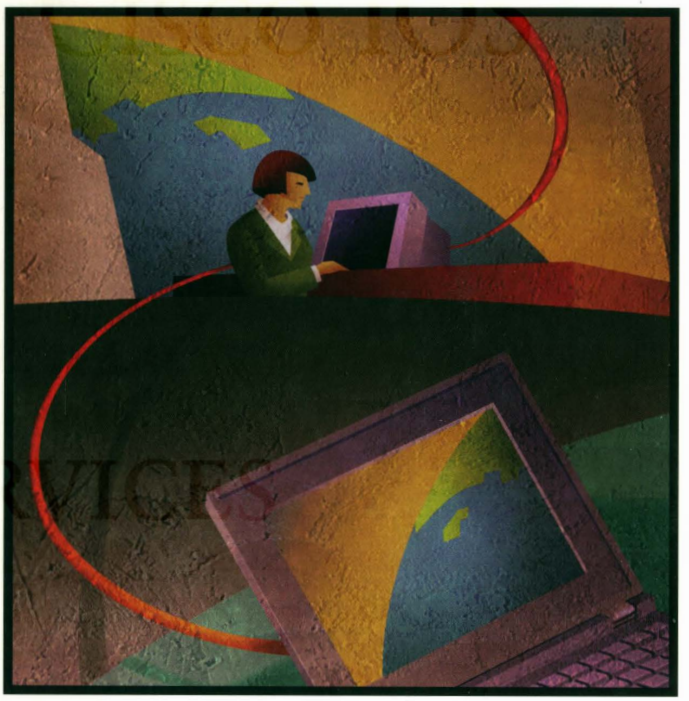
CISCO DOCUMENTATION

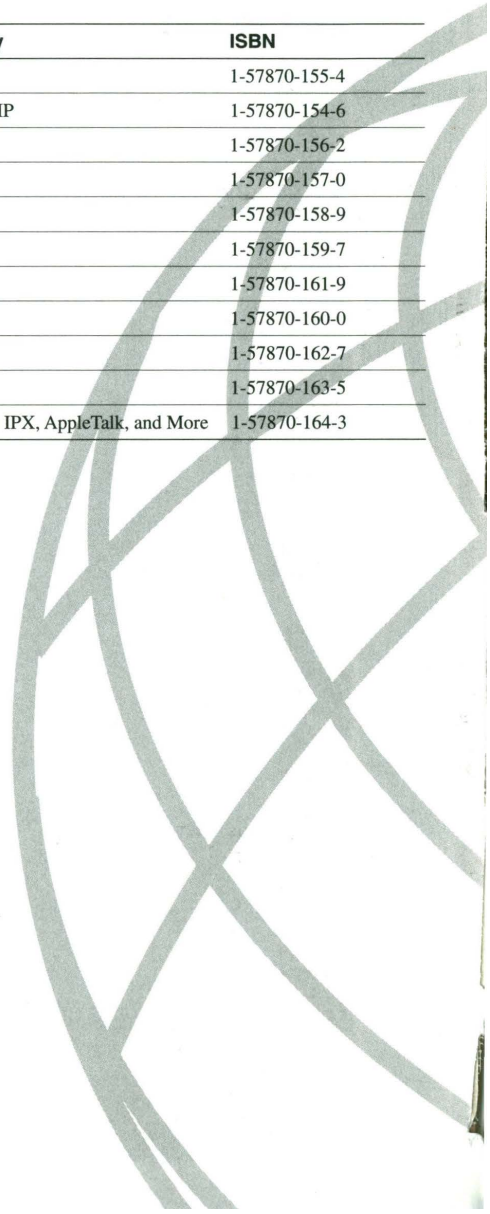


Cisco IOS™ 12.0 Switching Services

Documentation from the Cisco IOS Reference Library

Cisco Systems
Cisco Press
www.ciscopress.com

Books Available in the Cisco IOS Reference Library	ISBN
Cisco IOS 12.0 Configuration Fundamentals	1-57870-155-4
Cisco IOS 12.0 Solutions for Network Protocols, Volume I: IP	1-57870-154-6
Cisco IOS 12.0 Interface Configuration	1-57870-156-2
Cisco IOS 12.0 Switching Services	1-57870-157-0
Cisco IOS 12.0 Wide Area Networking Solutions	1-57870-158-9
Cisco IOS 12.0 Multiservice Applications	1-57870-159-7
Cisco IOS 12.0 Quality of Service	1-57870-161-9
Cisco IOS 12.0 Network Security	1-57870-160-0
Cisco IOS 12.0 Bridging and IBM Network Solutions	1-57870-162-7
Cisco IOS 12.0 Dial Solutions	1-57870-163-5
Cisco IOS 12.0 Solutions for Network Protocols, Volume II: IPX, AppleTalk, and More	1-57870-164-3



Cisco IOS 12.0 Switching Services



Cisco Systems
Cisco Press

Cisco Press
201 W 103rd Street
Indianapolis, IN 46290

Cisco IOS 12.0 Switching services

Cisco Systems, Inc.

Copyright © 1999 Cisco Systems, Inc.

Cisco Press logo is a trademark of Cisco Systems, Inc.

Published by:
Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Library of Congress Cataloging-in-Publication Number 99-60809

ISBN: 1-57870-157-0

Warning and Disclaimer

This book is designed to provide information about *Cisco IOS 12.0 Switching Services*. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at ciscopress@mcp.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Associate Publisher	Jim LeValley
Executive Editor	Alicia Buckley
Cisco Systems Program Manager	H. Kim Lew
Managing Editor	Patrick Kanouse
Acquisitions Editor	Tracy Hughes
Copy Editor	Kitty Wilson Jarrett
Team Coordinator	Amy Lewis
Book Designer	Scott Cook
Cover Designer	Karen Ruggles
Production Team	Lisa England Christy Lemasters Elise Walter
Indexer	Craig Small

Acknowledgments

