PortChannel is configured. If you change the links after the PortChannel is configured, be sure to reconnect the links to interfaces within the PortChannel and reenabling the links.

If all three conditions are not met, the faulty link is disabled.

## Configuring PortChannels Using the Wizard

To create a PortChannel using the PortChannel Wizard in Fabric Manager, follow these steps:

- Step 1** Click the **PortChannel Wizard** icon in the toolbar (see [Figure 8-8](#)).

**Figure 8-8** PortChannel Wizard Icon

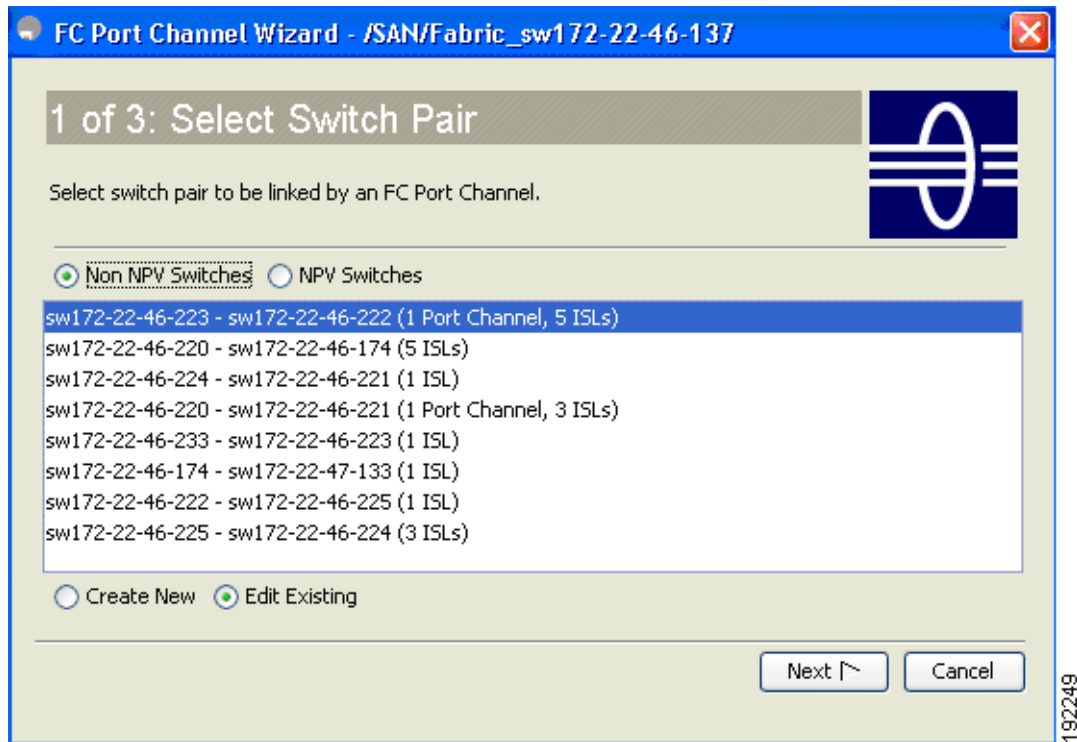


You see the first PortChannel Wizard screen.

- Step 2** Select a switch pair. [Figure 8-9](#) shows a list of the switch pairs.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-9**      **Select Switch Pairs**

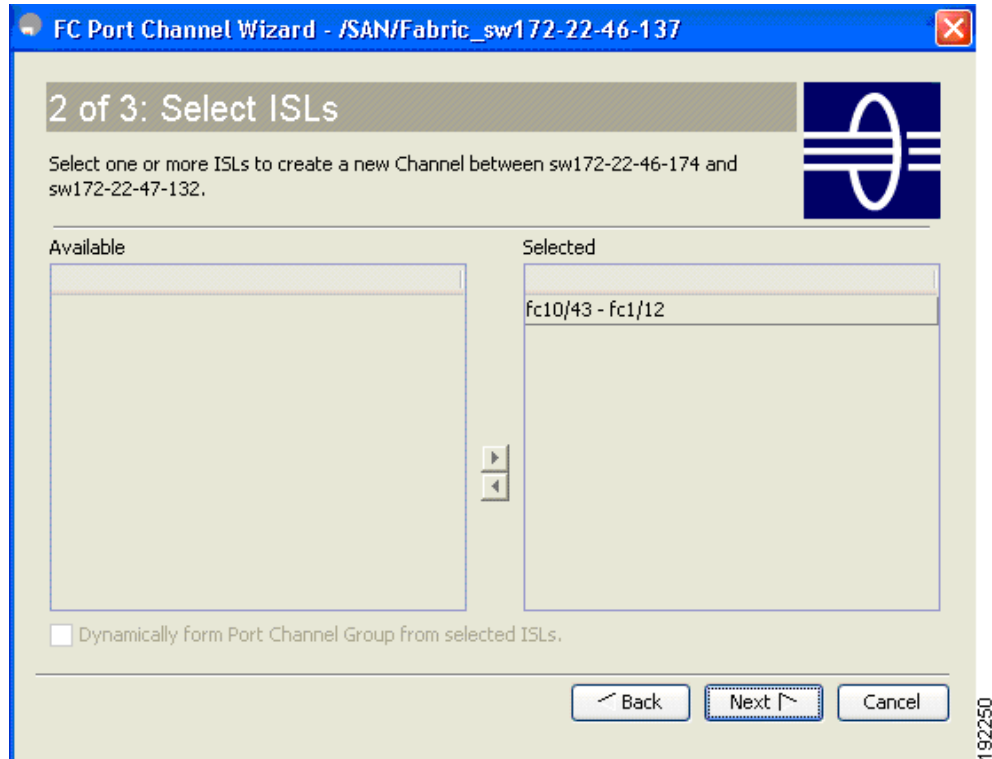


**Step 3**      Click Next.

**Step 4**      Select the ISLs. [Figure 8-10](#) shows a list of the ISLs.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-10**      **Select ISLs**



- Step 5** (Optional) Check the **Dynamically form Port Channel Group from selected ISLs** check box if you want to dynamically create the PortChannel and make the ISL properties identical for the Admin, Trunk, Speed, and VSAN attributes.
- Step 6** Click **Next**.
- Step 7** If you chose to dynamically form a PortChannel from selected ISLs, you see the final PortChannel Wizard screen (see [Figure 8-11](#)). Set the VSAN List, Trunk Mode, and Speed and proceed to [Step 11](#).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-11 Dynamically Form a PortChannel**

**3 of 3: Create Port Channel**

Specify the attributes which will be assigned to selected ISL ports of sw172-22-46-220 (fcip3, fcip5) and sw172-22-46-233 (fcip3, fcip5) to ensure automatic Port Channel creation. NOTE: the Channel may take time to appear in map.

**Port Attributes**

VSAN List:  (1-4093) e.g. 1-22,29-45

Trunk Mode: ☐ nonTrunk ☒ trunk ☐ auto

Speed: ☒ auto ☐ 1Gb ☐ 2Gb ☐ 4Gb ☐ autoMax2G

Back Finish Cancel

144889

**Step 8** If you did not choose to dynamically form a PortChannel, you see the third PortChannel Wizard dialog box(see [Figure 8-12](#)).



**Note** Dynamic VSAN creation is not supported on NPV switches.



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-12 Create a PortChannel**

**FC Port Channel Wizard - /SAN/Fabric\_q148**

**3 of 3: Create Port Channel**

Please review the Channel attributes before pressing Finish to create. Converting all ISL(s) simultaneously into a port channel may be disruptive.  
NOTE: the Channel may take time to appear in map. For NPV Port Channel the Trunking will be enabled

**Between Switch v-32 (fc8/10, fc8/14, fc8/13)**

Channel Id: 1 1..256

Description: To npv1

**And Switch npv1 ((NPV) fc1/3, fc1/6, fc1/7)**

Channel Id: 1 1..256

Description: To v-32

**Channel Attributes**

Port VSAN: 1 1..4093

VSAN List: 1-4093 (1-4093) e.g. 1-22,29-45

☒ Force Admin, Trunk, Speed, and VSAN attributes to be Identical

Speed: ☒ auto ☐ 1Gb ☐ 2Gb ☐ 4Gb ☐ autoMax2G

Back Finish Cancel

**Step 9** Change the channel ID or description for each switch, if necessary.

**Step 10** Review the attributes at the bottom of the screen, and set them if applicable.

The following attributes are shown in [Figure 8-12](#):

- VSAN List—This gives a list of VSANs to which the ISLs belong.
- Trunk Mode—You can enable trunking on the links in the PortChannel. Select **trunking** if your link is between TE ports. Select **nontrunking** if your link is between E ports. Select **auto** if you are not sure.
- Force Admin, Trunk, Speed, and VSAN attributes to be identical—This check box ensures that the same parameter settings are used in all physical ports in the channel. If these settings are not identical, the ports cannot become part of the PortChannel.
- Speed—The port speed values are **auto**, **1Gb**, **2Gb**, **4Gb**, **8Gb**, **autoMax2G**, and **autoMax4G**.

**Step 11** Click **OK**.

The PortChannel is created. Note that it may take a few minutes before the new PortChannel is visible in the Fabric pane.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Configuring the PortChannel Mode

By default, the CLI and the Device Manager create the PortChannel in ON mode in the NPIV core switches and ACTIVE mode on the NPV switches. The Fabric Manager creates all PortChannels in ACTIVE mode. We recommend that you create PortChannels in ACTIVE mode. An F PortChannel is supported only on ACTIVE mode.

To configure ACTIVE mode using Fabric Manager, follow these steps:

- 
- Step 1** Expand **ISLs** and then select **Port Channels** in the Physical Attributes pane.  
You see the PortChannels configured in the Information pane.
- Step 2** Click the **Protocols** tab, and then from the Mode drop-down menu, select the appropriate mode for the Port Channel.
- Step 3** Click the **Apply Changes** icon to save any modifications.
- 

## About PortChannel Deletion

When you delete the PortChannel, the corresponding channel membership is also deleted. All interfaces in the deleted PortChannel convert to individual physical links. After the PortChannel is removed, regardless of the mode used (ACTIVE and ON), the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the [“Graceful Shutdown” section on page 2-11](#)).

If you delete the PortChannel for one port, then the individual ports within the deleted PortChannel retain the compatibility parameter settings (speed, mode, port VSAN, allowed VSAN, and port security). You can explicitly change those settings as required.

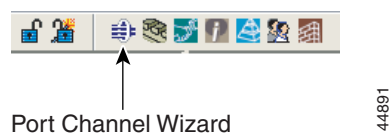
- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the ACTIVE mode, then the PortChannel ports automatically recover from the deletion.

## Deleting PortChannels

To delete a PortChannel using the PortChannel Wizard in Fabric Manager, follow these steps:

- 
- Step 1** Click the **PortChannel Wizard** icon in the toolbar (see [Figure 8-13](#)).

**Figure 8-13** PortChannel Wizard Icon



You see the first PortChannel Wizard screen.

- Step 2** Select the existing PortChannel that you want to delete and click **Next**. You see a list of the ISLs currently associated with this PortChannel.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- Step 3** Click **Next**. You see an editable list of associated ISLs and available ISLs for this PortChannel.
  - Step 4** Click each associated ISL and click the **left arrow** to remove all ISLs from the PortChannel.
  - Step 5** Check the **Delete Port Channel If Empty** check box to delete this PortChannel.
  - Step 6** Click **Finish** to save any modifications or click **Cancel** to discard any changes.
- 

## Interfaces in a PortChannel

You can add or remove a physical interface (or a range of interfaces) to an existing PortChannel. The compatible parameters on the configuration are mapped to the PortChannel. Adding an interface to a PortChannel increases the channel size and bandwidth of the PortChannel. Removing an interface from a PortChannel decreases the channel size and bandwidth of the PortChannel.

This section describes interface configuration for a PortChannel and includes the following topics:

- [About Interface Addition to a PortChannel, page 8-17](#)
- [Adding an Interface to a PortChannel, page 8-18](#)
- [Forcing an Interface Addition, page 8-19](#)
- [About PortChannel Deletion, page 8-16](#)
- [Deleting an Interface from a PortChannel, page 8-20](#)



### Note

For information about PortChannel support on Generation 2 switching modules, see the [“PortChannels” section on page 5-12](#).

---

## About Interface Addition to a PortChannel

You can add a physical interface (or a range of interfaces) to an existing PortChannel. The compatible parameters on the configuration are mapped to the PortChannel. Adding an interface to a PortChannel increases the channel size and bandwidth of the PortChannel.

A port can be configured as a member of a static PortChannel only if the following configurations are the same in the port and the PortChannel:

- Speed
- Mode
- Rate mode
- Port VSAN
- Trunking mode
- Allowed VSAN list or VF-ID list

After the members are added, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the [“Generation 1 PortChannel Restrictions” section on page 8-7](#) and [“Graceful Shutdown” section on page 2-11](#)).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Compatibility Check

A compatibility check ensures that the same parameter settings are used in all physical ports in the channel. Otherwise, they cannot become part of a PortChannel. The compatibility check is performed before a port is added to the PortChannel.

The check ensures that the following parameters and settings match at both ends of a PortChannel:

- Capability parameters (type of interface, Gigabit Ethernet at both ends, or Fibre Channel at both ends).
- Administrative compatibility parameters (speed, mode, rate mode, port VSAN, allowed VSAN list, and port security).




---

**Note** Ports in shared rate mode can also form a PortChannel or a trunking PortChannel.

---

- Operational parameters (remote switch WWN and trunking mode).

A port addition procedure fails if the capability and administrative parameters in the remote switch are incompatible with the capability and administrative parameters in the local switch. If the compatibility check is successful, the interfaces are operational and the corresponding compatibility parameter settings apply to these interfaces.

## Suspended and Isolated States

If the operational parameters are incompatible, the compatibility check fails and the interface is placed in a suspended or isolated state based on the configured mode:

- An interface enters the suspended state if the interface is configured in the ON mode.
- An interface enters the isolated state if the interface is configured in the ACTIVE mode.

## Adding an Interface to a PortChannel



**Note**

---

By default, the CLI adds a interface normally to a PortChannel, while the Fabric Manager adds the interface by force, unless specified explicitly.

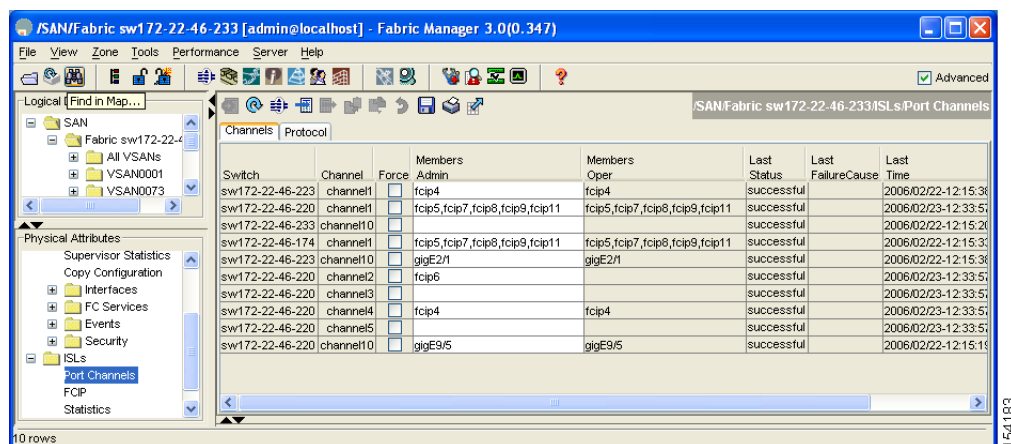
---

To add an interface or range of interfaces to a PortChannel using Fabric Manager, follow these steps:

- 
- Step 1** Expand **ISLs** and then select **Port Channels** in the Physical Attributes pane.  
You see the PortChannels configured in the Information pane (see [Figure 8-14](#)).

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 8-14** Port Channels



- Step 2** Click the **Channels** tab and find the switch and PortChannel that you want to edit.
- Step 3** Set Members Admin to the interface or list of interfaces that you want to add to the PortChannel.
- Step 4** Click the **Apply Changes** icon to save any modifications or click **Undo Changes** to discard any changes.

## Forcing an Interface Addition

You can force the port configuration to be overwritten by the PortChannel. In this case, the interface is added to a PortChannel.

- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the ACTIVE mode, then the PortChannel ports automatically recover from the addition.



### Note

When PortChannels are created from within an interface, the **force** option cannot be used.

After the members are forcefully added, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the “[Generation 1 PortChannel Restrictions](#)” section on page 8-7).

To force the addition of a port to a PortChannel using Fabric Manager, follow these steps:

- Step 1** Expand **ISLs** and then select **Port Channels** in the Physical Attributes pane. You see the PortChannels configured in the Information pane.
- Step 2** Click the **Channels** tab and find the switch and PortChannel that you want to edit.
- Step 3** Set Members Admin to the interface or list of interfaces that you want to add to the PortChannel.
- Step 4** Check the **Force** check box to force this interface addition.
- Step 5** Click the **Apply Changes** icon to save any modifications.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## About Interface Deletion from a PortChannel

When a physical interface is deleted from the PortChannel, the channel membership is automatically updated. If the deleted interface is the last operational interface, then the PortChannel status is changed to a down state. Deleting an interface from a PortChannel decreases the channel size and bandwidth of the PortChannel.

- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the ACTIVE mode, then the PortChannel ports automatically recover from the deletion.

After the members are deleted, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the [“Generation 1 PortChannel Restrictions”](#) section on page 8-7 and [“Graceful Shutdown”](#) section on page 2-11).

## Deleting an Interface from a PortChannel

To delete a physical interface (or a range of physical interfaces) from a PortChannel using Fabric Manager, follow these steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand <b>ISLs</b> and then select <b>Port Channels</b> in the Physical Attributes pane.<br>You see the PortChannels configured in the Information pane. |
| <b>Step 2</b> | Click the <b>Channels</b> tab and find the switch and PortChannel that you want to edit.   |
| <b>Step 3</b> | Remove the interface or list of interfaces you want deleted in the Members the Admin column.   |
| <b>Step 4</b> | Click the <b>Apply Changes</b> icon to save any modifications.   |
- 

## PortChannel Protocols

In earlier Cisco SAN-OS releases, PortChannels required additional administrative tasks to support synchronization. The Cisco NX-OS software provides robust error detection and synchronization capabilities. You can manually configure channel groups or they can be automatically created. In both cases, the channel groups have the same capability and configurational parameters. Any change in configuration applied to the associated PortChannel interface is propagated to all members of the channel group.

A protocol to exchange PortChannel configurations is available in all Cisco MDS switches. This addition simplifies PortChannel management with incompatible ISLs. An additional autocreation mode enables ISLs with compatible parameters to automatically form channel groups without manual intervention.

The PortChannel protocol is enabled by default.

The PortChannel protocol expands the PortChannel functional model in Cisco MDS switches. It uses the exchange peer parameters (EPP) services to communicate across peer ports in an ISL. Each switch uses the information received from the peer ports along with its local configuration and operational values to decide if it should be part of a PortChannel. The protocol ensures that a set of ports are eligible to be part of the same PortChannel. They are only eligible to be part of the same port channel if all the ports have a compatible partner.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

The PortChannel protocol uses two subprotocols:

- Bringup protocol—Automatically detects misconfigurations so you can correct them. This protocol synchronizes the PortChannel at both ends so that all frames for a given flow (as identified by the source FC ID, destination FC ID and OX\_ID) are carried over the same physical link in both directions. This helps make applications such as write acceleration, work for PortChannels over FCIP links.
- Autocreation protocol—Automatically aggregates compatible ports into a PortChannel.

This section describes how to configure the PortChannel protocol and includes the following sections:

- [About Channel Group Creation, page 8-21](#)
- [About Autocreation, page 8-22](#)
- [Enabling and Configuring Autocreation, page 8-23](#)
- [About Manually Configured Channel Groups, page 8-23](#)
- [Converting to Manually Configured Channel Groups, page 8-23](#)

## About Channel Group Creation

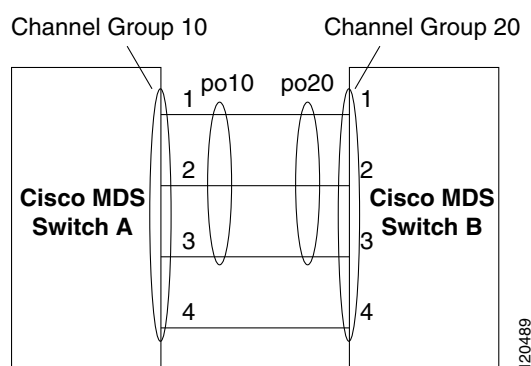


**Note**

Channel groups are not supported on internal ports in the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeSystem.

Assuming link A1-B1 comes up first (see [Figure 8-15](#)), that link is operational as an individual link. When the next link, say A2-B2 comes up, the PortChannel protocol identifies if this link is compatible with link A1-B1 and automatically creates channel groups 10 and 20 in the respective switches. If link A3-B3 can join the channel groups (the PortChannels), the respective ports have compatible configurations. If link A4-B4 operates as an individual link, it is because of the incompatible configuration of the two end ports with the other member ports in this channel group.

**Figure 8-15 Autocreating Channel Groups**



The channel group numbers are selected dynamically, and as such, the administrative configuration of the ports forming the channel group at either end are applicable to the newly created channel group. The channel group number being chosen dynamically may be different across reboots for the same set of PortChannels based on the order of ports that are initialized in the switch.

[Table 8-2](#) identifies the differences between user-configured and auto-configured channel groups.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Table 8-2 Channel Group Configuration Differences**

User-Configured Channel Group	Autocreated Channel Group
Manually configured by the user.	Created automatically when compatible links come up between two compatible switches, if channel group autocreation is enabled in all ports at both ends.
Member ports cannot participate in autocreation of channel groups. The autocreation feature cannot be configured.	None of these ports are members of a user-configured channel group.
You can form the PortChannel with a subset of the ports in the channel group. Incompatible ports remain in a suspended or isolated state depending on the ON or ACTIVE mode configuration.	All ports included in the channel group participate in the PortChannel—no member port becomes isolated or suspended; instead, the member port is removed from the channel group when the link is found to be incompatible.
Any administrative configuration made to the PortChannel is applied to all ports in the channel group, and you can save the configuration for the PortChannel interface.	Any administrative configuration made to the PortChannel is applied to all ports in the channel group, but the configurations are saved for the member ports; no configuration is saved for the PortChannel interface. You can explicitly convert this channel group, if required.
You can remove any channel group and add members to a channel group.	You cannot remove a channel group, or add/remove any of its members. The channel group is removed when no member ports exist.



**Note**

Autocreation is not supported as of MDS NX-OS Release 4.1(1b) and later.

## About Autocreation

The autocreation protocol has the following functionality:

- A port is not allowed to be configured as part of a PortChannel when the autocreation feature is enabled. These two configurations are mutually exclusive.
- Autocreation must be enabled in both the local and peer ports to negotiate a PortChannel.
- Aggregation occurs in one of two ways:
  - A port is aggregated into a compatible autocreated PortChannel.
  - A port is aggregated with another compatible port to form a new PortChannel.
- Newly created PortChannels are allocated from the maximum possible PortChannel (128 for Generation 1 or a combination of Generation 1 and Generation 2 switches, or 256 for Generation 2 switches) in a decreasing order based on availability. If all 128 (or 256) numbers are used up, aggregation is not allowed.
- You cannot change the membership or delete an autocreated PortChannel.
- When you disable autocreation, all member ports are removed from the autocreated PortChannel.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- Once the last member is removed from an autocreated PortChannel, the channel is automatically deleted and the number is released for reuse.
- An autocreated PortChannel is not persistent through a reboot. An autocreated PortChannel can be manually configured to appear the same as a persistent PortChannel. Once the PortChannel is made persistent, the autocreation feature is disabled in all member ports.
- You can enable or disable the autocreation feature on a per-port basis or for all ports in the switch. When this configuration is enabled, the channel group mode is assumed to be active. The default for this task is disabled.
- If autocreation of channel groups is enabled for an interface, you must first disable autocreation before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.



**Tip**

When enabling autocreation in any switch in the Cisco MDS 9000 Family, we recommend that you retain at least one interconnected port between the switches without any autocreation configuration. If all ports between two switches are configured with the autocreation feature at the same time, you may face a possible traffic disruption between these two switches as the ports are automatically disabled and reenabled when ports are added to an autocreated PortChannel.

## Enabling and Configuring Autocreation

To configure PortChannel autocreation, check the **Dynamically form Port Channel Group from selected ISLs** option in the PortChannel Wizard. For more information, see the [“Configuring PortChannels Using the Wizard”](#) section on page 8-11.

## About Manually Configured Channel Groups

A user-configured channel group cannot be converted to an autocreated channel group. However, you can convert an autocreated channel group to a manual channel group. Once performed, this task is irreversible. The channel group number does not change, but the member ports operate according to the properties of the manually configured channel group, and the autocreation of channel group is implicitly disabled for all member ports.