The Cisco IOS Reference Library is the result of collaborative efforts of many Cisco technical writers and editors over the years. This bookset represents the continuing development and integration of user documentation for the ever-increasing set of Cisco IOS networking features and functionality.

The current team of Cisco IOS technical writers and editors includes Katherine Anderson, Hugh Bussell, Melanie Cheng, Christy Choate, Sue Cross, Meredith Fisher, Tina Fox, Sheryl Kelly, Marsha Kinnear, Doug MacBeth, Lavanya Mandavilli, Mary Mangone, Andy Mann, Bob Marburg, Greg McMillan, Madhu Mitra, Vicki Payne, Jeremy Pollock, Patricia Rohrs, Teresa Oliver Schick, Wink Schuetz, Grace Tai, Brian Taylor, Jamianne Von-Prudelle, and Amanda Worthington.

The writing team wants to acknowledge the many engineering, customer support, and marketing subject-matter experts for their participation in reviewing draft documents and, in many cases, providing source material from which this book-set was developed.

Contents at a Glance

Introduction	Cisco IOS Switching Services Overview	xiii
Part 1	**Cisco IOS Switching Paths**	**1**
Chapter 1	Switching Paths Overview	3
Chapter 2	Configuring Switching Paths	11
Chapter 3	Cisco IOS Switching Commands	19
Part 2	**Cisco Express Forwarding**	**39**
Chapter 4	Cisco Express Forwarding Overview	41
Chapter 5	Configuring Cisco Express Forwarding	49
Chapter 6	Cisco Express Forwarding Commands	55
Part 3	**NetFlow Switching**	75
Chapter 7	NetFlow Switching Overview	77
Chapter 8	Configuring NetFlow Switching	81
Part 4	**Tag Switching**	**85**
Chapter 9	Tag Switching Overview	87
Chapter 10	Configuring Tag Switching	91
Chapter 11	Tag Switching Commands	107
Part 5	**Multilayer Switching**	**157**
Chapter 12	Multilayer Switching Overview	159
Chapter 13	Configuring Multilayer Switching	169
Chapter 14	Multilayer Switching Commands	177
Part 6	**Multicast Distributed Switching**	**185**
Chapter 15	Configuring Multicast Distributed Switching	187
Chapter 16	Multicast Distributed Switching Commands	191