**Tip**

If you enable persistence, be sure to enable it at both ends of the PortChannel.

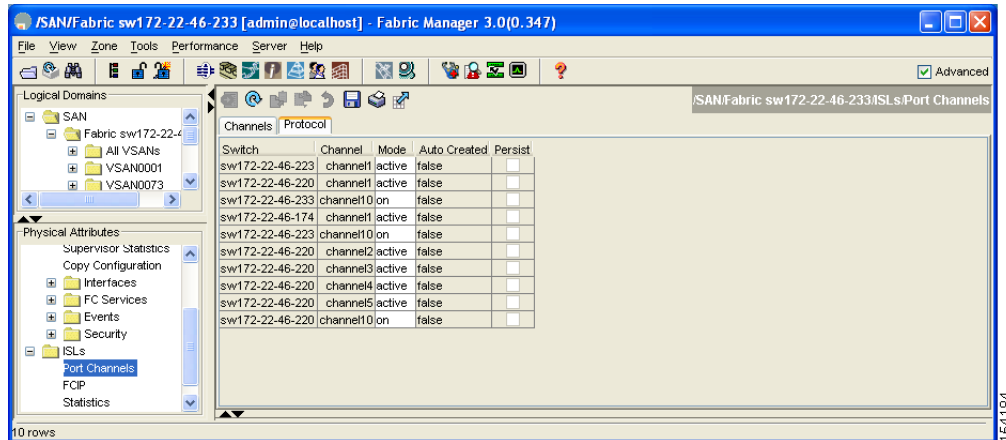
## Converting to Manually Configured Channel Groups

To convert an autocreated channel group to a user-configured channel group using Fabric Manager, follow these steps:

- Step 1** Expand **ISLs** and then select **Port Channels** in the Physical Attributes pane. Click the **Protocol** tab. You see the switch protocols as shown in [Figure 8-16](#).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 8-16** Switch Protocols

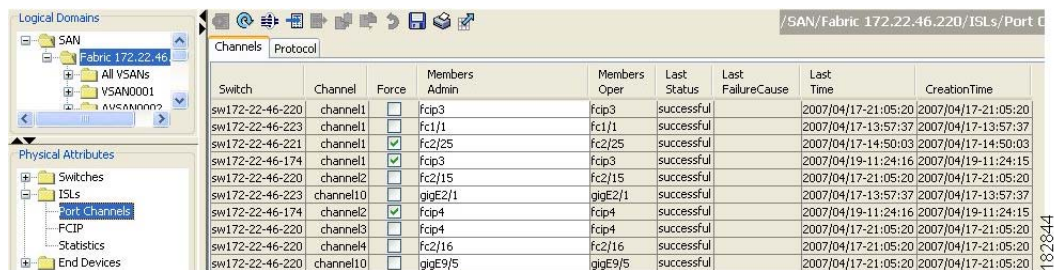


- Step 2** Check the **Persist** check box for each channel that you want to convert to a manually configured channel group.
- Step 3** Click the **Apply Changes** icon to save any modifications.

## Verifying the PortChannel Configuration

You can use the Information pane in Fabric Manager to verify your PortChannel Configuration (see [Figure 8-17](#)).

**Figure 8-17** PortChannel Summary in Fabric Manager



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Default Settings

Table 8-3 lists the default settings for PortChannels.

**Table 8-3**      ***Default PortChannel Parameters***

Parameters	Default
PortChannels	FSPF is enabled by default.
Create PortChannel	Administratively up.
Default PortChannel mode	ON mode on non-NPV and NPIV core switches. ACTIVE mode on NPV switches.
Autocreation	Disabled.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***



## CHAPTER 9

# Configuring N Port Virtualization

---

N port virtualization (NPV) reduces the number of Fibre Channel domain IDs in SANs. Switches operating in the NPV mode do not join a fabric. They pass traffic between NPV core switch links and end devices, which eliminates the domain IDs for these edge switches.

NPV is supported by the following Cisco MDS 9000 switches and Cisco Nexus 5000 Series switches only:

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 Fabric Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter
- Cisco Nexus 5000 Series switches



### Note

---

NPV is available on these switches only while in NPV mode; if in switch mode, NPV is not available.

---

This chapter includes the following sections:

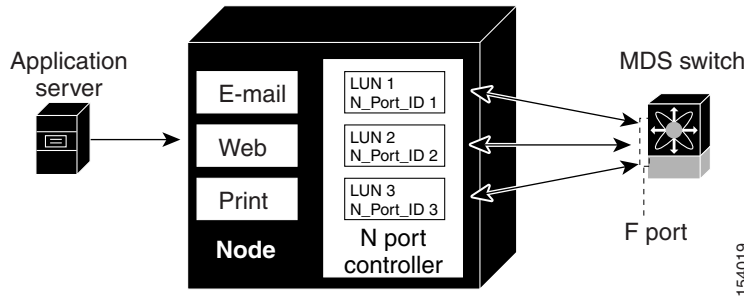
- [About N Port Identifier Virtualization, page 9-1](#)
- [About N Port Virtualization, page 9-2](#)
- [NPV Guidelines and Requirements, page 9-7](#)
- [Configuring NPV, page 9-8](#)
- [Using the NPV Setup Wizard, page 9-14](#)

## About N Port Identifier Virtualization

N port identifier virtualization (NPIV) provides a means to assign multiple FC IDs to a single N port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level. [Figure 9-1](#) shows an example application using NPIV.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 9-1 NPIV Example**



You must globally enable NPIV for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port identifiers.



**Note**

All of the N port identifiers are allocated in the same VSAN.

## Enabling N Port Identifier Virtualization

You must globally enable NPIV for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port identifiers.



**Note**

All of the N port identifiers are allocated in the same VSAN.

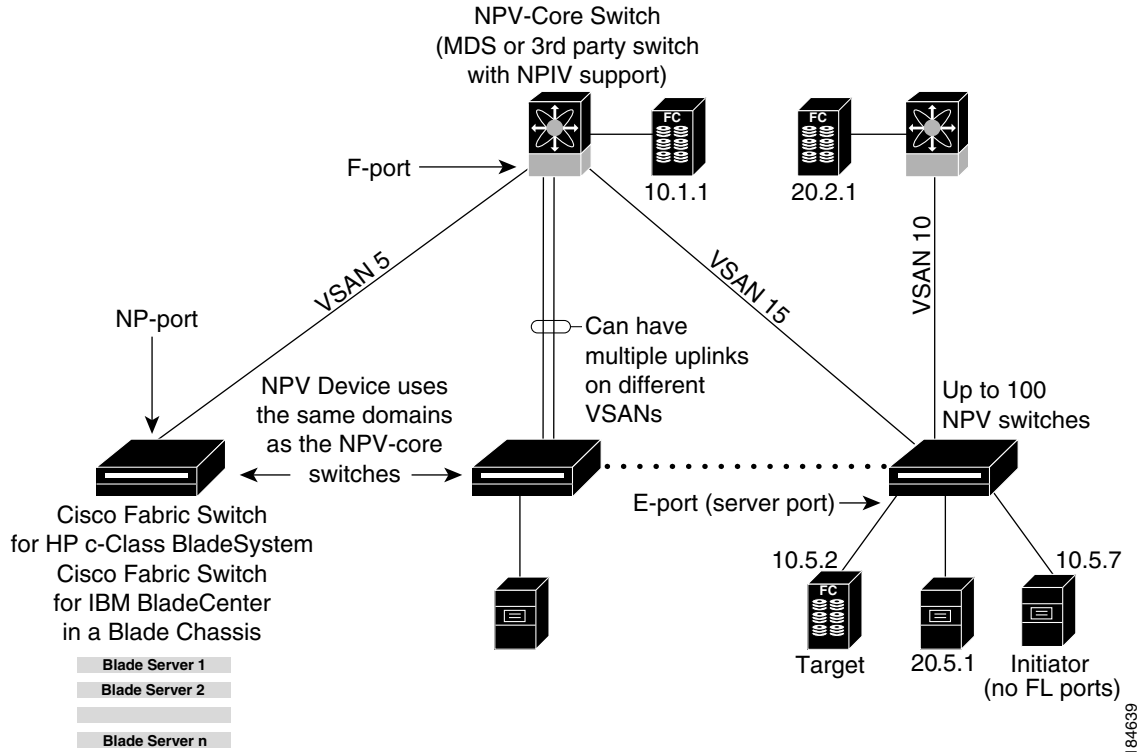
## About N Port Virtualization

Typically, Fibre Channel networks are deployed using a core-edge model with a large number of fabric switches connected to edge devices. Such a model is cost-effective because the per port cost for director class switches is much higher than that of fabric switches. However, as the number of ports in the fabric increases, the number of switches deployed also increases, and you can end up with a significant increase in the number of domain IDs (the maximum number supported is 239). This challenge becomes even more difficult when additional blade chassis are deployed in Fibre Channel networks.

NPV addresses the increase in the number of domain IDs needed to deploy a large number of the ports by making a fabric or blade switch appear as a host to the core Fibre Channel switch, and as a Fibre Channel switch to the servers in the fabric or blade switch. NPV aggregates multiple locally connected N ports into one or more external NP links, which shares the domain ID of the NPV core switch among multiple NPV switches. NPV also allows multiple devices to attach to same port on the NPV core switch, which reduces the need for more ports on the core.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

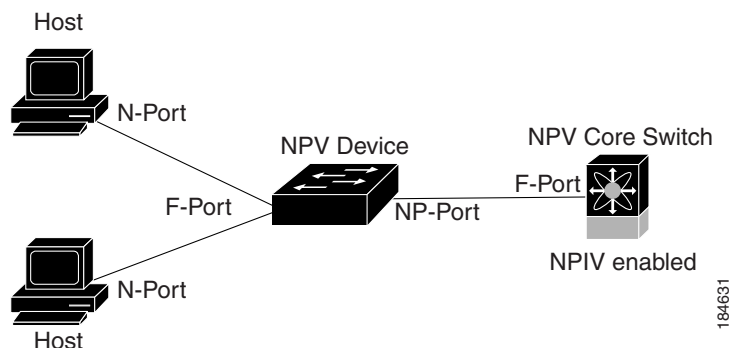
**Figure 9-2 Cisco NPV Fabric Configuration**



While NPV is similar to N port identifier virtualization (NPIV), it does not offer exactly the same functionality. NPIV provides a means to assign multiple FC IDs to a single N port, and allows multiple applications on the N port to use different identifiers. NPIV also allows access control, zoning, and port security to be implemented at the application level. NPV makes use of NPIV to get multiple FCIDs allocated from the core switch on the NP port.

Figure 9-3 shows a more granular view of an NPV configuration at the interface level.

**Figure 9-3 Cisco NPV Configuration–Interface View**



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## NPV Mode

A switch is in NPV mode after a user has enabled NPV and the switch has successfully rebooted. NPV mode applies to an entire switch. All end devices connected to a switch that is in NPV mode must log in as an N port to use this feature (loop-attached devices are not supported). All links from the edge switches (in NPV mode) to the NPV core switches are established as NP ports (not E ports), which are used for typical interswitch links. NPIV is used by the switches in NPV mode to log in to multiple end devices that share a link to the NPV core switch.



### Note

In-order data delivery is not required in NPV mode because the exchange between two end devices always takes the same uplink to the core from the NPV device. For traffic beyond the NPV device, core switches will enforce in-order delivery if needed and/or configured.

## NP Ports

An NP port (proxy N port) is a port on a device that is in NPV mode and connected to the NPV core switch using an F port. NP ports behave like N ports except that in addition to providing N port behavior, they also function as proxies for multiple, physical N ports.



### Note

A Cisco Nexus 5000 Series switch in NPV mode that runs Cisco NX-OS Release 4.2(1) or later releases supports trunking F port mode on NP ports. You can enable either, or both, VSAN trunking and an F port on an NP port.

## NP Links

An NP link is basically an NPIV uplink to a specific end device. NP links are established when the uplink to the NPV core switch comes up; the links are terminated when the uplink goes down. Once the uplink is established, the NPV switch performs an internal FLOGI to the NPV core switch, and then (if the FLOGI is successful) registers itself with the NPV core switch's name server. Subsequent FLOGIs from end devices in this NP link are converted to FDISCs. For more details refer to the [“Internal FLOGI Parameters” section on page 9-4](#).

Server links are uniformly distributed across the NP links. All the end devices behind a server link will be mapped to only one NP link.

## Internal FLOGI Parameters

When an NP port comes up, the NPV device first logs itself in to the NPV core switch and sends a FLOGI request that includes the following parameters:

- The fWWN (fabric port WWN) of the NP port used as the pWWN in the internal login.
- The VSAN-based sWWN (switch WWN) of the NPV device used as nWWN (node WWN) in the internal FLOGI.

After completing its FLOGI request, the NPV device registers itself with the fabric name server using the following additional parameters:

- Switch name and interface name (for example, fc1/4) of the NP port is embedded in the symbolic port name in the name server registration of the NPV device itself.



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- The IP address of the NPV device is registered as the IP address in the name server registration of the NPV device.



**Note**

The BB\_SCN of internal FLOGIs on NP ports is always set to zero. The BB\_SCN is supported at the F-port of the NPV device.

Figure 9-4 shows the internal FLOGI flows between an NPV core switch and an NPV device.

**Figure 9-4 Internal FLOGI Flows**

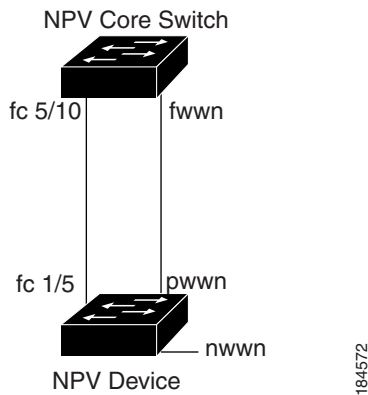


Table 9-1 identifies the internal FLOGI parameters that appear in Figure 9-4.

**Table 9-1 Internal FLOGI Parameters**

Parameter	Derived From
pWWN	The fWWN of the NP port.
nWWN	The VSAN-based sWWN of the NPV device.
fWWN	The fWWN of the F port on the NPV core switch.
symbolic port name	The switch name and NP port interface string. <b>Note</b> If there is no switch name available, then the output will display “switch.” For example, switch: fc1/5.
IP address	The IP address of the NPV device.
symbolic node name	The NPV switch name.

Although fWWN-based zoning is supported for NPV devices, it is not recommended because:

- Zoning is not enforced at the NPV device (rather, it is enforced on the NPV core switch).
- Multiple devices behind an NPV device log in via the same F port on the core (they use same fWWN and cannot be separated into different zones).
- The same device might log in using different fWWNs on the core switch (depending on the NPV link it uses) and may need to be zoned using different fWWNs.

**[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

## Default Port Numbers

Port numbers on NPV-enabled switches will vary depending on the switch model. For details about port numbers for NPV-eligible switches, see the *Cisco NX-OS Family Licensing Guide*.

## NPV CFS Distribution over IP

NPV devices use only IP as the transport medium. CFS uses multicast forwarding for CFS distribution. NPV devices do not have ISL connectivity and FC domain. To use CFS over IP, multicast forwarding has to be enabled on the Ethernet IP switches all along the network that physically connects the NPV switch. You can also manually configure the static IP peers for CFS distribution over IP on NPV-enabled switches. For more information, see the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*.

## NPV Traffic Management

This sections discusses the following aspects of load balancing:

- [Auto, page 9-6](#)
- [Traffic Map, page 9-6](#)
- [Disruptive, page 9-7](#)

### Auto

Before Cisco MDS SAN-OS Release 3.3(1a), NPV supported automatic selection of external links. When a server interface is brought up, an external interface with the minimum load is selected from the available links. There is no manual selection on the server interfaces using the external links. Also, when a new external interface was brought up, the existing load was not distributed automatically to the newly available external interface. This newly brought up interface is used only by the server interfaces that come up after this interface.

### Traffic Map

As in Cisco MDS SAN-OS Release 3.3(1a) and NX-OS Release 4.1(1a), NPV supports traffic management by allowing you to select and configure the external interfaces that the server uses to connect to the core switches.



#### Note

When the NPV traffic management is configured, the server uses only the configured external interfaces. Any other available external interface will not be used.

The NPV traffic management feature provides the following benefits:

- Facilitates traffic engineering by providing dedicated external interfaces for the servers connected to NPV.
- Uses the shortest path by selecting external interfaces per server interface.
- Uses the persistent FC ID feature by providing the same traffic path after a link break, or reboot of the NPV or core switch.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- Balances the load by allowing the user to evenly distribute the load across external interfaces.

## Disruptive

Disruptive load balance works independent of automatic selection of interfaces and configured traffic map of external interfaces. This feature forces reinitialization of the server interfaces to achieve load balance when this feature is enabled and whenever a new external interface comes up. To avoid flapping the server interfaces too often undesirably, enable this feature once and then disable it whenever the needed load balance is achieved.

If disruptive load balance is not enabled, you need to manually flap the server interface to move some of the load to a new external interface.

## Multiple VSAN Support

By grouping devices into different NPV sessions based on VSANs, it is possible to support multiple VSANs on the NPV-enabled switch. The correct uplink must be selected based on the VSAN that the uplink is carrying.

# NPV Guidelines and Requirements

Following are recommended guidelines and requirements when deploying NPV:

- NPV core switches must support NPIV.
- You can have up to 100 NPV devices.
- Nondisruptive upgrades are supported. See the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*.
- Port tracking is supported. See the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.
- You can configure zoning for end devices that are connected to NPV devices using all available member types on the NPV core switch. If fWWN, sWWN, domain, or port-based zoning is used, then fWWN, sWWN or the domain/port of the NPV core switch should be used.
- Port security is supported on the NPV core switch for devices logged in via NPV.
- NPV uses a load balancing algorithm to automatically assign end devices in a VSAN to one of the NPV core switch links (in the same VSAN) upon initial login. If there are multiple NPV core switch links in the same VSAN, then you cannot assign a specific one to an end device.
- Both servers and targets can be connected to an NPV device.
- Remote SPAN is not supported.
- Local switching is not supported; all traffic is switched using the NPV core switch.
- NPV devices can connect to multiple NPV core switches. In other words, different NP ports can be connected to different NPV core switches.
- NPV supports NPIV-capable module servers (nested NPIV).
- Only F, NP, and SD ports are supported in NPV mode.
- In the case of servers that are booted over the SAN with NPV, if an NPV link failover occurs, servers will lose access to their boot LUN temporarily.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- NPV switches do not recognize the BB\_SCN configuration on the xNP ports because of interoperability issues with the third-party core switches.

## NPV Traffic Management Guidelines

When deploying NPV traffic management, follow these guidelines:

- Use NPV traffic management only when the automatic traffic engineering by the NPV device is not sufficient for the network requirements.
- Do not configure traffic maps for all the servers. For non-configured servers, NPV will use automatic traffic engineering.
- Configure the Persistent FC ID on the core switch. Traffic engineering directs the associated server interface to external interfaces that lead to the same core switch. The server will be assigned the same FC ID for every log in. This guideline is not applicable if a 91x4 switch is used as the core switch.
- Server interfaces configured to a set of external interfaces cannot use any other available external interfaces, even if the configured interfaces are not available.
- Do not configure disruptive load balancing because this involves moving a device from one external interface to another interface. Moving the device between external interfaces requires NPV relogin to the core switch through F port leading to traffic disruption.
- Link a set of servers to a core switch by configuring the server to a set of external interfaces that are linked to the core switch.

## Configuring NPV

When you enable NPV, the system configuration is erased and the system reboots with the NPV mode enabled.



### Note

We recommend that you save the current configuration either on bootflash or a TFTP server before NPV (if the configuration is required for later use). Use the following commands to save either your non-NPV or NPV configuration:

```
switch# copy running bootflash:filename
```

The configuration can be reapplied later using the following command:

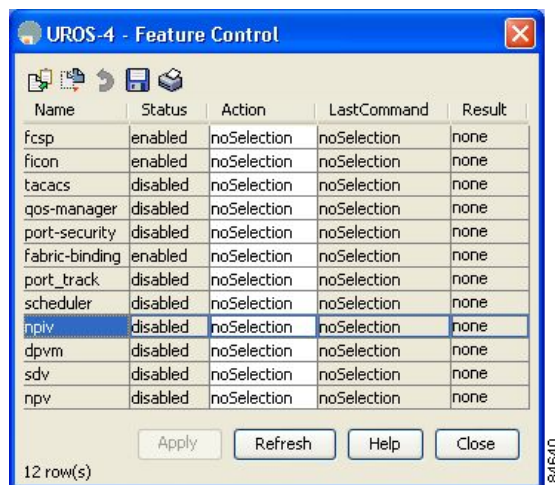
```
switch# copy bootflash:filename running-config
```

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

To use Fabric Manager and Device Manager to configure NPV, follow these steps:

- Step 1** Launch Device Manager from the core NPV switch to enable NPIV on the core NPV switch. From the Admin drop-down menu, select Feature Control. Select **enable** for the NPIV feature (see [Figure 9-5](#)).

**Figure 9-5 Enabling NPIV and NPV**



- Step 2** Click **Apply**.
- Step 3** From the Interface drop-down menu, select **FC All** to configure the NPIV core switch port as an F Port.
- Step 4** In the Mode Admin column, select the F port mode and click **Apply**.
- Step 5** Launch Device Manager from the NPV device to enable NPV on the NPV device. From the Admin drop-down menu, select Feature Control. Select enable for the NPV feature and click **Apply**.
- Step 6** From the Interface drop-down menu, select **FC All** to configure the external interfaces on the NPV device.
- Step 7** In the Mode Admin column, select the NP port mode and click **Apply**.
- Step 8** From the Interface drop-down menu, select FC All to configure the server interfaces on the NPV device.
- Step 9** In the Mode Admin column, select F port mode and click **Apply**.
- Step 10** The default Admin status is down. After configuring port modes, you must select up Admin Status to bring up the links.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## Configuring NPV Traffic Management

The NPV traffic management feature is enabled after configuring NPV. Configuring NPV traffic management involves configuring a list of external interfaces to the servers, and enabling or disabling disruptive load balancing.

### Configuring List of External Interfaces per Server Interface

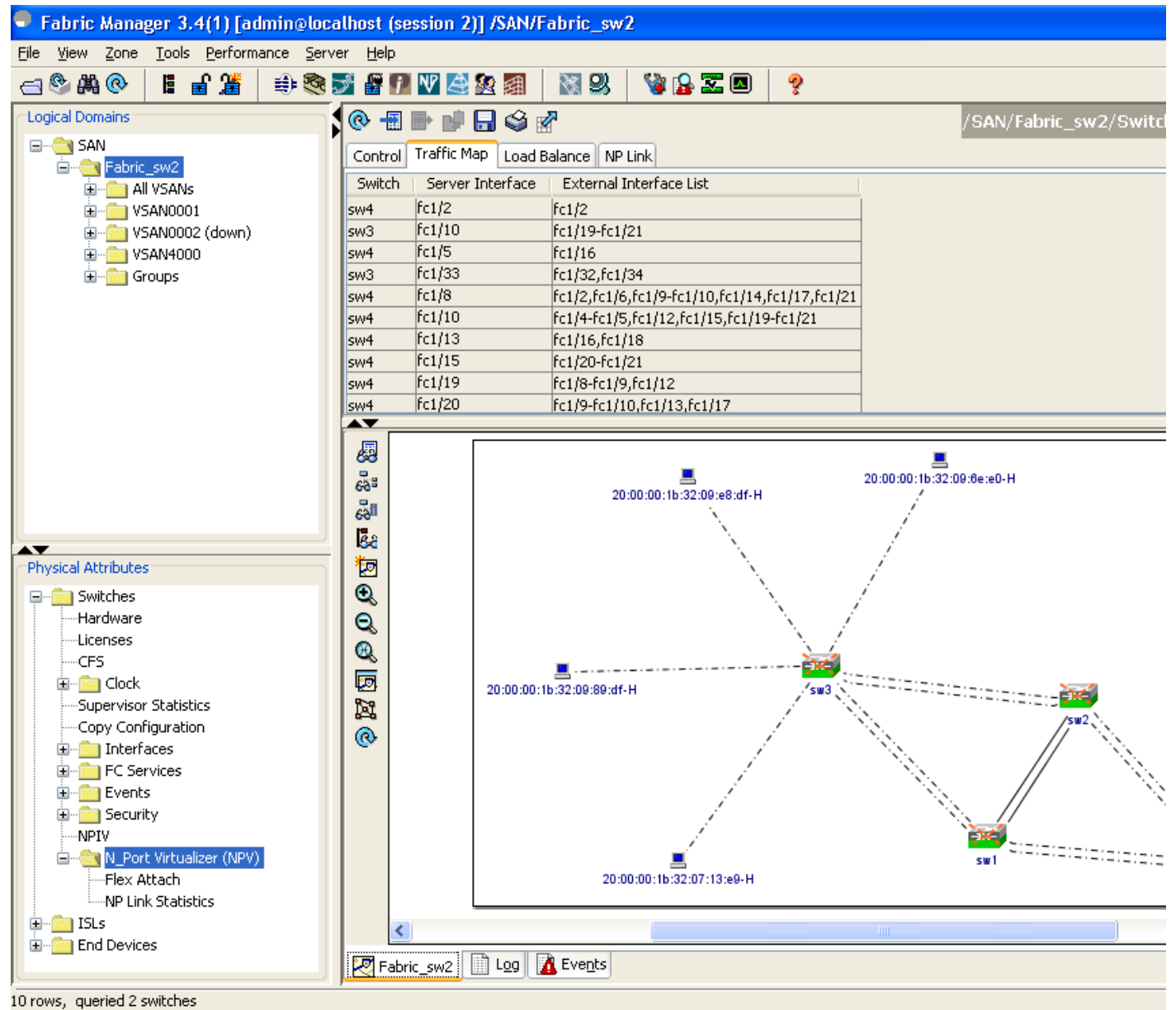
A list of external interfaces are linked to the server interfaces when the server interface is down, or if the specified external interface list includes the external interface already in use.

To configure the list of external interfaces per server interface using Fabric Manager, perform the following tasks:


- 
- Step 1** Choose **Physical Attributes > Switches > N\_Port Virtualizer (NPV)** (see [Figure 9-6](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 9-6 NPV Traffic Map Tab**



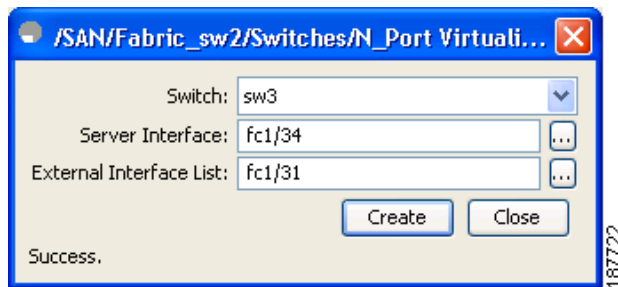
**Step 2** Click the **Traffic Map** tab.

**Step 3** Click the  icon in the toolbar or right click and then select **Create Row...**

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

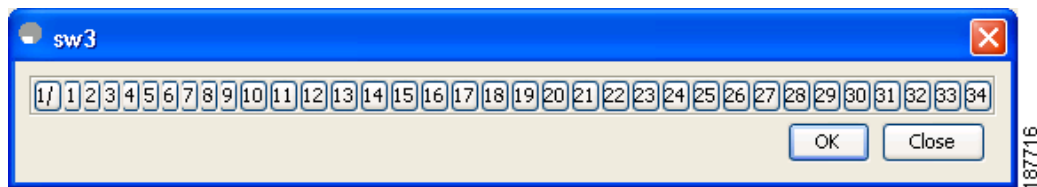
**Step 4** Select the Switch from the drop-down list (see Figure 9-7).

**Figure 9-7 Map Entry Dialog Box**




**Step 5** Type the port numbers or click the [...] button (not available on blade server switches) to select the Server Interface and External Interfaces from the port selection dialog box (see Figure 9-8).

**Figure 9-8 Port Selection Dialog Box**



**Note** You can select only one Server Interface but multiple External Interfaces can be mapped on to it. Previously selected ports are disabled and cannot be selected.

To delete the map entry, select the row from the Traffic Map tab, and then click the  icon in the toolbar or right click and select **Delete Row**.

## Enabling the Global Policy for Disruptive Load Balancing

Disruptive load balancing allows you to review the load on all the external interfaces and balance the load disruptively. Disruptive load balancing is done by moving the servers using heavily loaded external interfaces, to the external interfaces running with fewer loads.

To enable disruptive load balancing using Fabric Manager, perform the following tasks:

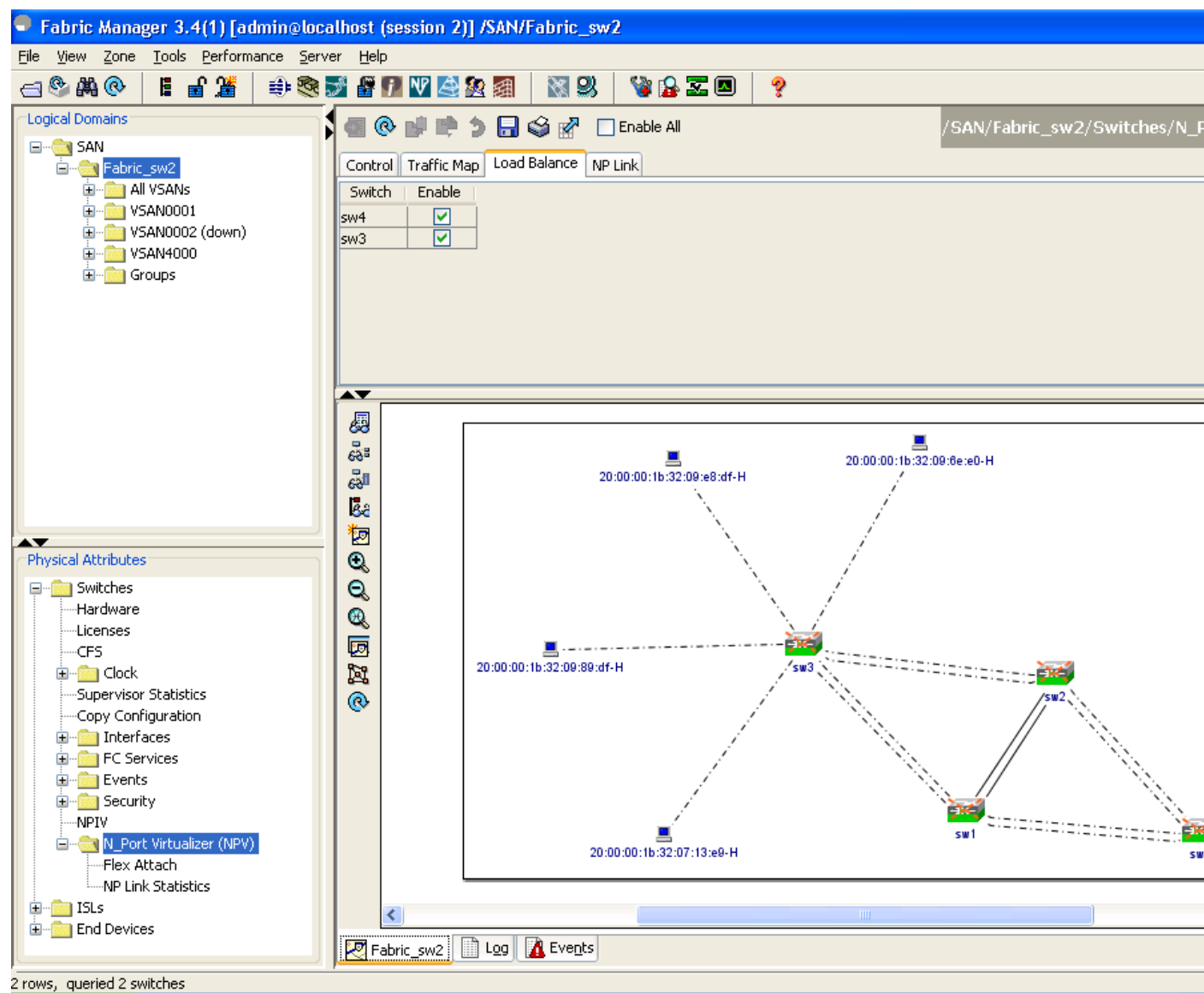
- Step 1** Choose **Physical Attributes > Switches > N\_Port Virtualizer (NPV)** (see Figure 9-9).
- Step 2** Click the **Load Balance** tab.
- Step 3** Check the **Enable** check box to enable disruptive load balancing on the switch.



*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

To enable disruptive load balancing on all the switches, check the **Enable All** check box (see Figure 9-9).

**Figure 9-9** NPV Load Balance Tab



## Displaying the External Interface Usage for Server Interfaces

To display the external interface usage for the server interfaces, follow these steps:

- Step 1** Choose **Physical Attributes > Switches > N\_Port Virtualizer (NPV)** (see Figure 9-10).
- Step 2** Click the **External Interface Usage** tab.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 9-10      External Interface Usage**

Table

Control

Traffic Map

Load Balance

External Interface Usage

NP Link

Switch	Server Interface	External Interface In Use
sw113	fc1/13	fc1/2
sw113	fc1/24	fc1/1

194160

## Using the NPV Setup Wizard



**Note**

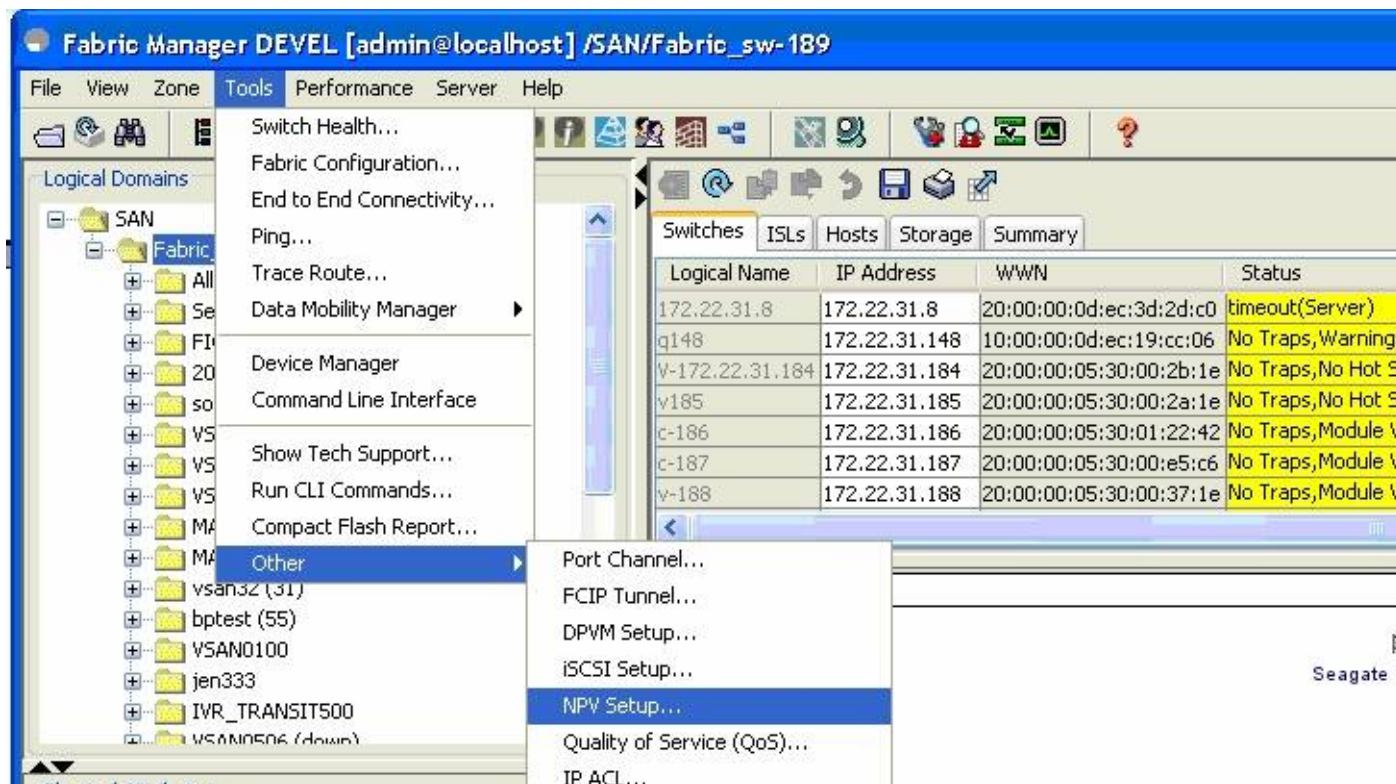
For Cisco Nexus 5000 Series switches, you must first enable the NPV mode for the switch by choosing **Switches > N\_Port Virtualization (NPV)** in the Physical Attributes pane, and then use the NPV wizard to configure other NPV-related settings on the switch.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

To configure NPV using the wizard, follow these steps:

- Step 1** Select **Tools > NPV > NPV Setup...** to launch NPV Setup Wizard from Fabric Manager (see Figure 9-11).

**Figure 9-11** Launching NPV Setup Wizard



Before the wizard starts, Fabric Manager checks if there are any NPV- and NPIV-capable switches from the client's SAN. An NPV-capable switch has to be a Cisco MDS 9124, 9134, a Cisco Nexus 5000 Series switch, an HP Blade Server, or an IBM Blade Server with SAN-OS Release 3.2.2 and later. An NPIV-capable switch has to be Cisco switch with SAN-OS Release 3.0.1 and later. If there are no NPV-capable switches, Fabric Manager displays an error message (see Figure 9-12).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 9-12 Error in Launching**



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 2** Select the NPV devices (see Figure 9-13).

**Figure 9-13** Selecting the NPV Devices

**NPV Setup Wizard**

**Step 1 of 7 Select NPV Devices**

Select one or more NPV devices or NPV capable switches. NPV capable switches can be configured as NPV devices. MD5 9124, 9134 and Blade Server v3.2(2) or later are NPV capable.

Select	NPV Device	IP Address	NPV State
<input checked="" type="checkbox"/>	sw4	172.22.34.11	Enabled
<input checked="" type="checkbox"/>	sw3	172.22.34.97	Enabled

**Note: Please ensure boot variables are set before enabling NPV feature and that there are no port-channels configured.**

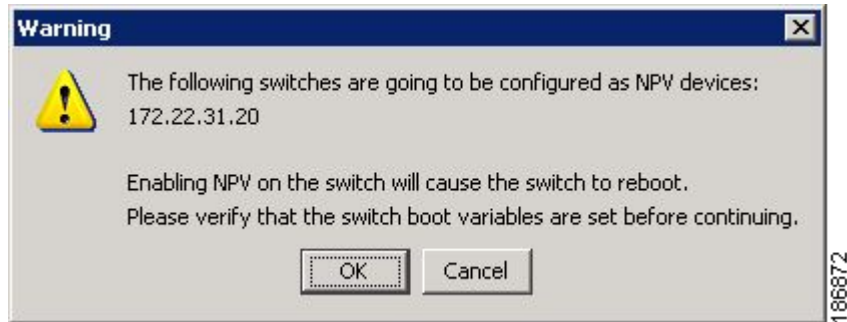
Next Cancel

A table lists all the available NPV-capable switches including the switches on which NPV is not yet enabled. Check the check boxes to select the required NPV devices. On devices that are not NPV enabled, this wizard will enable NPV on the devices in the final step.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

If you choose switches that are NPV disabled and click **Next**, a warning message appears with a list of IP addresses of the NPV devices on which NPV will be enabled. Enabling NPV on the switch will result in reboot of the switch. Boot variables of the switches have to be set, to enable NPV on them through this wizard (see [Figure 9-14](#)).

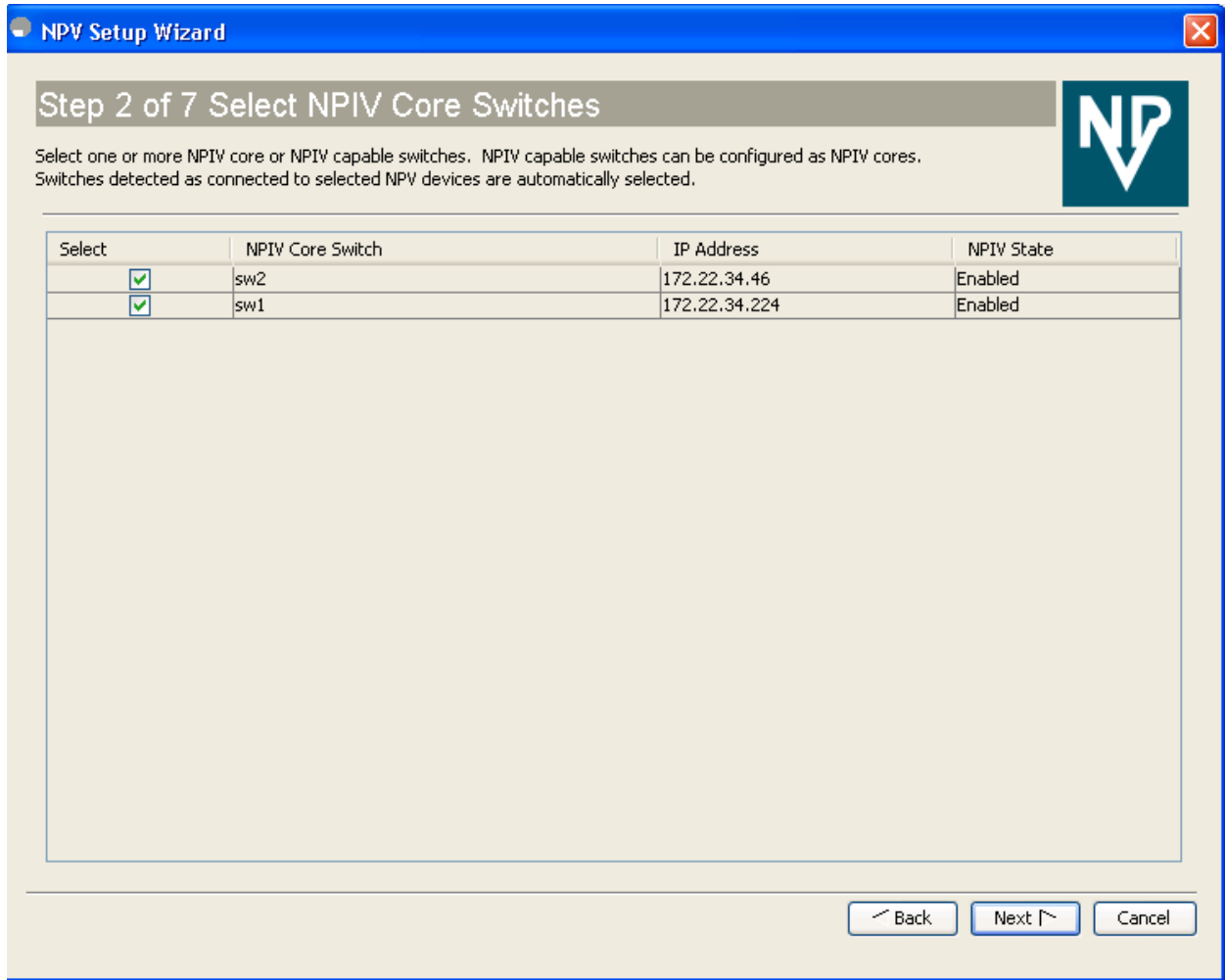
**Figure 9-14**      **Warning to Enable NPV Feature on NPV-Capable Switches**



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Step 3** Select the NPIV core switches (see [Figure 9-15](#)).

**Figure 9-15** Selecting the NPIV Core Switches



**NPV Setup Wizard**

**Step 2 of 7 Select NPIV Core Switches**

Select one or more NPIV core or NPIV capable switches. NPIV capable switches can be configured as NPIV cores. Switches detected as connected to selected NPV devices are automatically selected.

Select	NPIV Core Switch	IP Address	NPIV State
<input checked="" type="checkbox"/>	sw2	172.22.34.46	Enabled
<input checked="" type="checkbox"/>	sw1	172.22.34.224	Enabled

Back Next Cancel

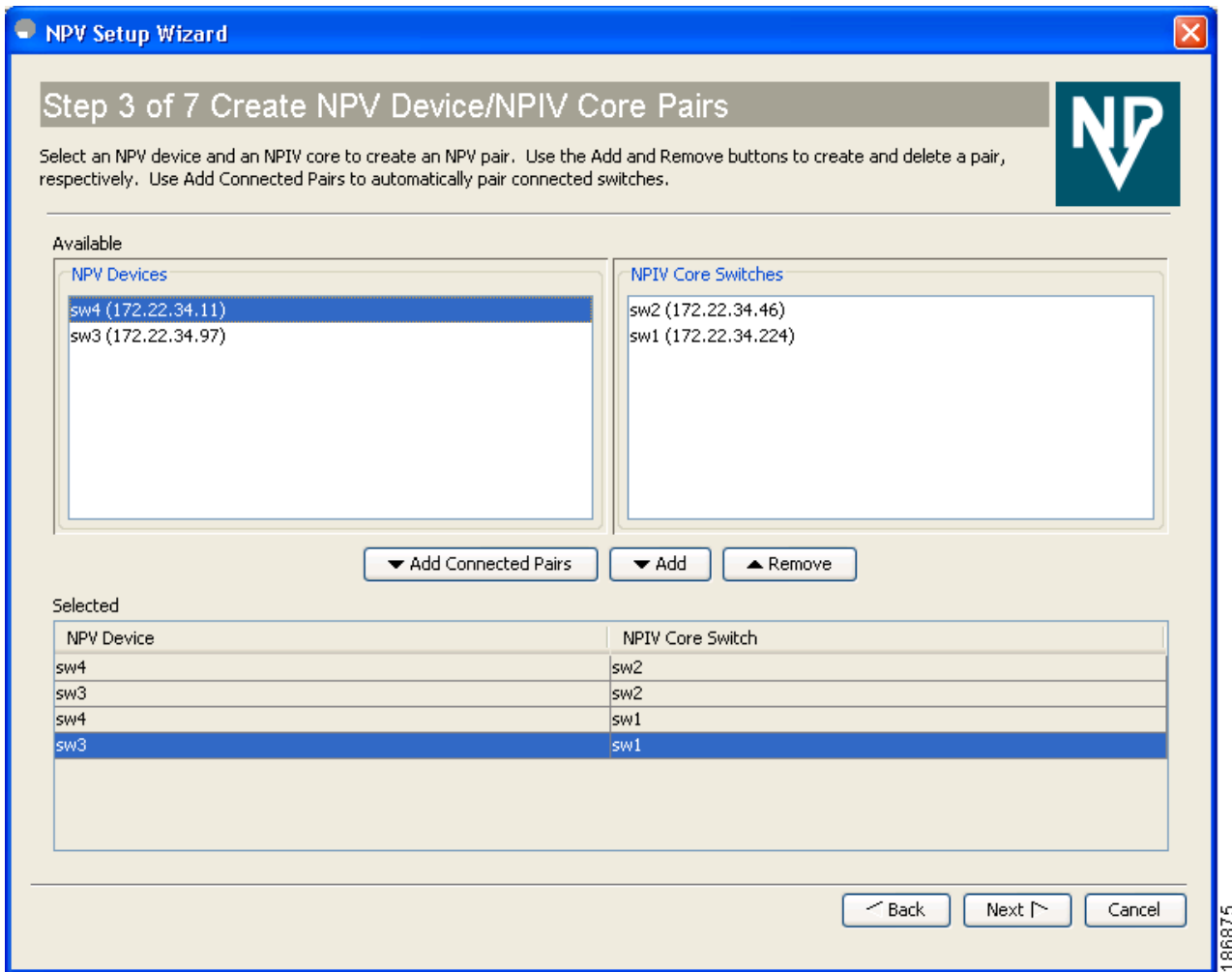
186874

Check the check boxes to select the required NPIV core switches. The table lists all the available NPIV core switches including the core switches that have not yet enabled the NPIV feature. NPIV core switches that are not NPIV-enabled. This wizard will enable NPIV in the final step.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Step 4** Create new NPV device and NPIV core switch pairs as required (see [Figure 9-16](#)).

**Figure 9-16** Creating NPV Device and NPIV Core Switch Pairs



Based on selections in the previous steps, the wizard displays all available NPV devices and NPIV core switches in separate lists. You can select one from each list and click **Add** or **Remove** buttons to create new NPV device and NPIV core switch combinations or pairs.

The NPV wizard checks if there are any NPIV core switches that are already connected to the NPV devices selected in the previous step. Click the **Add Connected Pairs** button to add a list of all the existing pairs that are interconnected, to the Selected table.

The Selected table is then populated with both the existing and the intended pairs. Each NPIV core switch can be paired with multiple NPV devices.

After Step 6, the wizard prompts you to physically connect the new pairs that are not yet connected.

On the switches that are not paired, the NPV wizard enables the NPV and NPIV modes. However, there is a possibility that these unpaired switches may be segmented and lose their presence on the fabric.



## Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

After you click the Next button in Step 3 of 6, the wizard determines if you have selected all the connected pairs. A warning message is displayed (See [Figure 9-19](#)) that lists all the connected pairs that you have not selected and warns that they will be segmented after the NPV setup.