Part 7 **Virtual LANs 205**

Chapter 17 Routing between Virtual LANs Overview 207

Chapter 18 Configuring Routing between VLANs with ISL Encapsulation 215

Chapter 19 Configuring Routing between VLANs with IEEE 802.10 Encapsulation 241

Chapter 20 LAN Emulation Overview 245

Chapter 21 Configuring LAN Emulation 253

Chapter 22 LAN Emulation Commands 295

Chapter 23 MPOA Overview 347

Chapter 24 Configuring the MPOA Client 353

Chapter 25 Configuring the MPOA Server 359

Chapter 26 MPOA Commands 365

Index **389**

Table of Contents

Cisco IOS Switching Services Overview xiii

Document Organization xiii

About the Cisco IOS 12.0 Reference Library xiv

Using Cisco IOS Software xviii

Part I **Cisco IOS Switching Paths 1**

Chapter 1 Switching Paths Overview 3

Overview of Basic Router Platform Architecture and Processes 3

Features That Affect Performance 8

Chapter 2 Configuring Switching Paths 11

Fast Switching Configuration Task List 11

Disabling Fast Switching for Troubleshooting 13

Controlling the Route Cache 15

Chapter 3 Cisco IOS Switching Commands 19

Part II **Cisco Express Forwarding 39**

Chapter 4 Cisco Express Forwarding Overview 41

CEF Components 42

Supported Media 44

CEF Operation Modes 44

Additional Capabilities 47

Chapter 5 Configuring Cisco Express Forwarding 49
Cisco Express Forwarding Configuration Task List 49
Enabling and Disabling CEF or dCEF 49
Configuring Load Balancing for CEF 50
Configuring Network Accounting for CEF 52
Configuring Distributed Tunnel Switching for CEF 53

Chapter 6 Cisco Express Forwarding Commands 55

Part III NetFlow Switching 75

Chapter 7 NetFlow Switching Overview 77
NetFlow Switching 77

Chapter 8 Configuring NetFlow Switching 81
Configuring NetFlow Switching 81
NetFlow Switching Configuration Example 84

Part IV Tag Switching 85

Chapter 9 Tag Switching Overview 87
Tag Functions 87
Distribution of Tag Bindings 88
Tag Switching and Routing 88
Tag Switching and Traffic Engineering 88

Chapter 10 Configuring Tag Switching 91
Traffic Engineering 95
Configuration Examples 98

Chapter 11 Tag Switching Commands 107

Part V Multilayer Switching 157

Chapter 12 Multilayer Switching Overview 159
Terminology 160
Key MLS Features 160
Introduction to Multilayer Switching 161
Multilayer Switching Implementation 162
Standard and Extended Access Lists 164
Restrictions on Using IP Router Commands with MLS Enabled 165
General Guidelines 165
Software and Hardware Requirements 166
Guidelines for External Routers 166
Features That Affect MLS 166

Chapter 13 Configuring Multilayer Switching 169
Configuring and Monitoring MLS 169
Configuring NetFlow Data Export 172
Multilayer Switching Configuration Examples 173

Chapter 14 Multilayer Switching Commands 177

Part VI Multicast Distributed Switching 185

Chapter 15 Configuring Multicast Distributed Switching 187
Configure MDS 187

Chapter 16 Multicast Distributed Switching Commands 191

Part VII Virtual LANs 205

Chapter 17 Routing Between Virtual LANs Overview 207
What Is a Virtual LAN? 207
VLAN Colors 209
Why Implement VLANs? 210
VLAN Interoperability 211
Designing Switched VLANs 212