### Note

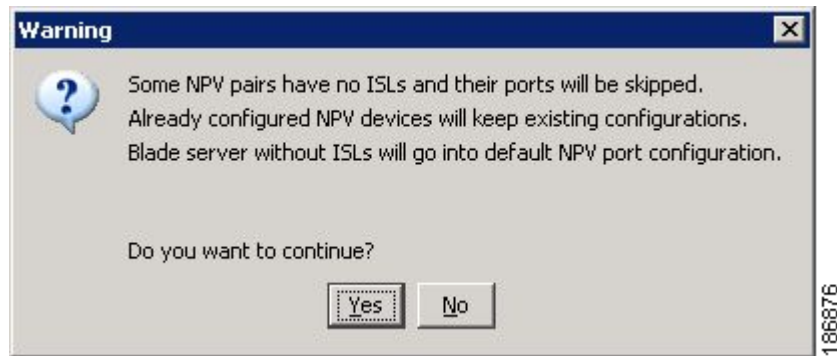
- NPV wizard does not detect ports that are in a channel group and that are not connected by ISLs. The wizard does not configure any port in a Port Channel Group to F ports on the core switch. Port channel grouping is not applicable to NPV devices. (See [Figure 9-17](#).)
- Remove the port channel groups if you need to select those particular ports as F ports during the setup. For more information, see the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.

**Figure 9-17 Port Channel Group Detected**



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 9-18**      **Warning, NPV Setup Wizard**



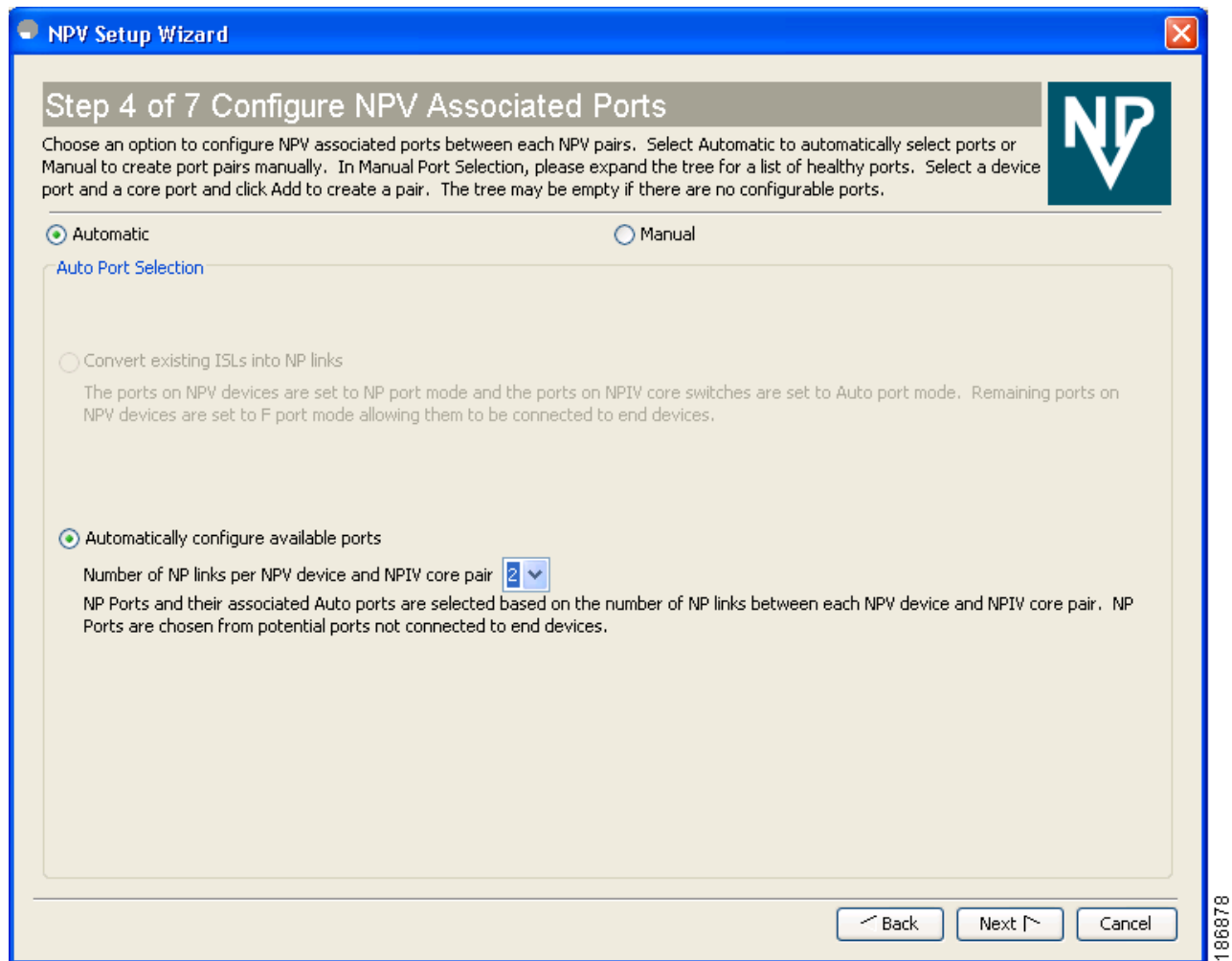
**Figure 9-19**      **Warning, NPV Setup Wizard Continued**



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 5** You can configure NPV associated ports either through automated or manual methods. (See [Figure 9-20](#).)

**Figure 9-20** Configuring NPV Associated Ports by the Automatic Method



The Auto Port Selection has two options:

- Choosing the first option allows you to convert the existing ISLs to be run as NPV links. If you want ISLs to take priority, then choose the Convert existing ISLs option.

The wizard discovers ISLs (Up or Down) between the selected switches, that are available at the time of wizard launch.

- Choosing the second option allows the NPV wizard to automatically configure free ports for NPV usage. In the second option, you can choose up to a maximum of six additional NPV links per NPV device and core switch pair.

During automatic port selection on the NPV switch, ports are defined as licensed FC ports with “Operational status” = Auto and “Status Cause” = none(2), offline(8), or sfp not present(29), and “Operational Status” = TE or E.

Ports on the NPV switch are selected in the following way:

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

The ISLs are considered in the second method. The selection algorithm spreads out the free port selections, so that the first port in every four ports is selected, for example, the 1st, 5th, 9th, etc. If after going through the 1st port in every four ports, you still have not selected enough ports (because the preferred ports were not free) then move to the second port in every four, for example, the 2nd, 6th, 10th etc. Different switches have different port preferences.

Ports on the NPIV switch are selected in the following way:

During automatic port selection on the NPIV switch free ports are defined as ports that are licensed FC ports and ports that have "Operational status" = Auto and "Status Cause" =none(2), offline(8) or sfp not present(29). If the ports are found in any other operational state, (for example F, NP, E, TE etc), then they are considered used, except for E and TE ports that are in ISLs connected to NPV device switches that will be enabled for NPV mode in this wizard session, as they will be considered to be free. However, these ISL ports will not necessarily be the ports selected by the automatic port selection algorithm as they are treated no different then any other free port. If you want to convert those used ISL ports, then choose the Convert existing ISLs option first and then run the wizard a second time choosing Automatic port selection (option 2) to add additional links.

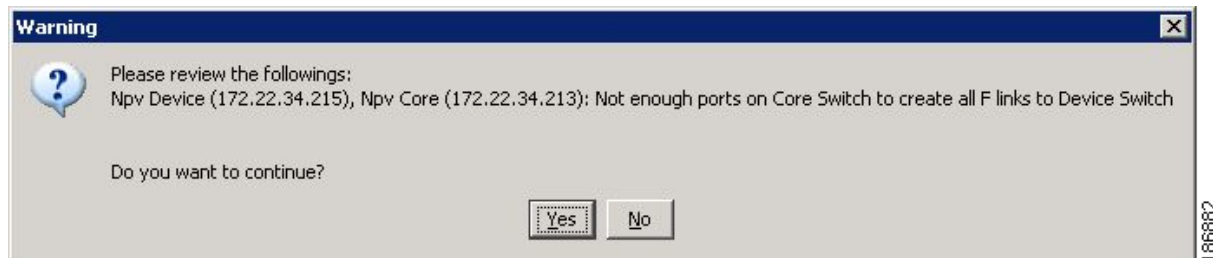
When you choose to configure ports from available ports, the wizard searches for ports that are not currently participating in NP link configuration. It is possible that all ports can be participating in NP port configuration. In that case a warning message is displayed. (See [Figure 9-21](#).)

**Note**

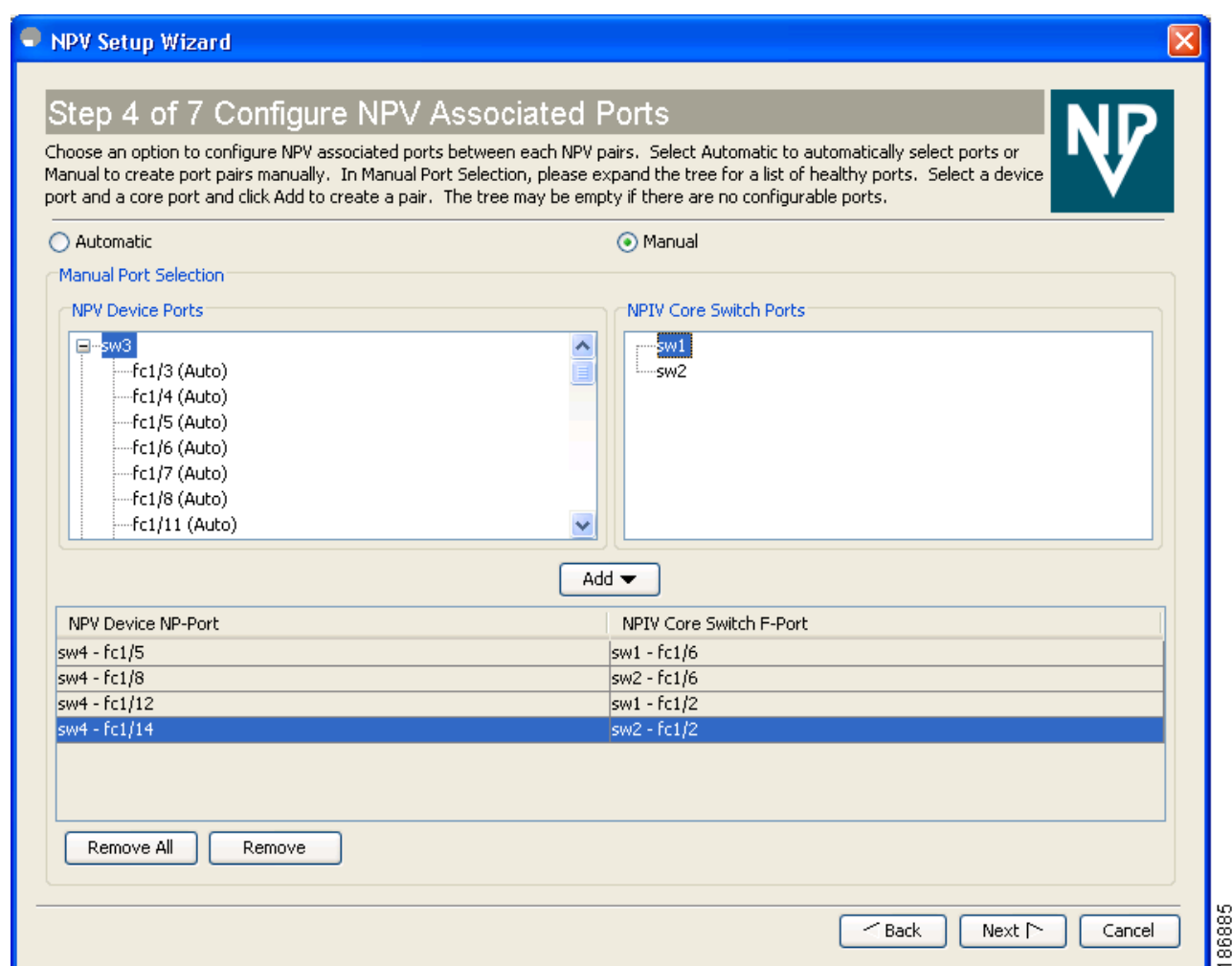
In both manual and automatic methods of configuring NPV associated ports, the ports that are unhealthy or that are in adminDown state are not considered during port selection.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 9-21 Warning, not Enough Number of Ports**



**Figure 9-22 Configuring NPV Associated Ports by the Manual Method**



Select the **Manual** method to manually create port pairs (see [Figure 9-22](#).) Click on a satellite switch and select the NP device port expanded under each of the NPV switches listed. Then select the required F port on the NPIV core switch and click **Add** for them to pair.

## ***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

During manual selection from the list for NPV and NPIV, ports are defined as the licensed FC ports with "Operational status" = Auto and "Status Cause" = none(2), offline(8), or sfp not present(29) and "Operational Status" = TE or E.



**Note** Failed ports with the Auto operational status will not be listed. Failed ports with the E operational status will be listed and available for NPV configuration.

Based on user selection, the wizard decides which ports are set to NP ports on the NPV device side and which are F ports on the core switch side to make an NPV connection.



**Note**

Some times the **Manual** selection in step 4 does not show any port when the NPV switch tree is expanded as the NPV Wizard filters out ports that are in fail or down status. Only healthy ports are made visible in the NPV Switch tree. Check your port settings.

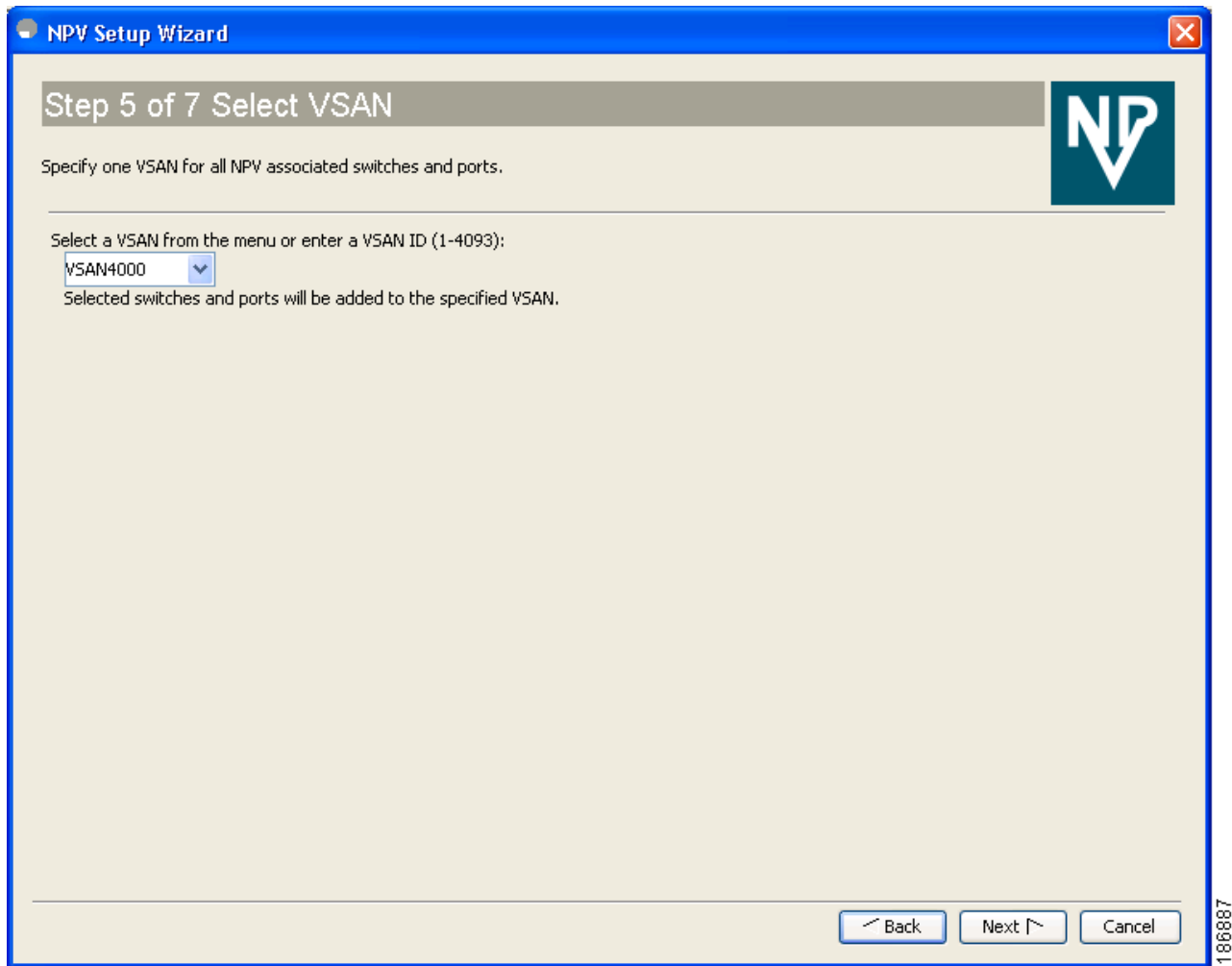
**Figure 9-23 Message Alert to Connect Port Pair**



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Step 6** Select a VSAN as shown in [Figure 9-24](#).

**Figure 9-24** Selecting a VSAN



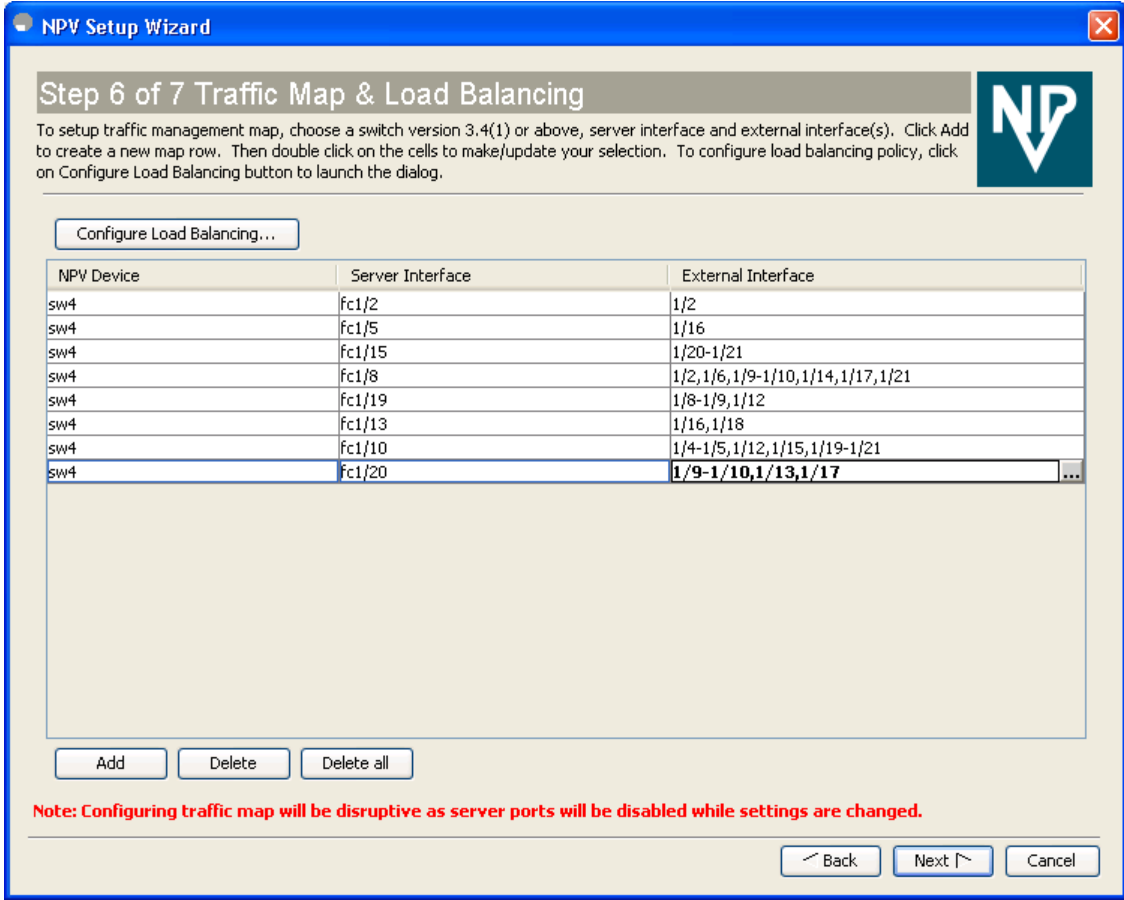
From the drop-down list select a VSAN or enter a VSAN ID to specify the VSAN. All selected NPV devices and NPIV core switches are added to the specified VSAN. All ports on the selected NPV devices and associated ports on the NPIV core switches are added to the VSAN.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

The VSAN configuration is applied in the final step.

**Step 7** Map the server interfaces with external interfaces for disruptive load balancing as shown in Figure 9-25.

**Figure 9-25 Mapping Server Interfaces with External Interfaces for Load Balancing**



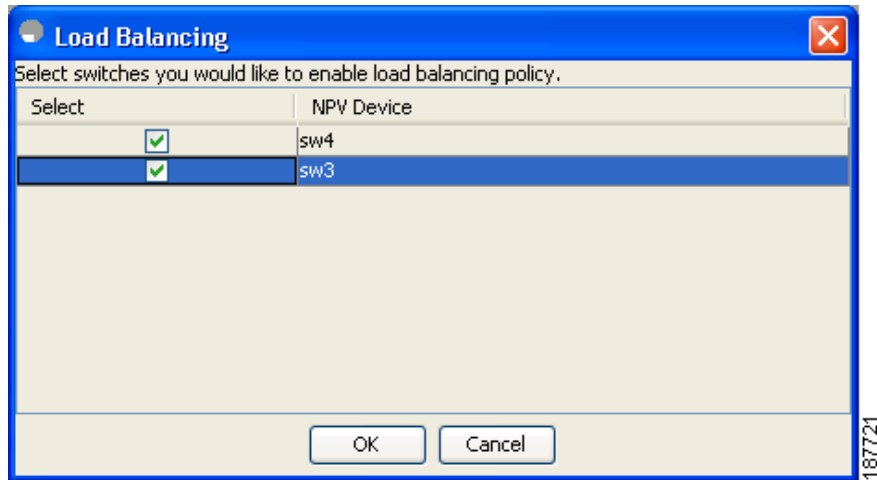
187720



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

To select the NPV devices that need load balancing, click **Configure Load Balancing**, and then select the NPV devices for disruptive load balancing as shown in Figure 9-26.

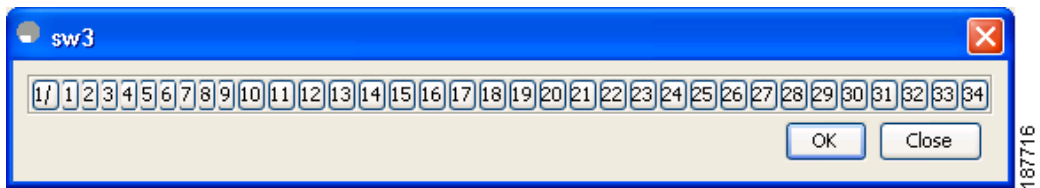
**Figure 9-26** Select the NPV Devices for Load Balancing



To set up the traffic management map, select at least one switch of version 4.1(1a) or above, a server interface, and external interfaces. To add a map entry, follow these steps:

- Click **Add** to create a new map row.
- Double-click the NPV Device cell and select the switch from the drop-down list.
- Double-click the Server Interface cell and then type the port numbers or click the [...] button (not available on blade server switches) in the cell to display the port selection dialog box. In the port selection dialog box, click the numbered buttons to select the ports as shown in Figure 9-27.

**Figure 9-27** Select the Interfaces



**Note**

You can select only one Server Interface port in a row, but multiple External Interface ports can be mapped to it. Previously selected ports are disabled and cannot be selected.

- Double-click the External Interfaces cell and type the port numbers or click the [...] button (not available on blade server switches) in the cell to display the port selection dialog box. In the port selection dialog box, click the numbered buttons to select the ports as shown in Figure 9-27.

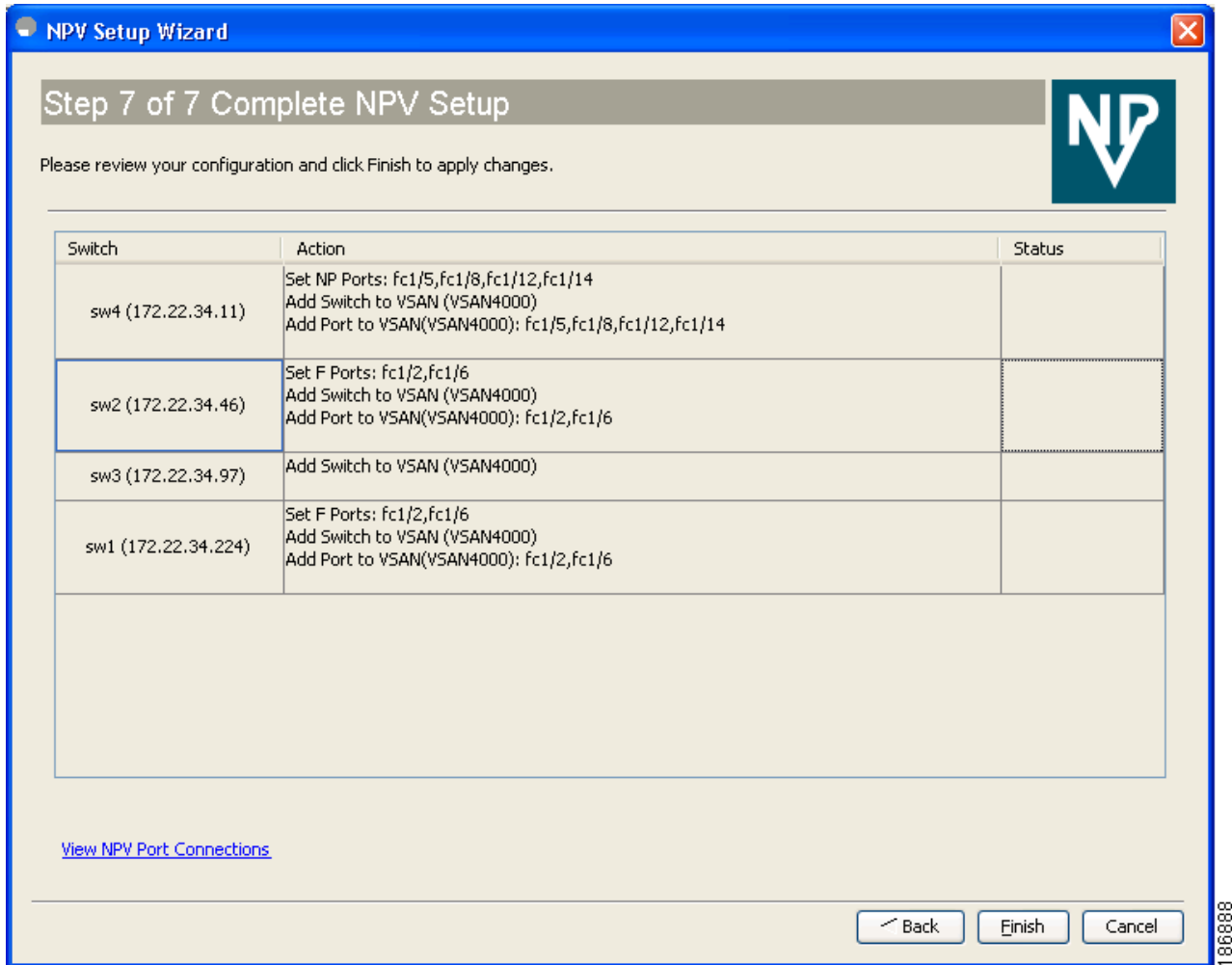
To delete an existing map entry, select the row, and then click **Delete**.

To delete all the existing map entries, click **Delete All**.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 8** Review all the NPV Setup configurations you entered in the earlier steps and click **Finish** to complete the setup as shown in [Figure 9-28](#).

**Figure 9-28** Completing the NPV Setup



**Enable Switch Feature** lists the switches, the impending actions against them with reference to features, and the resultant status.

**Set Port Type** lists the switches and the ports to be set on the switches to configure NPV associate ports.

**Configure VSAN** lists the switches and ports to be added to the specified VSAN.

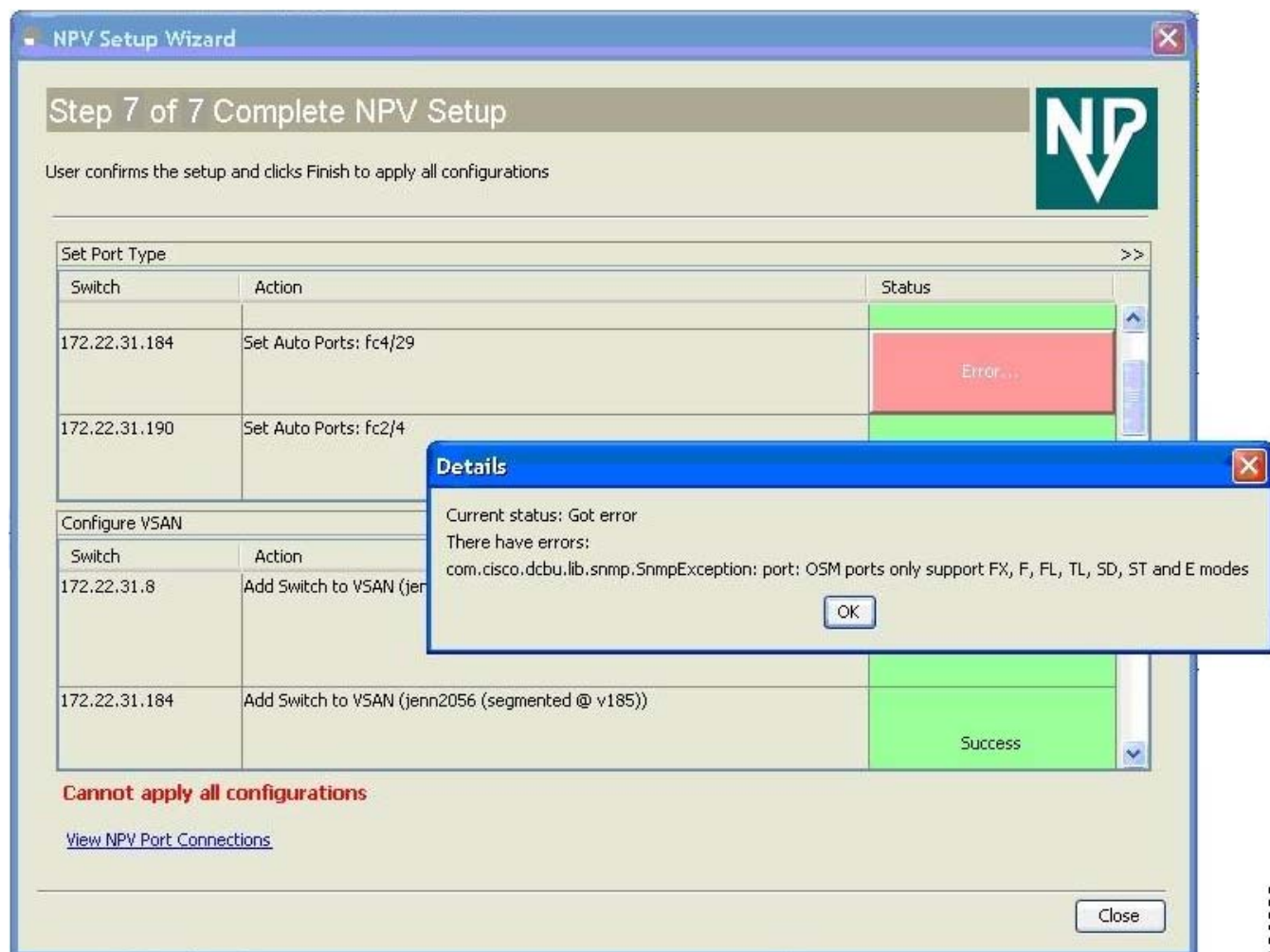
Click >> to view the expanded the panes. Click << to collapse the panes.

A progress bar at the bottom of the window indicates the overall extent of completion of the configuration tasks. A text message that runs below the progress bar indicates the current task in progress.

The status cells against each item indicate **In progress**, **Success**, and **Error** states. When a configuration cannot be applied, the status cell against the task is changed to **Error**. Click **Error** to view **Details**. A message is displayed in place of the progress bar stating, Cannot apply all configurations as shown in [Figure 9-29](#).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 9-29 Error in Applying Configurations and Details**

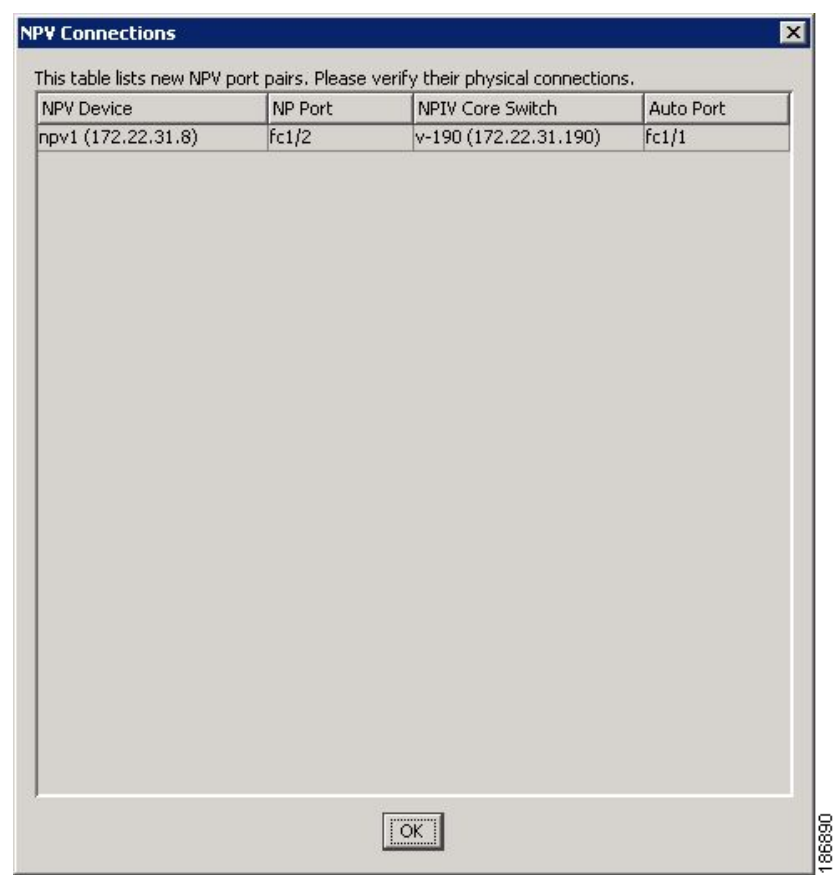


After the completion of all the tasks, a **View NPV Port Connections** link is displayed in the place of the progress bar. (See [Figure 9-29](#).)

Click **View NPV Port Connections** to view the NPV port connections in a table (See [Figure 9-31](#)). Refer to this list to verify the physical connections between NP Port on NPV devices and Auto ports on NPV core switches. The physical connections already exist for the ISLs and they have to be verified. In some cases when the physical connections do not exist, they have to be established manually.

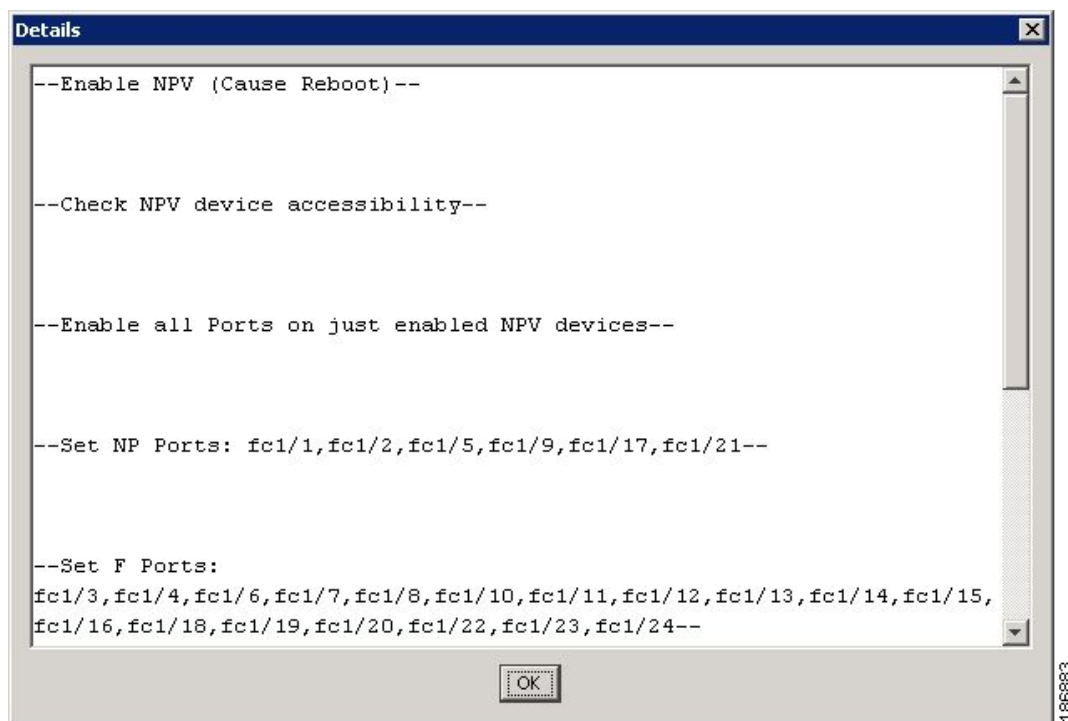
*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

**Figure 9-30**      **New NPV Port Pairs**



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 9-31** New NPV Port Pairs, Details



## DPVM Configuration

When NPV is enabled, the following requirements must be met before you configure DPVM on the NPV core switch:

- You must explicitly configure the WWN of the internal FLOGI in DPVM. If DPVM is configured on the NPV core switch for an end device that is connected to the NPV device, then that end device must be configured to be in the same VSAN. Logins from a device connected to an NPV device will fail if the device is configured to be in a different VSAN. To avoid VSAN mismatches, ensure that the internal FLOGI VSAN matches the port VSAN of the NP port.
- The first login from an NP port determines the VSAN of that port. If DPVM is configured for this first login, which is the internal login of the NPV device, then the NPV core switch's VSAN F port is located in that VSAN. Otherwise, the port VSAN remains unchanged.

For details about DPVM configuration, see the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.

## NPV and Port Security

Port security is enabled on the NPV core switch on a per interface basis. To enable port security on the NPV core switch for devices logging in via NPV, you must adhere to the following requirements:

- The internal FLOGI must be in the port security database; in this way, the port on the NPV core switch will allow communications/links.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- All the end device pWWNs must also be in the port security database.

Once these requirements are met, you can enable port security as you would in any other context. For details about enabling port security, see the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.



## CHAPTER 10

# Configuring FlexAttach Virtual pWWN

---

This chapter describes the FlexAttach virtual port world-wide name (pWWN) feature and includes the following sections:

- [About FlexAttach Virtual pWWN, page 10-1](#)
- [FlexAttach Virtual pWWN Guidelines and Requirements, page 10-2](#)
- [Configuring FlexAttach Virtual pWWN, page 10-2](#)
- [Using the Server Admin FlexAttach Wizards, page 10-9](#)
- [Difference Between San Device Virtualization and FlexAttach Port Virtualization, page 10-25](#)

## About FlexAttach Virtual pWWN

FlexAttach virtual pWWN feature facilitates server and configuration management. In a SAN environment, the server installation or replacement, requires interaction and coordination among the SAN and server administrators. For coordination, it is important that the SAN configuration does not change when a new server is installed, or when an existing server is replaced. FlexAttach virtual pWWN minimizes the interaction between the server administrator and the SAN administrator by abstracting the real pWWN using virtual pWWNs.

When FlexAttach virtual pWWN is enabled on an interface, a virtual pWWN is assigned to the server interface. The real pWWN is replaced by a virtual pWWN, which is used for a SAN configuration such as zoning.

Server administrators can benefit from FlexAttach in the following scenarios:

- **Pre-configure**—Pre-configure SAN for new servers that are not available physically yet. For example, they may be on order. FlexAttach can be enabled on the ports designated for the new servers and use the virtual WWNs assigned for configuring SAN. The new servers are then plugged into the fabric without any change needed in the SAN.
- **Replacement to the same port**—A failed server can be replaced onto the same port without changing the SAN. The new server gets a same pWWN as the failed server because the virtual pWWN is assigned to the port.
- **Replacement to (spare)**—A spare server, which is on the same NPV device or a different NPV device) can be brought online without changes to the SAN. This action is achieved by moving the virtual port WWN from the current server port to the spare port.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- **Server Mobility**—A server can be moved to another port on the same NPV device or another NPV device without changing the SAN. This is accomplished by moving the virtual pWWN to the new port. No change is needed if FlexAttach was configured using the physical port WWN of the server to the virtual port WWN mapping.

## FlexAttach Virtual pWWN Guidelines and Requirements

Following are recommended guidelines and requirements when deploying FlexAttach virtual pWWN:

- FlexAttach configuration is supported only on NPV switches.
- Cisco Fabric Services (CFS) IP version 4 (IPv4) distribution should be enabled.
- Virtual WWNs should be unique across the fabric.

## Configuring FlexAttach Virtual pWWN

This section describes how to configure FlexAttach virtual pWWN feature and includes the following topics:

- [Enabling FlexAttach Virtual pWWN, page 10-2](#)
- [Debugging FlexAttach Virtual pWWN, page 10-8](#)
- [Security Settings for FlexAttach Virtual pWWN, page 10-8](#)
- [FlexAttach Virtual pWWN CFS Distribution, page 10-9](#)

## Enabling FlexAttach Virtual pWWN

The FlexAttach virtual pWWN feature is enabled automatically, manually, or by mapping pWWN to virtual pWWN. [Figure 10-1](#) shows how the FlexAttach virtual pWWN feature is enabled.

### Automatically Enabling FlexAttach Virtual pWWN

The virtual pWWN is enabled automatically on all the NPV switches or per port on the NPV box. When enabled automatically, a virtual WWN is generated from the device switch WWN. This WWN is used as the virtual pWWN. Virtual pWWNs are generated using the local switch WWNs.



#### Note

The port must be in a shut state when the virtual pWWN is enabled.

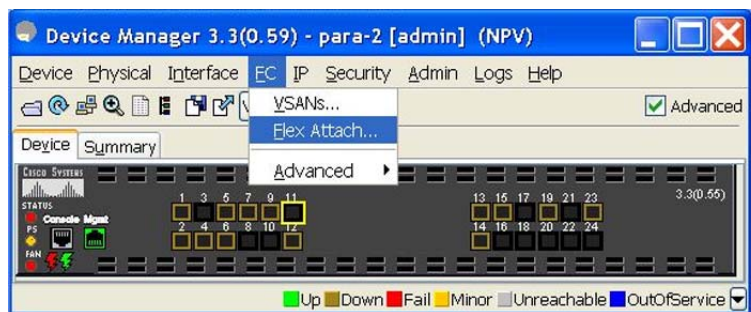
To enable virtual pWWN automatically for all the interfaces, follow these steps:

- Step 1** From the Device Manager menu bar, select **FC > FlexAttach**. ([Figure 10-1](#)).



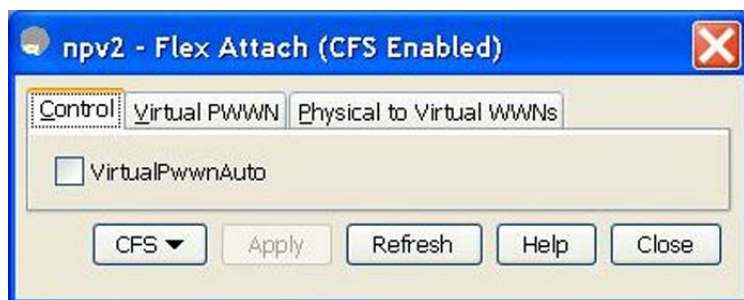
**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-1 FlexAttach in Device Manager**



You see the FlexAttach window. (Figure 10-2).

**Figure 10-2 FlexAttach Window in Device Manager**



- Step 2** Check the **VirtualPwwnAuto** check box to enable automatic generation of virtual WWNs on all the fabric port interfaces.



**Note**

- When the *interface-list* value is not included in the command, virtual pWWN is enabled globally.
- All the interfaces mentioned in the *interface-list* value must be in a shut state.

## Launching FlexAttach in Fabric Manager

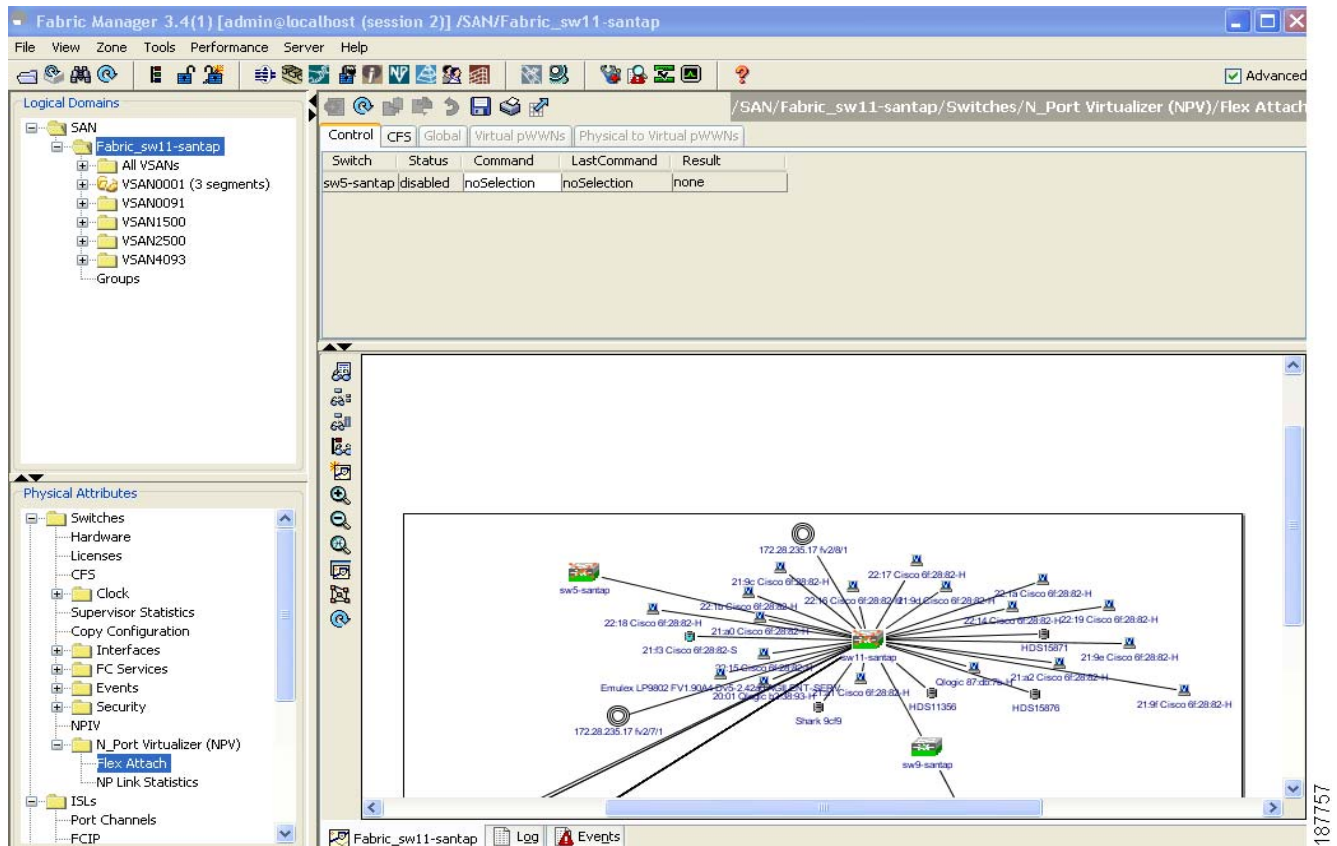
To launch FlexAttach in Fabric Manager, follow these steps:

- Step 1** In the Logical Domains pane, select a switch.
- Step 2** In the Physical Attributes pane, expand **Switches > NPIV**.
- Step 3** Select **NPIV > N\_Port Virtualizer (NPV) > FlexAttach**.

The FlexAttach configuration pane appears to the right. (Figure 10-3).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-3 FlexAttach Menu**



## Manually Enabling FlexAttach Virtual pWWN

You can manually assign a WWN to the interface, without generating it through the switch. Several checks are done by the NPV core to ensure the uniqueness of virtual pWWNs in the switch. When duplicate virtual pWWNs are configured, the subsequent logins are rejected by the NPV core switch.



### Note

- Some ports may be in automode, some in manual mode, and the virtual pWWNs need not be assigned.
- The port must be in a shut state when a virtual pWWN is enabled.