Chapter 18 Configuring Routing Between VLANs with ISL Encapsulation 215
Overview of ISL Protocol 215
ISL Encapsulation Configuration Task List 216
ISL Encapsulation Configuration Examples 229

Chapter 19 Configuring Routing Between VLANs with IEEE 802.10 Encapsulation 241
Configure AppleTalk Routing over IEEE 802.10 241
Routing AppleTalk over IEEE 802.10 Configuration Example 242

Chapter 20 LAN Emulation Overview 245
LANE 245

Chapter 21 Configuring LAN Emulation 253
LANE on ATM 253
Implementation Considerations 255
LANE Configuration Task List 259
LANE Configuration Examples 278

Chapter 22 LAN Emulation Commands 295

Chapter 23 MPOA Overview 347
Platforms 348
How MPOA Works 348
Configuring an MPC/MPS 351

Chapter 24 Configuring the MPOA Client 355
How MPC Works 353
MPC Configuration Task List 353
MPC Configuration Examples 356
Chapter 25 Configuring the MPOA Server 359
How MPS Works 359
MPS Configuration Task List 360
MPS Configuration Examples 362
Chapter 26 MPOA Commands 365

Cisco IOS Switching Services Overview

Cisco IOS 12.0 Switching Services provides guidelines for configuring switching paths and routing between virtual local-area networks (VLANs) with the Cisco IOS software.

This guide is intended for the network administrator who designs and implements router-based internetworks and needs to incorporate switching, NetFlow accounting, or routing between VLANS into the network. It presents a set of general guidelines for configuring switching of various protocols, NetFlow accounting, routing between VLANs, and local-area network (LAN) emulation. The objective of this guide is to provide you with the information you need to configure any of these features.

You should know how to configure a Cisco router and should be familiar with the protocols and media that your routers are configured to support. Knowledge of basic network topology is essential.

Document Organization

This document comprises seven parts, each focusing on a different aspect of switching within Cisco IOS software. Each part begins with a brief technology overview and follows with the corresponding configuration guidelines for that technology or set of features. This document contains these parts:

- Cisco IOS Switching Paths – Provides an overview of basic routing and switching processes. It describes switching paths available in Cisco IOS software. Configuration guidelines are provided for configuring and managing fast switching of various protocols.
- Cisco Express Forwarding – Provides an overview of Cisco Express Forwarding (CEF), the advanced Layer 3 IP switching technology that optimizes performance and scalability in networks with large and dynamic traffic patterns. Guidelines for configuring and managing CEF are provided.
- NetFlow Switching – Provides an overview of the NetFlow switching technology and describes the NetFlow accounting features. Guidelines for configuring and managing NetFlow switching are provided.
- Tag Switching – Provides an overview of Tag Switching, the switching technology that combines the performance of Layer 2 switching with the scalability of Layer 3 routing. Guidelines for configuring and managing Tag Switching are provided.

- Multilayer Switching – Provides an overview of Multilayer Switching. Multilayer Switching provides high-performance Layer 3 switching for the Catalyst 5000 series LAN switches working in conjunction with Cisco routers. Guidelines for configuring and managing Multilayer Switching on Cisco routers are provided.
- Multicast Distributed Switching – Provides an overview of Multicast Distributed Switching (MDS). MDS performs distributed switching of multicast packets in the line cards of Route Switch Processor (RSP)-based platforms. Guidelines for configuring and managing MDS are provided.
- Virtual LANs – Provides an overview of VLANs. Guidelines for configuring routing between VLANs using the Inter-Switch Link (ISL) and IEEE 802.10 protocols for packet encapsulation follow the overview. LAN Emulation for defining VLANs in ATM networks and Multiprotocol Over ATM (MPOA) is described, along with related configuration guidelines.

About the Cisco IOS 12.0 Reference Library

The Cisco IOS 12.0 Reference Library books are Cisco documentation that describe the tasks and commands necessary to configure and maintain your Cisco IOS network.