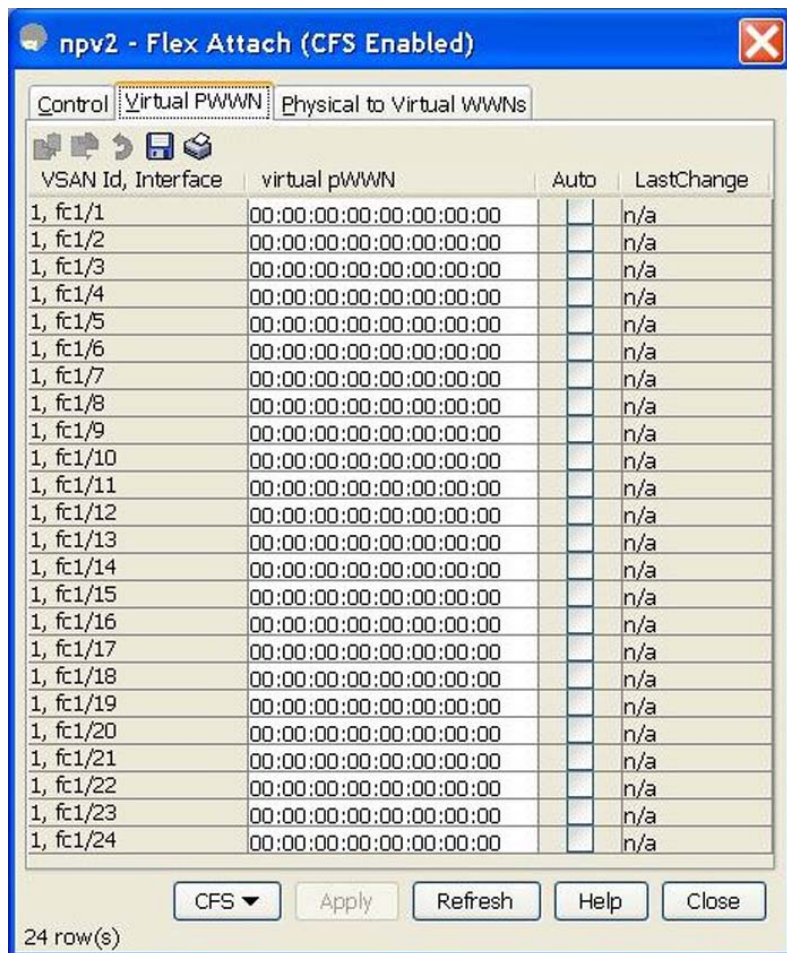
To enable virtual pWWN on each interface manually, follow these steps:

**Step 1** Click the **Virtual pWWN** tab.

A list of interfaces is displayed. (Figure 10-4).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-4 Virtual PWWN Tab View in Device Manager**



The Virtual pWWN tab view displays a list of the interfaces.

**Step 2** Check the **Auto** check box to automatically generate the virtual pWWN value for the selected interface.



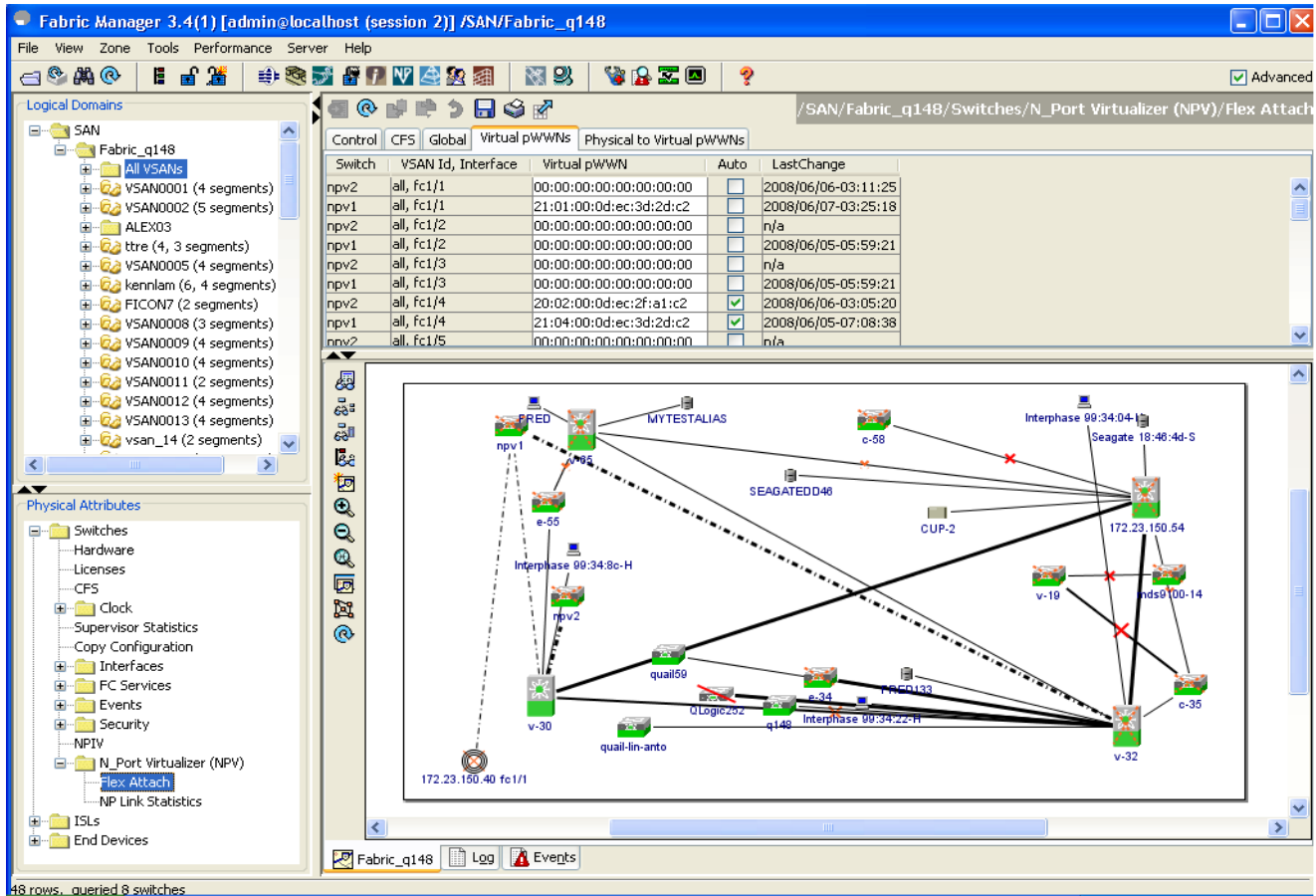
**Note**

The interface mentioned in the interface value must be in a shut state.

The virtual port WWN value for the selected interface in Fabric Manager is automatically generated. (Figure 10-5).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-5** Virtual pWWN Tab View in Fabric Manager



#### Note

The interface mentioned in the *interface* value must be in a shut state.

## Mapping pWWN to Virtual pWWN

You can configure virtual pWWNs through real pWWNs. This process is required for NPIV hosts containing multiple pWWNs, of which only FLOGI is mapped to the virtual pWWN. Subsequent FDSIDs will have different mappings.

Several checks are done by the NPV core to ensure the uniqueness of virtual pWWNs in the switch across the NPV switches. When duplicate virtual pWWNs are configured, the subsequent logins are rejected by the NPV core switch.

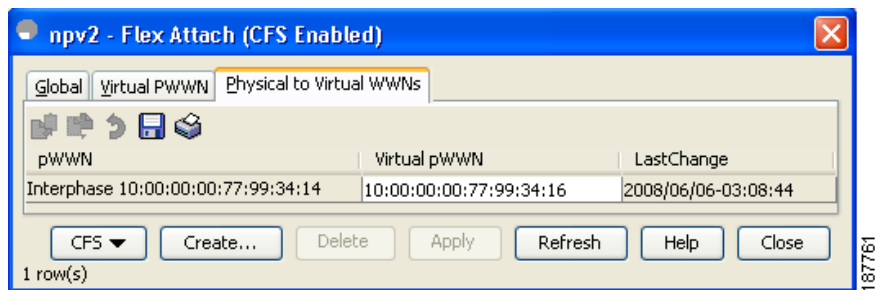
To map pWWN to virtual pWWN, follow these steps:

**Step 1** In the FlexAttach window, select the **Physical to Virtual WWNs** tab.

You see the **Physical to Virtual WWNs** tab view (see [Figure 10-6](#)).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-6 Physical to Virtual WWNs Tab View in Device Manager**



The LastChange field displays the time when the virtual pWWN was changed.

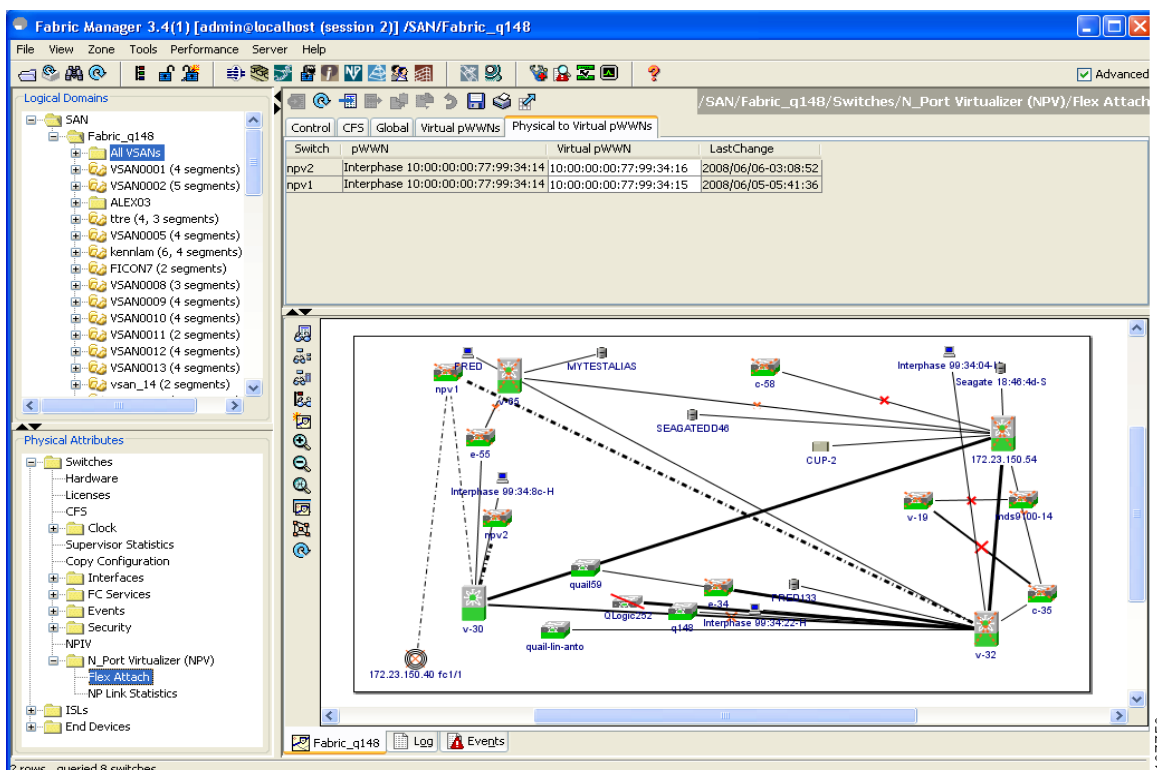


**Note**

The interface must be in a shut state and the specified virtual pWWN should not be logged in.

The [Figure 10-7](#) shows the Physical to Virtual pWWNs tab view in the Fabric Manager.

**Figure 10-7 Physical to Virtual pWWNs Tab View in Fabric Manager**



**Note**

The specified virtual pWWN and the real pWWN must not be logged in.



***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Debugging FlexAttach Virtual pWWN

Table 10-1 lists the errors that might be displayed and provides the workarounds.

**Table 10-1 FlexAttach Errors and Workarounds**

Error	Description	Workaround
fc1/1 : interface is not down	FlexAttach configuration fails because the configuration is enabled for an active interface with the operation state as up.	To move the port to the shut state, enable the FlexAttach configuration, and then move the port to no shut state.
FlexAttach configuration is not distributed to the peers	The FlexAttach configuration on one peer NPV is not available to any other peer NPV.	FlexAttach configuration will not be distributed if <b>cfs ipv4 distribute</b> , or <b>cfs ipv6 distribute</b> is disabled. Enable <b>cfs ipv4 distribute</b> , or <b>cfs ipv6 distribute</b> .
Even with CFS distribution enabled Inagua does not become a peer with other NPVs	CFS over IP is enabled, and the Inagua in one blade center is not the peer NPV for other NPVs.	CFS over IP uses IP multicast to discover the NPV peers in the network. IBM MM does not support multicast and cannot act as a peer with NPV. This prevents the FlexAttach configuration from getting distributed to other peer NPVs in the network.
NP port uses physical pWWN instead of virtual pWWN configured through FlexAttach	This occurs when NP port uses physical pWWN instead of virtual pWWN, that is configured through FlexAttach.	FlexAttach is supported on server interfaces like F ports, and not on external interfaces such as NP ports.
real port WWN and virtual WWN cannot be same	This occurs when you try to configure FlexAttach with a similar value for pWWN and virtual pWWN.	Use different values for pWWN and virtual pWWN, as similar values for pWWN and virtual pWWN are not allowed.
Virtual port WWN already exists	This occurs when you try to configure an already defined pWWN to a different interface.	Use an undefined virtual pWWN for a new interface.

## Security Settings for FlexAttach Virtual pWWN

Security settings for the FlexAttach virtual pWWN feature are done by port security at the NPV core. Node WWN of the end device is used to provide physical security.

For more details on enabling port security, refer to the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.

*Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)*

## FlexAttach Virtual pWWN CFS Distribution

The FlexAttach virtual pWWN configuration is distributed for CFS through IPv4, and is enabled by default. The FlexAttach virtual pWWN distribution, by default, is on CFS region 201. The CFS region 201 links only to the NPV-enabled switches. Other CFS features such as syslog is on region 0. Region 0 will be linked through IPv4 for all NPV switches on the same physical fabric. If CFS has an option to link through IPv4 or ISL, then CFS will select the ISL path.



**Note**

NPV switches do not have ISL (E or TE ports) and are linked through IPv4.

## Using the Server Admin FlexAttach Wizards

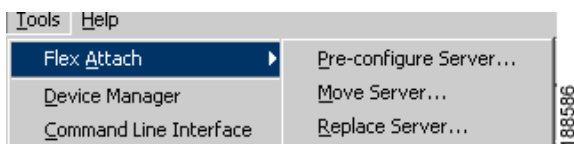
As in Fabric Manager Release 4.1(1) and later, the Server Admin perspective view of the Fabric Manager GUI provides the following FlexAttach wizards, which the Fabric Manager users with server-admin role can use to configure FlexAttach:

- [Pre-Configuring FlexAttach for a New Server, page 10-9](#)
- [Moving a Server to Another Port or Switch, page 10-15](#)
- [Replacing a Server with Another Server, page 10-19](#)

To access the FlexAttach wizards, follow these steps:

- Step 1** Log in to Fabric Manager with a username and password that has the server-admin role assigned.
- Step 2** Discover and open the fabric on which you want to configure FlexAttach.
- Step 3** In the Fabric Manager window displayed, select **Tools > FlexAttach** to display the list of wizards. (Figure 10-8).

**Figure 10-8** FlexAttach Wizards Menu Bar



## Pre-Configuring FlexAttach for a New Server

Using the Pre-configure Server wizard, you can configure FlexAttach for servers that are not physically available currently. FlexAttach can be enabled on the ports designated for the new servers and can use the virtual WWNs assigned for configuring SAN. When the new servers are available, the servers can then be plugged into the fabric without any change needed in the SAN.

The Pre-Configure Server wizard can be used to accomplish the following tasks:

- [Pre-Configuring FlexAttach for All the Ports, page 10-10](#)
- [Pre-Configuring FlexAttach for Each Port Individually, page 10-12](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Pre-Configuring FlexAttach for All the Ports

Using the Pre-Configure Server Basic configuration wizard, you can set the following port configurations for all the ports in one or more switches in common:

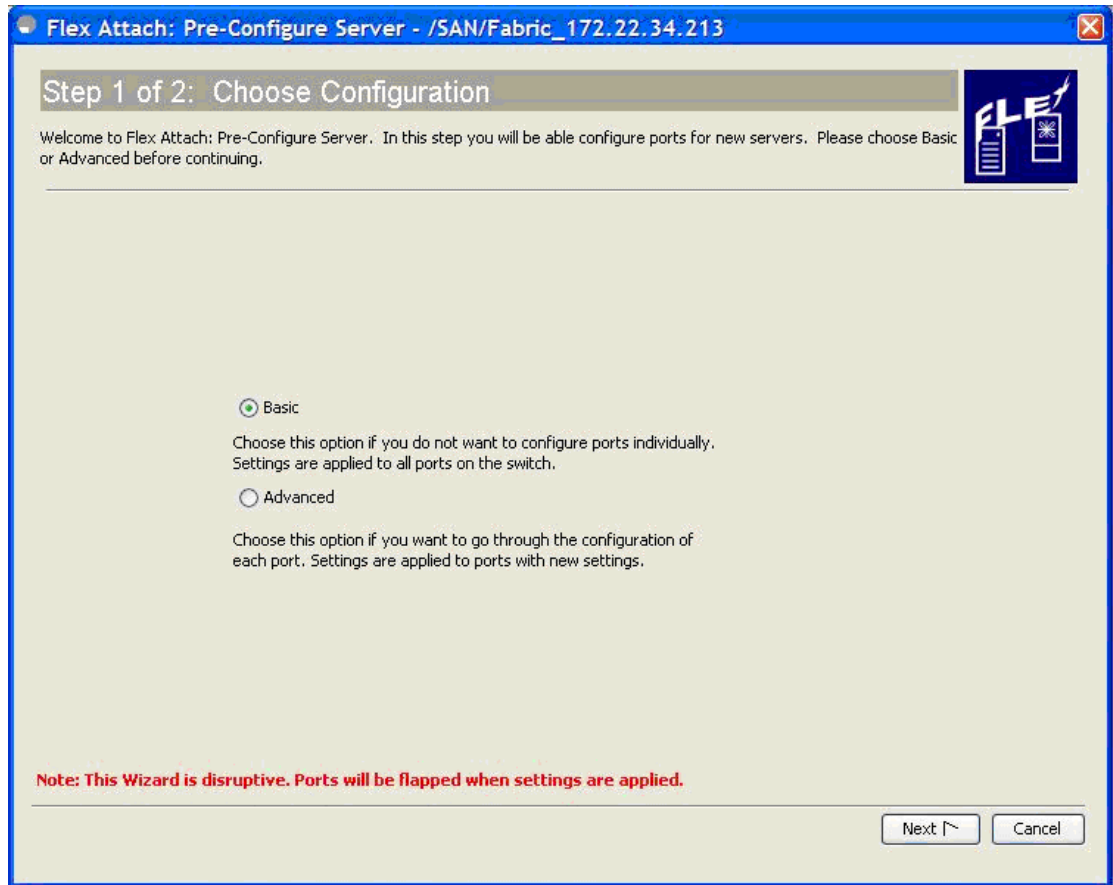
- Enable or disable FlexAttach Auto on all ports
- Set the default VSAN ID for all the ports
- Set the interface status for all the ports.

To pre-configure a common setting for all the ports in one or more switches, follow these steps:

**Step 1** In the Fabric Manger window, select **Tools > FlexAttach > Pre-configure Server**.

The Pre-Configure Wizard is displayed. (Figure 10-9)

**Figure 10-9 Pre-Configure Server Wizard**



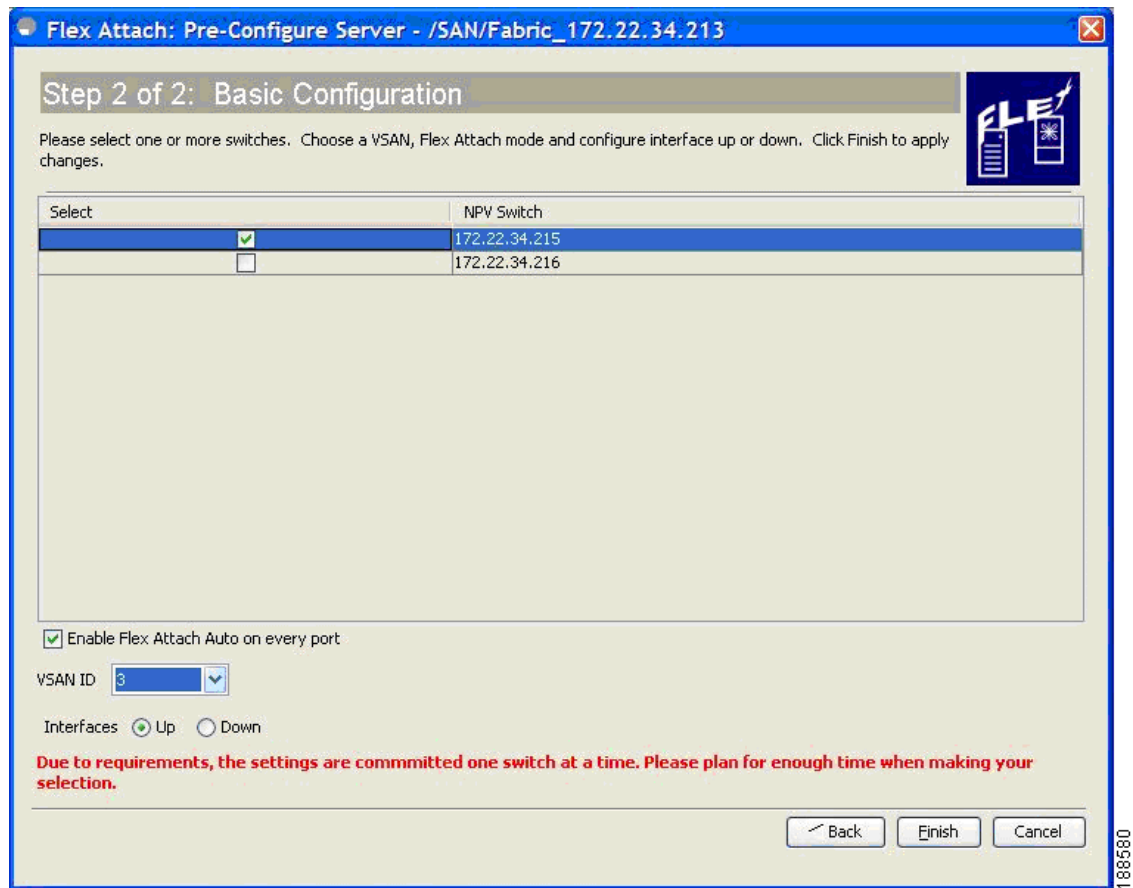
**Step 2** In the Pre-Configure Server window, click the **Basic** radio button to configure a common setting to all the ports on one or more switches.

The Basic Configuration window is displayed. (Figure 10-10)



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-10 Pre Configure Server - Basic Configuration**



- Step 3** In the Basic Configuration window, check the check box to select one or more switches from the list of NPV switches in the fabric.
- Step 4** Check the **Enable FlexAttach Auto on every port** check box to enable FlexAttach on all the ports of all the selected switches.
- Step 5** (Optional) From the VSAN ID drop-down list, select a VSAN ID to assign the selected VSAN ID to all the ports.



**Note** Only the set of VSANs to which all the selected switches belong are listed. If no VSAN ID is selected, then the existing VSAN configuration is retained.

- Step 6** Click the **Up** or **Down** radio button to assign the selected interface status.

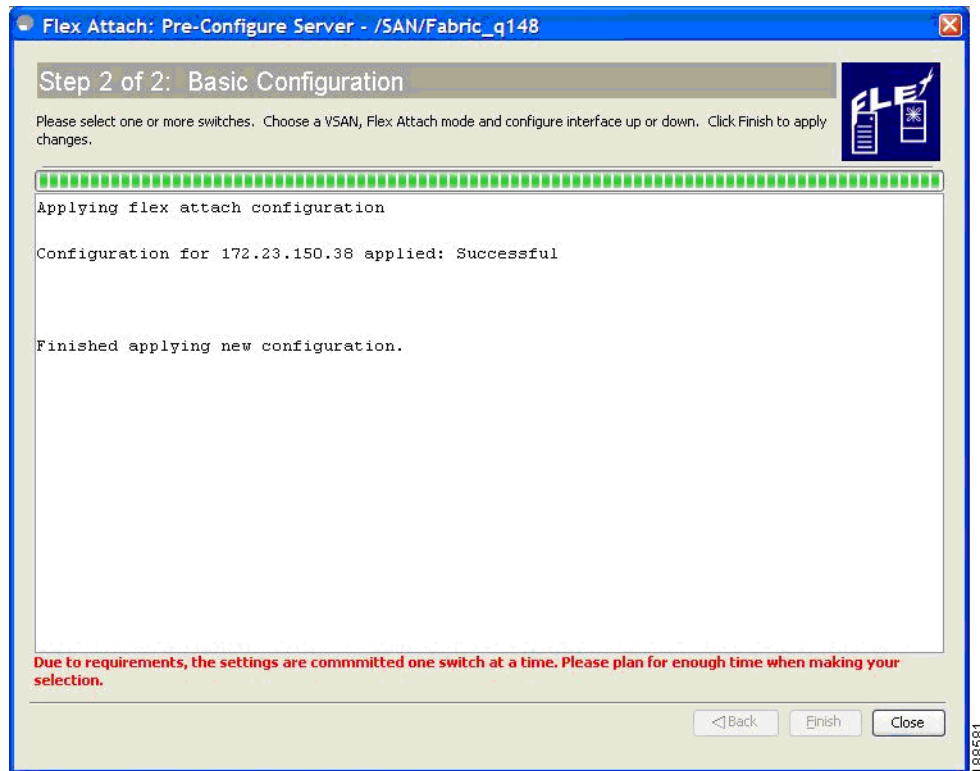


**Note** The status of only the F ports in the selected switches will be brought to up or down state.

- Step 7** Click **Finish** to pre-configure the selected settings to all the ports on all the selected switches. The Configuration window is displayed with the finished message. (Figure 10-11)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-11 Pre-Configure Server - Finish**



## Pre-Configuring FlexAttach for Each Port Individually

Using the Pre-Configure Server Advanced configuration wizard, you can set the following port configurations for each port in one or more switches individually:

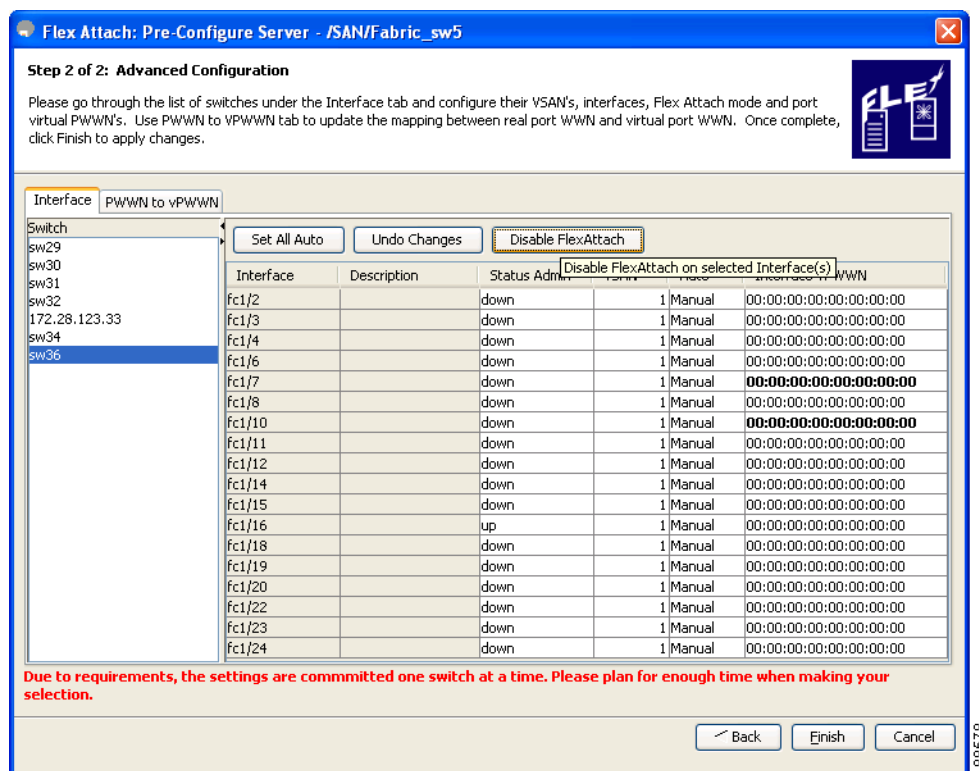
- Enable FlexAttach Auto on all ports.
- Enable FlexAttach Auto or Manual on individual ports.
- Set the virtual PWWN for ports where FlexAttach is enabled Manually.
- Set pWWN to vPWWN mapping.
- Set the default VSAN ID for each port.
- Set the Interface status for each port.

To pre-configure FlexAttach on each port individually, follow these steps:

- 
- Step 1** In the Fabric Manager window, select **Tools > FlexAttach > Pre-configure Server**.  
The Pre-Configure Server window is displayed. (Figure 10-9)
- Step 2** In the Pre-Configure Server window, click the **Advanced** radio button to configure FlexAttach on each port individually.  
The Pre-Configure Server Advanced configuration window is displayed. (Figure 10-12)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-12 Pre-Configure Server - Advanced Configuration**



**Note** From the **Interface** tab, you can select a switch from the list of switches displayed in the left pane and click **Disable FlexAttach** to change the switches to manual configuration. Select **Undo Changes** to return to the previous configuration.

**Step 3** In the Interface tab, click to select a switch from the list of switches displayed in the left pane.

The switch configuration details are displayed in the right pane with tabs and columns.

**Step 4** Configure the following settings, for each interface:

- In the Status column corresponding to the interface, double-click and then select up or down from the drop-down list.
- In the VSAN column corresponding to the interface, double-click and then select the VSAN ID from the drop-down list of existing VSAN IDs.
- In the Auto column corresponding to the interface, double-click and then select Auto to automatically enable FlexAttach or select Manual to manually enable FlexAttach later.
  - In the Interface vPWWN cell, enter the vPWWN if Manual was selected in the Auto FlexAttach configuration cell.



**Note** You can click **Set All Auto** to change all the interfaces with manual FlexAttach configuration to Auto on the selected switch. However, if a valid vPWWN value is already configured, then changing it to Auto does not change the configuration. Before you change from Manual to Auto, update the Interface vPWWN column with the 00:00:00:00:00:00:00 value.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

- Step 5** Repeat Step 3 through Step 4 for each switch.
- Step 6** Click the **PWWN to vPWWN** tab to configure pWWN to vPWWN mapping.  
The Advanced Configuration window is displayed. (Figure 10-13)

**Figure 10-13 Pre-Configure Server - PWWN to vPWWN Configuration**

Flex Attach: Pre-Configure Server - /SAN/Fabric\_q148

**Step 2 of 2: Advanced Configuration**

Please go through the list of switches and configure their VSAN's, interfaces, Flex Attach mode and port virtual PWWNs. Once complete, click Finish to apply changes.

Interface: PWWN to vPWWN

Select Switch: npv1

Add Row... Delete Row

pWWN	Virtual pWWN
00:00:00:00:00:00:01	00:00:00:00:00:00:02

Flex Attach: Pre-Configure Server: PWWN to Virtual PWWN

pWWN:

Virtual pWWN:

Create Cancel

Due to requirements, the settings are committed one switch at a time. Please plan for enough time when making your selection.

Back Finish Cancel

- Step 7** From the Select Switch drop-down list, select the switch to display the existing pWWN to Virtual PWWN mapping table for the CFS region to which the switch belongs, and then follow these steps to add vPWWN to vPWWN autopmap entries:
- Click **Add Row** to display the PWWN to vPWWN dialog box.
  - Enter the pWWN and the corresponding virtual pWWN.
  - Click **Create** to add the mapping list.



**Note** To delete an existing mapping, select the row, and then click **Delete Row**. Only one pWWN to vPWWN table can be updated at a time. To update the table for each CFS region, perform Step 6 through Step 8 for a switch from each CFS region.

- Step 8** Click **Finish** to complete the configurations for each port.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## Moving a Server to Another Port or Switch

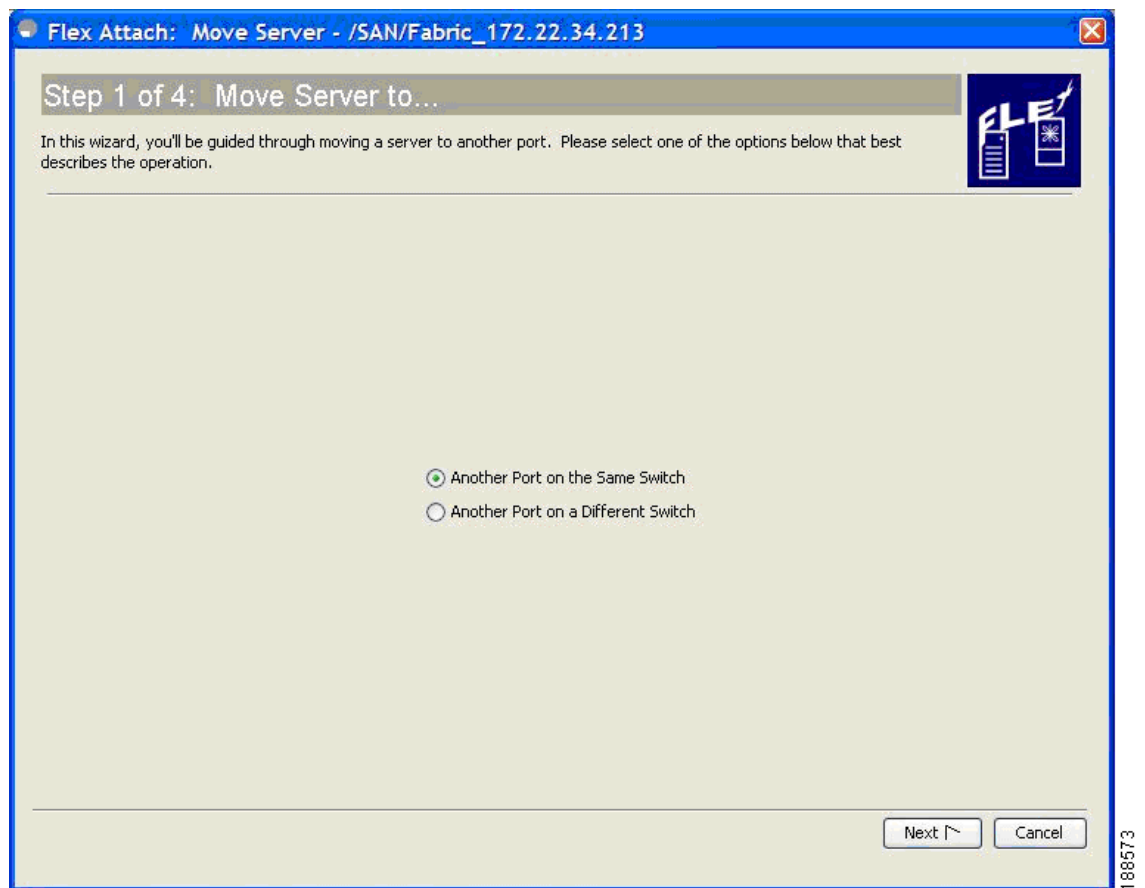
Using the Move Server wizard, you can move a server to another port on the same NPV device or another NPV device without changing the SAN. This is accomplished by moving the virtual pWWN to the new port. No change is needed if FlexAttach was configured using the physical port WWN of the server to the virtual port WWN mapping.

To move a server to a different port in the same switch, or in a different switch, follow these steps:

**Step 1** In the Fabric Manger window, select **Tools > FlexAttach > Move Server**.

The Move Server wizard is displayed. (Figure 10-14)

**Figure 10-14** Move Server Wizard



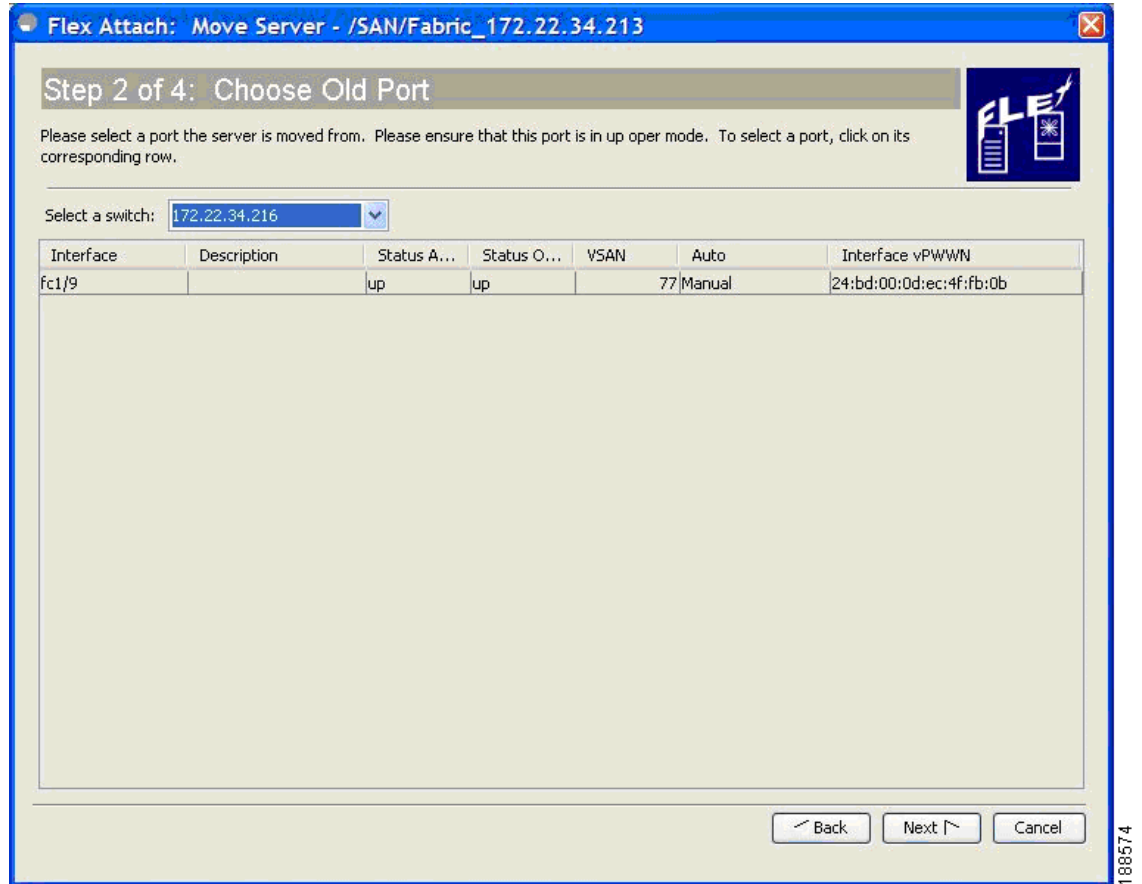
**Step 2** In the Move Server window, click the **Another Port on the Same Switch** radio button or click the **Another Port on a Different Switch** radio button.

**Step 3** Click **Next**.

The Move Port window is displayed. (Figure 10-15)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-15 Move Port Selection**



**Step 4** From the Select a Switch drop-down list, select the switch.

The switch ports are listed. To support moving a server from a failed port that is in down state, the ports in down state are also listed.

**Step 5** From the list of interfaces, select the port from which you want to move the server from.

**Step 6** Click **Next**.

The New Port window is displayed (Figure 10-16).

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-16 New Port Selection**

**Flex Attach: Move Server - /SAN/Fabric\_172.22.34.213**

**Step 3 of 4: Choose New Port**

Please select a new port the server is moved to. Please ensure that this port is not being used and in down oper mode. To select a port, click on its corresponding row.

Select a switch: 172.22.34.215

Interface	Description	Status A...	Status ...	VSAN	Auto	Interface vPWWN
fc1/1		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/2		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/3		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/4		down	down	1	Manual	00:00:00:00:00:00:00:00
<b>fc1/5</b>		<b>down</b>	<b>down</b>	<b>1</b>	<b>Manual</b>	<b>00:00:00:00:00:00:00:00</b>
fc1/6		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/7		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/8		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/10		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/11		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/12		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/14		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/15		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/16		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/17		down	down	1	Manual	44:44:44:44:44:44:11
fc1/18		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/19		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/20		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/21		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/22		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/23		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/24		down	down	1	Manual	00:00:00:00:00:00:00:00

Back Next Cancel

**Step 7** From the Select a Switch drop-down list box, select the switch.



**Note** If the **Another Port on the Same Switch** radio button was chosen, then the Select Switch drop-down list is disabled.

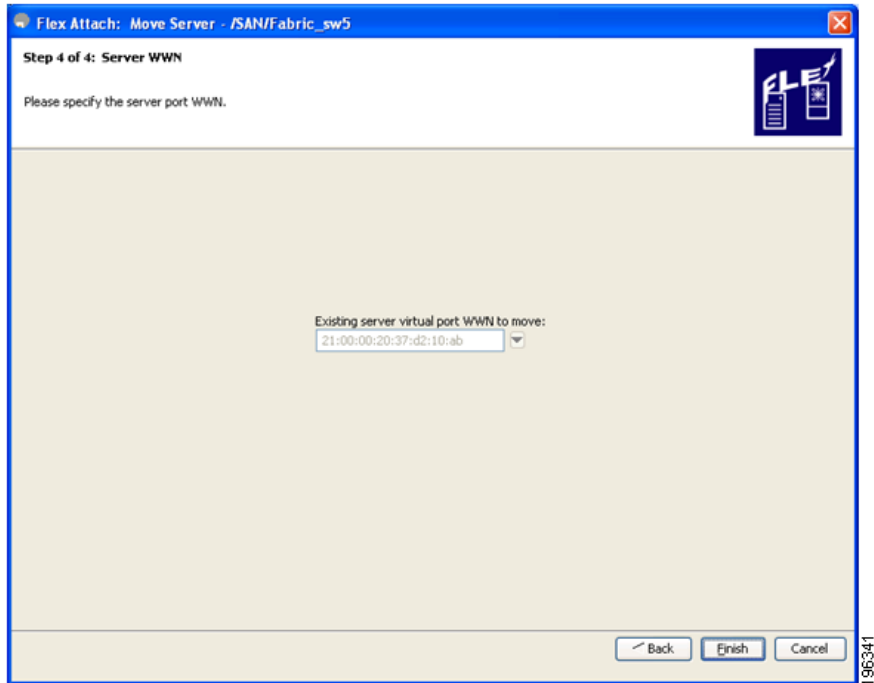
**Step 8** From the list of interfaces, select the port to which you want to move the server to.

**Step 9** Click **Next**.

The Server WWN window is displayed. (Figure 10-17).

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 10-17 Existing Server Virtual Port WWN Entry**



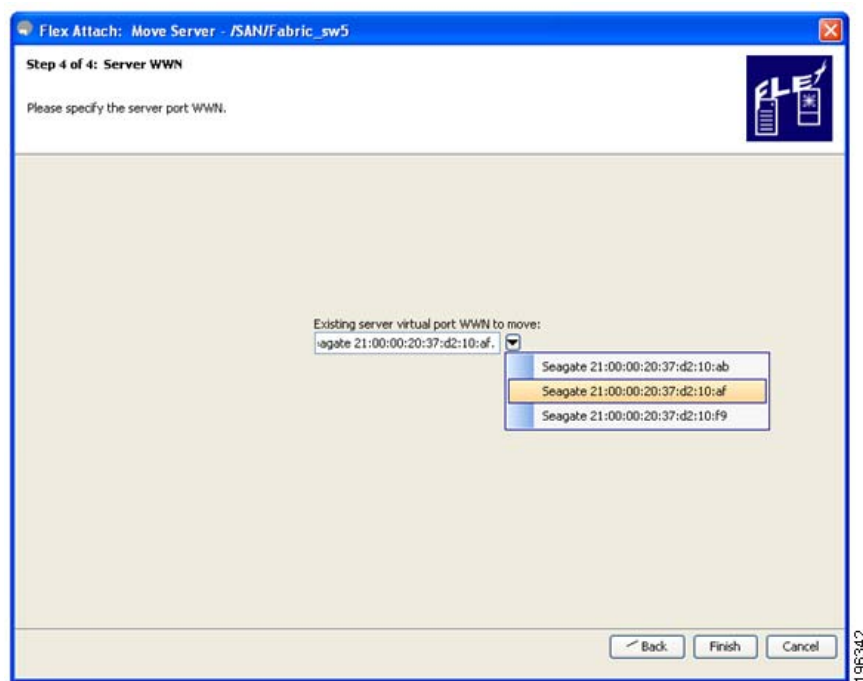
In the Server WWN window, if the FlexAttach global mapping table is empty, the wizard automatically prefills the drop-down table with the interface virtual VPWWN of the source port, and the VPWWN field is not editable.

If the FlexAttach global mapping table is not empty, the VPWWN field is blank and editable. From the drop-down list box that displays all existing entries from the global mapping table, select the VPWWN entry or type the required entry (Figure 10-18).



**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-18** Select Server Virtual Port WWN Entry



**Step 10** Click **Finish**.

## Replacing a Server with Another Server

You can use the Replace Server wizard to accomplish the following tasks:

- Replace a failed server with a new server onto the same port without changing the SAN. The new server gets the same virtual pWWN as the failed server because the virtual pWWN is assigned to the port.
- Replace a server with a spare server on the same NPV device or a different NPV device, which can be brought online without changes to the SAN. This is achieved by moving the virtual port WWN from the current server port to the spare port.

### Replacing a Server on the Same Port

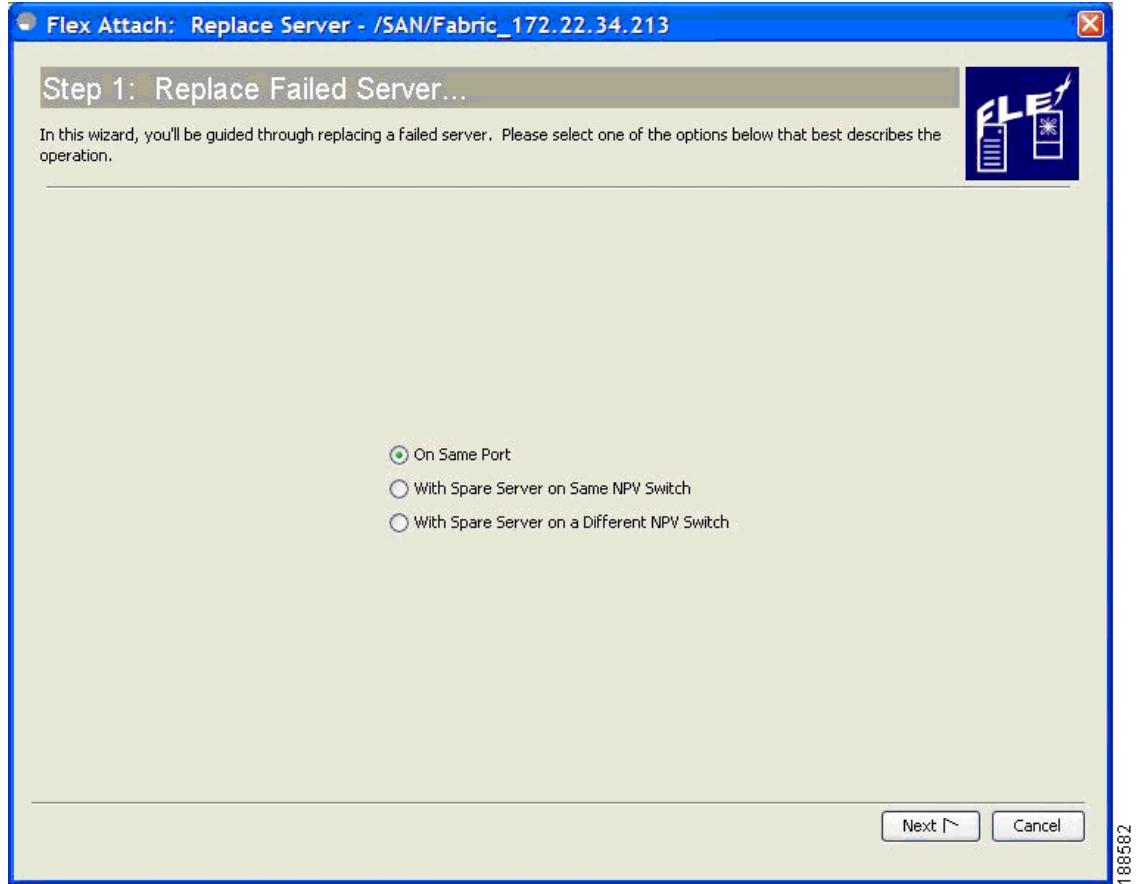
To replace a failed server with a new server on the same port, follow these steps:

**Step 1** In the Fabric Manager window, select **Tools > FlexAttach > Replace Server**.

The Replace Failed Server window is displayed. (Figure 10-19)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

**Figure 10-19** Replace Server Wizard



**Step 2** In the Replace Server Wizard, click the **On Same Port** radio button.

**Step 3** Click **Next**.

The Failed Port window is displayed. (Figure 10-20)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-20 Failed Port Selection**

**Flex Attach: Replace Server - /SAN/Fabric\_172.22.34.213**

**Step 2: Choose Failed Port**

Please select a port you like to replace. To select a port, click on its corresponding row.