The Cisco IOS software bookset is intended primarily for users who configure and maintain access servers and routers, but are not necessarily familiar with the tasks, the relationship between tasks, or the commands necessary to perform particular tasks.

Cisco IOS Reference Library Organization

The Cisco IOS 12.0 Reference library consists of eleven books. Each book contains technology-specific configuration chapters with corresponding command reference chapters. Each configuration chapter describes Cisco's implementation of protocols and technologies, related configuration tasks, and contains comprehensive configuration examples. Each command reference chapter complements the organization of its corresponding configuration chapter and provides complete command syntax information.

Books Available in the Cisco IOS 12.0 Reference Library

- *Cisco IOS 12.0 Solutions for Network Protocols, Volume I: IP*, 1-57870-154-6.

  This book is a comprehensive guide detailing available IP and IP routing alternatives. It describes how to implement IP addressing and IP services and how to configure support for a wide range of IP routing protocols, including BGP for ISP networks and basic and advanced IP Multicast functionality.

- *Cisco IOS 12.0 Interface Configuration*, 1-57870-156-2.

  This book is a comprehensive guide detailing how to configure physical and virtual interfaces—the two types of interfaces supported on Cisco routers. It provides readers with the most current router task and command information for their network environments and teaches how to effectively implement these techniques and commands on their networks.

- *Cisco IOS 12.0 Configuration Fundamentals*, 1-57870-155-4.

  This comprehensive guide details Cisco IOS software configuration basics. It offers thorough coverage of router and access server configuration and maintenance techniques. In addition to hands-on implementation and task instruction, this book also presents the complete syntax for router and access server commands, and individual examples for each command.

- *Cisco IOS 12.0 Wide Area Networking Solutions*, 1-57870-158-9.

  This book offers thorough, comprehensive coverage of internetworking technologies, particularly ATM, Frame Relay, SMDS, LAPB, and X.25, teaching the reader how to configure the technologies in a LAN/WAN environment.

- *Cisco IOS 12.0 Multiservice Applications*, 1-57870-159-7.

  This book shows you how to configure your router or access server to support voice, video, and broadband transmission. Cisco's voice and video support are implemented using voice packet technology. In voice packet technology, voice signals are packetized and transported in compliance with ITU-T specification H.323, which is the ITU-T specification for transmitting multimedia (voice, video, and data) across a local-area network (LAN).

- *Cisco IOS 12.0 Network Security*, 1-57870-160-0.

  This book documents security configuration from a remote site and for a central enterprise or service provider network. It describes AAA, Radius, TACACS+, and Kerberos network security features. It also explains how to encrypt data across enterprise networks. The book includes many illustrations that show configurations and functionality, along with a discussion of network security policy choices and some decision-making guidelines.

- *Cisco IOS 12.0 Quality of Service*, 1-57870-161-9.

  Cisco IOS 12.0 Quality of Service Solutions Configuration Guide is a comprehensive guide detailing available Cisco IOS quality of service (QoS) features. This book suggests benefits you can gain from implementing Cisco IOS QoS features and describes how to effectively configure and implement the various QoS features. Some of the features described in this book include Committed Access Rate (CAR), Weighted Fair Queueing (WFQ), and Weighted Random Early Detection (WRED), as well as many other features.

- *Cisco IOS 12.0 Solutions for Network Protocols, Volume II: IPX, AppleTalk, and More*, 1-57870-164-3.

  This book is a comprehensive guide detailing available network protocol alternatives. It describes how to implement various protocols in your network. This book includes documentation of the latest functionality for the IPX and AppleTalk desktop protocols as well as the following network protocols: Apollo Domain, Banyan VINES, DECNet, ISO CLNS, and XNS.

- *Cisco IOS 12.0 Bridging and IBM Network Solutions*, 1-57870-162-7.