Select a switch: 172.22.34.215

Interface	Description	Status Admin	Status Oper	VSAN	Auto	Interface vPWWN
fc1/1		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/2		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/3		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/4		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/5		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/6		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/7		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/8		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/10		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/11		down	down	1	Manual	00:00:00:00:00:00:00:00
<b>fc1/12</b>		<b>down</b>	<b>down</b>	<b>1</b>	<b>Manual</b>	<b>00:00:00:00:00:00:00:00</b>
fc1/14		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/15		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/16		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/17		down	down	1	Manual	44:44:44:44:44:44:11
fc1/18		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/19		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/20		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/21		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/22		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/23		down	down	1	Manual	00:00:00:00:00:00:00:00
fc1/24		down	down	1	Manual	00:00:00:00:00:00:00:00

Back Next Cancel

**Step 4** In the Failed Port selection window, from the Select a Switch drop-down list, select the switch.

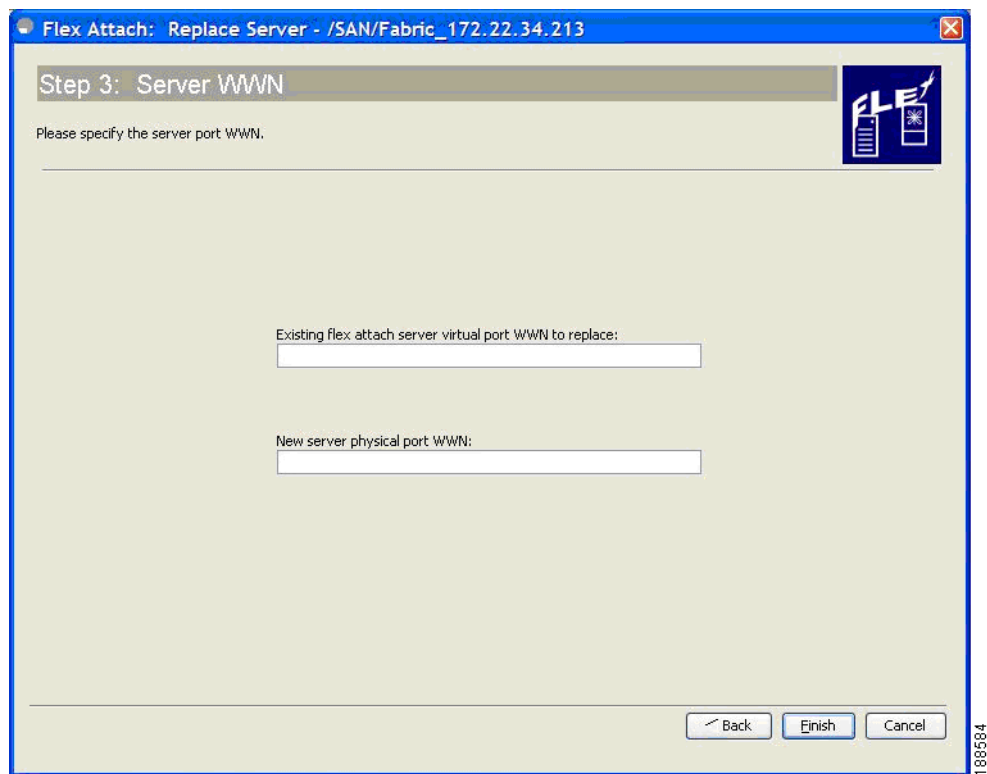
**Step 5** From the list of interfaces displayed, select the port on which the server needs to be replaced.

**Step 6** Click **Next**.

The Server WWN window is displayed. (Figure 10-21)

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**

**Figure 10-21 Server WWN Entries**



- Step 7** In the Server WWN window, enter the existing FlexAttach server virtual port WWN that needs to be replaced, and the new server physical port WWN.
- Step 8** Click **Finish** to complete the FlexAttach configuration for the new server.

## Replacing the Server to a Different Port on the Same Switch

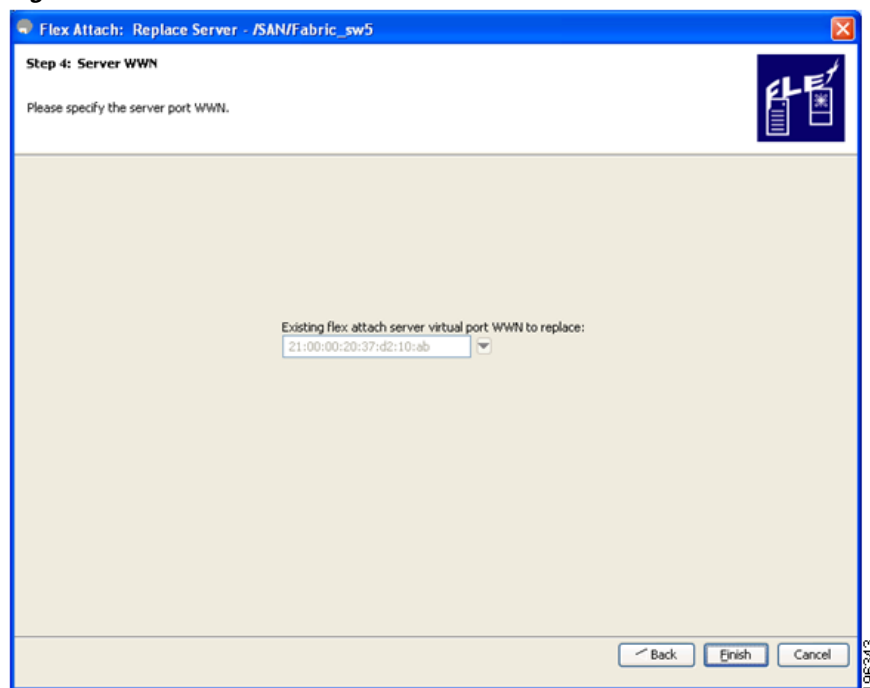
To replace a server with a spare server on a different port in the same switch, follow these steps:

- Step 1** In the Fabric Manger window, select **Tools > FlexAttach > Replace Server**.  
The Replace Failed Server wizard is displayed. (Figure 10-19)
- Step 2** In the Replace Failed Server wizard, click the **With Spare Server on Same NPV Switch** radio button.
- Step 3** Click **Next**.  
The Choose Failed Port window is displayed. (Figure 10-20)
- Step 4** In the Choose Failed Port selection window, from the Select a Switch drop-down list, select the switch.
- Step 5** From the list of interfaces displayed, select the port from which the server needs to be detached.
- Step 6** Click **Next**.  
The New Port window is displayed. (Figure 10-16)
- Step 7** In the New Port selection window, select the port on which the spare server is connected.
- Step 8** Click **Next**.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

The Server WWN window is displayed. (Figure 10-22)

**Figure 10-22 Server WWN Entries**



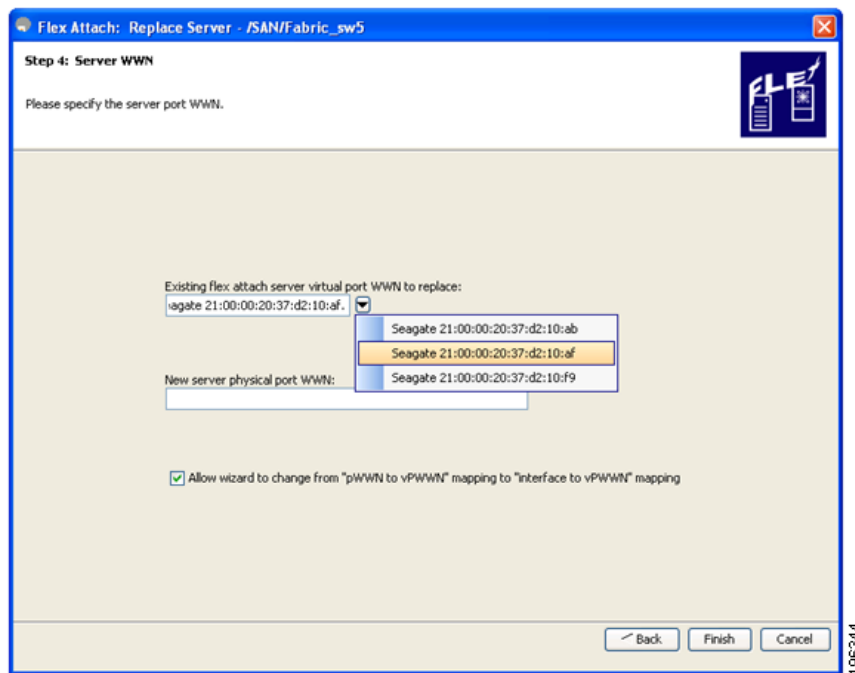
In the Server WWN window, if the FlexAttach global mapping table is empty, the wizard automatically prefills the drop-down table with the interface virtual VPWWN of the source port to be replaced, and the VPWWN field is not editable. In this case, the **Allow wizard to change from “pWWN to vPWWN” mapping to “interface to vPWWN” mapping** is treated as true.

If the FlexAttach global mapping table is not empty, the VPWWN field is blank and editable. From the drop-down list box that displays all existing entries from the global mapping table, select the VPWWN entry or type the required entry, and the new server physical port WWN (Figure 10-23).

**Figure 10-23 Select Server WWN Entries**

Check the **Allow wizard to change from “pWWN to vPWWN” mapping to “interface to vPWWN” mapping** check box to remove the pWWN to vPWWN entry from the CFS Region mapping table, and configure the mapping only at the interface.

**Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)**



**Step 9** Click **Finish** to complete the FlexAttach configuration for the spare server.

## Replacing with a Server on a Different Switch

To replace a server with a spare server on a different switch, follow these steps:

- Step 1** In the Fabric Manger window, select **Tools > FlexAttach > Replace Server**.  
The Replace Server wizard is displayed. (Figure 10-19)
- Step 2** In the Replace Server wizard, click the **With Spare Server on a Different NPV switch** radio button.
- Step 3** Click **Next**.  
The Failed Server Port window is displayed. (Figure 10-20)
- Step 4** In the Failed Server Port selection window, from the Select a Switch drop-down list, select the switch.
- Step 5** From the list of interfaces displayed, select the port from which the server needs to be detached.
- Step 6** Click **Next**.  
The New Port window is displayed. (Figure 10-16)
- Step 7** In the New Port selection window, select the switch and the port on which the spare server is connected.
- Step 8** Click **Next**.  
The Server WWN window is displayed. (Figure 10-22)  
In the Server WWN window, if the FlexAttach global mapping table is empty, the wizard automatically prefills the table with the interface virtual VPWWN of the source port to be replaced, and the VPWWN field is not editable. In this case, the **Allow wizard to change from “pWWN to vPWWN” mapping to “interface to vPWWN” mapping** is treated as true.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

If the FlexAttach global mapping table is not empty, the VPWWN field is blank and editable. From the drop-down list box which displays all existing entries from the global mapping table, select the VPWWN entry or type the required entry, and the new server physical port WWN (Figure 10-23).

Check the **Allow wizard to change from “pWWN to vPWWN” mapping to “interface to vPWWN” mapping** check box to remove the pWWN to vPWWN entry from the CFS Region mapping table, and configure the mapping only at the interface.

**Step 9** Click **Finish** to complete the FlexAttach configuration for the spare server.

## Difference Between San Device Virtualization and FlexAttach Port Virtualization

Table 10-2 describes the difference between SAN device virtualization (SDV) and FlexAttach port virtualization.

**Table 10-2 Difference Between SDV and FlexAttach Virtualization**

<b>SAN Device Virtualization (SDV)</b>	<b>FlexAttach Virtualization</b>
Facilitates target and disk management, and only facilitates disk and data migration.	Facilitates server management and has no restriction on the end devices used.
WWN NAT and Fibre Channel ID (FC-ID) are allocated on the virtual device, both primary and secondary.	WWN and Network Address Transport (NAT) is allocated to host bus adapter (HBA).
FC-ID rewrite on the switch indicates a rewrite-capable switch on the path.	No rewrite requirements.
Configuration is distributed. This allows programming rewrites and connectivity anywhere.	Configuration distribution is not required for any of the interface-based configurations.
Configuration is secured to device alias.	Does not require device alias for virtual pWWN.
Does not allow automapping to the secondary device.	Allows automapping to the new HBA. Mapping process is manual for NPIV.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***





## INDEX

---

### Numerics

#### 12-port 4-Gbps switching modules

BB\_credit buffers [6-12](#)

configuration guidelines [5-17](#)

default settings [5-30](#)

See also switching modules

#### 16-port switching modules

configuring BB\_credits [6-1](#)

LEDs [2-16](#)

See also switching modules

#### 24-port 4-Gbps switching modules

bandwidth fairness [5-24](#)

configuration guidelines [5-16](#)

default settings [5-30](#)

example configurations [6-11](#)

oversubscription [5-20](#)

shared resources [5-10](#)

See also switching modules

#### 24-port 8-Gbps switching modules

default settings [5-30](#)

example configurations [6-7](#)

#### 32-port switching modules

configuring BB\_credits [6-1](#)

See also switching modules

#### 4/44-port 8-Gbps switching modules

default settings [5-30](#)

example configurations [6-8](#)

#### 48-port 4-Gbps switching modules

bandwidth fairness [5-24](#)

configuration guidelines [5-16](#)

default settings [5-30](#)

example configurations [6-9](#)

oversubscription [5-20](#)

shared resources [5-10](#)

See also switching modules

#### 48-port 8-Gbps switching modules

default settings [5-30](#)

example configurations [6-6](#)

See also switching modules

#### 4-port 10-Gbps switching modules

BB\_credit buffers [6-13](#)

configuration guidelines [5-18](#)

default settings [5-30](#)

See also switching modules

---

### A

#### administrative speeds

configuring [2-12](#)

#### administrative states

description [2-8](#)

setting [2-11](#)

#### ALPA caches

description [2-22](#)

#### auto port mode

description [2-7](#)

interface configuration [2-3](#)

#### autosensing speed

Generation 2 switching modules [2-13](#)

---

### B

#### bandwidth fairness

disabling [5-26](#)

enabling [5-24](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

Generation 2 switching modules [5-24](#)

#### BB\_credit buffers

12-port 4-Gbps switching module allocations [6-12](#)

12-port 4-Gbps switching module  
considerations [6-12](#)

24-port 4-Gbps switching module allocations [6-10](#)

24-port 4-Gbps switching module  
considerations [6-11, 6-12](#)

24-port 8-Gbps switching module considerations [6-7](#)

4/44-port 8-Gbps switching module  
considerations [6-8](#)

48-port 4-Gbps switching module considerations [6-9](#)

48-port 8-Gbps switching module considerations [6-6](#)

4-port 10-Gbps switching module allocations [6-13](#)

4-port 10-Gbps switching module  
considerations [6-13, 6-14, 6-15](#)

allocation defaults (table) [6-6, 6-7, 6-8, 6-9](#)

#### BB\_credits

configuring [6-2](#)

description [6-1](#)

reason codes [2-9](#)

#### BB\_SC

enabling [6-19](#)

#### beacon modes

configuring [2-17](#)

identifying LEDs [2-16](#)

#### bit errors

reasons [2-17](#)

#### bit error thresholds

configuring [2-17](#)

description [2-17](#)

#### B port mode

description [2-7](#)

interface modes [2-7](#)

bridge port mode. See B port mode

#### buffer pools

Generation 2 switching modules [6-3](#)

buffer-to-buffer credits. See BB\_credits

buffer-to-buffer start change. See BB\_SC

## C

### Cisco MDS 9216i switches

configuring extended BB\_credits [6-17](#)

configuring NPV [9-8](#)

## D

### dedicated rate mode

description [5-6](#)

migrating from shared rate mode [5-15, 5-16](#)

migrating to shared rate mode [5-16, 5-17](#)

### destination IDs

exchange based [8-5](#)

flow based [8-4](#)

### domain IDs

assignment failures [2-10](#)

### domain manager

isolation [2-10](#)

### dynamic bandwidth management

description [5-9](#)

## E

### EISLs

PortChannel links [8-2](#)

enhanced ISLs. See EISLs

### E port mode

classes of service [2-4](#)

description [2-4](#)

### E ports

32-port guidelines [2-3](#)

32-port switching module configuration  
guidelines [8-8](#)

configuring [2-12](#)

isolation [2-10](#)

### Ethernet interface

configuring [3-1](#)

default settings [3-3](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- interface information [3-1](#)
  - Device Manager [3-2](#)
  - Fabric Manager [3-1](#)
- overview [3-1](#)
- exchange link parameter. See ELP
- expansion port mode. See E port mode
- extended BB\_credits
  - configuring [6-18](#)
  - Generation 2 switching modules [6-16](#)
  - licensing [6-16](#)

## F

- fabric loop port mode. See FL port mode
- fabric port mode. See F port mode
- fcdomains
  - overlap isolation [2-10](#)
- FCoE Configuration Wizard [4-9](#)
- Fibre Channel interface
  - default settings [2-29](#)
- Fibre Channel interfaces
  - administrative states [2-8](#)
  - BB\_credits [6-1](#)
  - characteristics [2-2 to 2-11](#)
  - configuring [2-10](#)
  - configuring beacon modes [2-17](#)
  - configuring bit error thresholds [2-17](#)
  - configuring descriptions [2-13](#)
  - configuring frame encapsulation [2-16](#)
  - configuring port modes [2-12](#)
  - configuring receive data field sizes [6-19](#)
  - configuring speeds [2-12](#)
  - deleting from PortChannels [8-20](#)
  - disabling [2-11](#)
  - enabling [2-11](#)
  - graceful shutdown [2-11](#)
  - modes [2-3 to 2-7](#)
  - operational states [2-8](#)
  - performance buffers [6-2](#)

- reason codes [2-8](#)
- states [2-8](#)
- taking out of service on Generation 2 switching modules [5-26](#)
- troubleshooting operational states [2-9](#)
- See also interfaces [2-8](#)
- FL port mode
  - classes of service [2-5](#)
  - description [2-5](#)
- FL ports
  - configuring [2-12](#)
  - description [2-5](#)
  - nonparticipating code [2-10](#)
  - See also Fx ports
- F port mode
  - classes of service [2-5](#)
  - description [2-5](#)
- F ports
  - configuring [2-12](#)
  - description [2-5](#)
  - See also Fx ports
- frame encapsulation
  - configuring [2-16](#)
- Fx ports
  - 32-port default [2-3](#)
  - configuring [2-12](#)
  - description [2-7](#)
  - interface modes [2-7](#)
  - See also F ports; FL ports [2-7](#)

## G

- Generation 1 switching modules
  - extended BB\_credits [6-16](#)
  - port index allocations [5-11](#)
- Generation 2 switching modules
  - buffer groups [6-3 to 6-14](#)
  - configuring [5-14 to 6-19](#)
  - configuring port speeds [5-18](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

- configuring rate modes [5-19](#)
- default settings [5-30](#)
- description [5-1 to 5-3](#)
- dynamic bandwidth management [5-9](#)
- extended BB\_credits [6-16, 6-17](#)
- out-of-service interfaces [5-10](#)
- port groups [5-3](#)
- port index allocations [5-11](#)
- port rate modes [5-4](#)
- recovering from powered-down state [5-12](#)
- releasing shared resources [5-27](#)
- taking interfaces out of service [5-26](#)

Generation 3 switching modules

- default settings [5-30](#)

## I

interfaces

- adding to PortChannels [8-17, 8-18](#)
- configuring data field size [6-19](#)
- configuring descriptions [2-13](#)
- default settings [2-29](#)
- deleting from PortChannels [8-20](#)
- forced addition to PortChannels [8-19](#)
- isolated states [8-18](#)
- SFP types [2-19](#)
- suspended states [8-18](#)

interface statistics

- gathering [2-19](#)

IPv4 default gateways

- configuring mgmt0 interfaces [2-27](#)

ISLs

- PortChannel links [8-2](#)

## L

LEDs

- beacon mode states [2-16](#)

- speed [2-17](#)

licenses

- extended BB\_credits [6-16](#)

load balancing

- description [8-4](#)
- PortChannels [8-2](#)

## M

management interfaces

- configuring [2-27](#)
- default settings [2-29](#)
- features [2-27](#)

mgmt0 interfaces

- configuring [2-27](#)
- default settings [2-29](#)
- features [2-27](#)

MPS-14/2 modules

- configuring extended BB\_credits [6-17](#)

## N

NL ports

- interface modes [2-7](#)

nonparticipating codes

- description [2-10](#)

NPIV

- description [9-1](#)
- enabling [9-2](#)

NP links [9-4](#)

N port identifier virtualization. See NPIV

NL ports

- See also Nx ports

NP-ports [9-4](#)

NPV, configuring [9-8](#)

NPV mode [9-4](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## O

### operational states

- configuring on Fibre Channel interfaces [2-12](#)
- description [2-8](#)

### out-of-service interfaces

- description [5-10](#)

### oversubscription

- disabling restrictions [5-22](#)
- enabling restrictions [5-23](#)
- Generation 2 switching modules [5-20](#)
- ratios [5-20](#)

## P

### performance buffers

- configuring [6-2](#)
- description [6-2](#)

### PortChannel modes

- description [8-6](#)

### PortChannel Protocol

- autocreation [8-22](#)
- configuring autocreation [8-23](#)
- converting autocreated groups to manually configured [8-23](#)
- creating channel group [8-21](#)
- description [8-20](#)
- enabling autocreation [8-23](#)

### PortChannels

- adding interfaces [8-17, 8-18](#)
- administratively down [2-10](#)
- comparison with trunking [8-3](#)
- compatibility checks [8-18](#)
- configuration guidelines [8-10](#)
- creating [8-16](#)
- default settings [8-25](#)
- deleting [8-16](#)
- deleting interfaces [8-20](#)
- description [8-1](#)

examples [8-2](#)

forcing interface additions [8-19](#)

Generation 2 switching module interfaces [5-12](#)

interface states [8-18](#)

load balancing [8-4](#)

misconfiguration error detection [8-11](#)

verifying configurations [8-24](#)

### port groups

- assigning extended BB\_credits [6-17](#)
- description [5-3](#)
- Generation 2 Fibre Channel switching modules [5-3](#)
- Generation 3 Fibre Channel switching modules [5-7](#)

### port indexes

- description [5-11](#)

### port modes

- auto [2-7](#)
- description [2-3 to 2-7](#)

### port rate modes

- configuring [5-19](#)
- dedicated [5-6](#)
- description [5-4](#)
- oversubscribed [5-7](#)
- shared [5-7](#)
- See also rate modes

### port speeds

- configuring [2-12](#)
- configuring on Generation 2 switching module interfaces [5-18](#)

## R

### rate modes

- configuring on Generation 2 switching module interfaces [5-19](#)
- See also port rate modes

### reason codes

- description [2-8](#)

receive buffer groups. See buffer groups

receive data field sizes

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

configuring [6-19](#)

recovery

from powered-down state [5-12](#)

## S

SD port mode

description [2-6](#)

interface modes [2-6](#)

SD ports

configuring [2-12](#)

SFPs

displaying transmitter types [2-19](#)

transmitter types [2-18](#)

shared rate mode

description [5-7](#)

migrating from dedicated rate mode [5-16, 5-17](#)

migrating to dedicated rate mode [5-15, 5-16](#)

oversubscription [5-20](#)

source IDs

exchange based [8-5](#)

flow based [8-4](#)

SPAN destination port mode. See SD port mode

SPAN tunnel port mode. See ST port mode

ST port mode

description [2-7](#)

interface modes [2-7](#)

limitations [2-7](#)

ST ports

interface modes [2-7](#)

subnet masks

configuring mgmt0 interfaces [2-27](#)

switch ports

configuring attribute default values [2-18](#)

classes of service [2-6](#)

description [2-6](#)

TE ports

trunking restrictions [7-3](#)

TF port mode

classes of service [2-6](#)

description [2-6](#)

TL port mode

classes of service [2-5](#)

description [2-5](#)

TL ports

ALPA caches [2-22](#)

configuring [2-12, 2-22](#)

description [2-20](#)

translative loop port mode. See TL port mode

trunk-allowed VSAN lists

description [7-9 to 7-11](#)

trunking

comparison with PortChannels [8-3](#)

configuration guidelines [7-4](#)

configuring modes [7-7](#)

default settings [7-11](#)

description [7-1](#)

link state [7-7](#)

merging traffic [7-4](#)

restrictions [7-3](#)

trunking E port mode. See TE port mode

trunking F port mode. See TF port mode

trunking protocol

default settings [7-11, 7-12](#)

default state [7-6](#)

description [7-6](#)

detecting port isolation [7-4](#)

disabling [7-7](#)

enabling [7-7](#)

trunk mode

configuring [7-7, 7-8](#)

default settings [7-11](#)

status [7-7](#)

## T

TE port mode

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

## V

### virtual FC interface

assigning to VSANs [4-8](#)

configuring [4-2](#)

Device Manager [4-4](#)

Fabric Manager [4-2](#)

creating

Device Manager [4-14](#)

Fabric Manager [4-13](#)

default settings [4-16](#)

deleting [4-15](#)

limitations [4-1](#)

overview [4-1](#)

### virtual interface

configuring

FCoE Configuration Wizard [4-9](#)

### VLANs

mapping to VSANs [4-5](#)

using Device Manager [4-7](#)

using Fabric Manager [4-5](#)

### VSAN IDs

allowed list [7-11](#)

multiplexing traffic [2-6](#)

### VSAN interfaces

configuring [2-28](#)

creating [2-28](#)

description [2-28](#)

### VSANs

allowed-active [7-4](#)

configuring allowed-active lists [7-11](#)

configuring trunk-allowed lists [7-9 to 7-11](#)

mismatches [2-10](#)

TE port mode [2-6](#)

TF port mode [2-6](#)

trunk-allowed [7-4](#)

VSAN trunking. See trunking

## W

### WWNs

suspended connections [2-10](#)

## Z

### zones

merge failures [2-10](#)

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***