  This book describes Cisco's support for networks in IBM and bridging environments. Support includes: transparent and source-route transparent bridging, source-route bridging (SRB), remote source-route bridging (RSRB), data link switching plus (DLS+), serial tunnel and block serial

tunnel, SDLC and LLC2 parameter, IBM network media translation, downstream physical unit and SNA service point, SNA Frame Relay access support, Advanced Peer-to-Peer Networking, and native client interface architecture (NCIA).

- *Cisco IOS 12.0 Dial Solutions*, 1-57870-163-5.

  This book provides readers with real-world solutions and how to implement them on a network. Customers interested in implementing dial solutions across their network environment include remote sites dialing in to a central office, Internet Service Providers (ISPs), ISP customers at home offices, and enterprise WAN system administrators implementing dial-on-demand routing (DDR).

Book Conventions

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	Represents the Control key. For example, when you read *^D* or *Ctrl-D*, you should hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
string	A string is defined as a nonquoted set of characters. For example, when setting an SNMP community string to public, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen`	Shows an example of information displayed on the screen.
`boldface screen`	Shows an example of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
!	Exclamation points at the beginning of a line indicate a comment line. They are also displayed by the Cisco IOS software for certain processes.
[ ]	Default responses to system prompts appear in square brackets.

The following conventions are used to attract the reader's attention:

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

NOTE Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

TIMESAVER Means the *described action saves time*. You can save time by performing the action described in the paragraph.

Within the Cisco IOS12.0 Reference Library, the term *router* is used to refer to both access servers and routers. When a feature is supported on the access server only, the term *access server* is used.

Within examples, routers and access servers are alternately shown. These products are used only for example purposes; that is, an example that shows one product does not indicate that the other product is not supported.

Command Syntax Conventions

Command descriptions use the following conventions:

Convention	Description
boldface	Indicates commands and keywords that are entered literally as shown.
italics	Indicates arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).
[x]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords (represented by **x**, **y**, and **z**) appears in braces separated by vertical bars. You must select one.
[x {y | z}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to select one. If you do, you have some required choices.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

Using Cisco IOS Software

This section provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI).

Getting Help

Entering a question mark (**?**) at the system prompt displays a list of commands available for each command mode. You can also get a list of any command's associated keywords and arguments with the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Obtains a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists a command's associated keywords. (Space between command and question mark.)
command keyword **?**	Lists a keyword's associated arguments. (Space between the keyword and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list of keywords available along with a brief description of the keywords. For example, if you were in global configuration mode, typed the command **arap**, and wanted to see all the keywords for that command, you would type **arap ?**.

Table I-1 shows examples of how you can use the question mark (**?**) to assist you in entering commands. It steps you through entering the following commands:

- `controller t1 1`
- `cas-group 1 timeslots 1-24 type e&m-fgb dtmf`

Table I-1 *How to Find Command Options*

Command	Comment
`Router> enable` `Password: <password>` `Router#`	Enter the **enable** command and password to access privileged EXEC commands. You have entered privileged EXEC mode when the prompt changes to `Router#`.
`Router# config terminal` `Enter configuration commands, one per line.` `End with CNTL/Z.` `Router(config)#`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.
`Router(config)# controller t1 ?` `  <0-3>  Controller unit number` `Router(config)# controller t1 1` `Router(config-controller)#`	Enter controller configuration mode by specifying the T1 controller that you want to configure using the **controller t1** global configuration command. Enter a **?** to display what you must enter next on the command line. In this example, you must enter a controller unit number from 0 to 3. You have entered controller configuration mode when the prompt changes to `Router(config-controller)#`.

Continues

Table I-1 *How to Find Command Options (Continued)*

Command	Comment
`Router(config-controller)# ?` `Controller configuration commands:` `  cablelength  Specify the cable length for a DS1 link` `  cas-group  Configure the specified timeslots for CAS (Channel Associate Signals)` `  channel-group  Specify the timeslots to channel-group mapping for an interface` `  clock  Specify the clock source for a DS1 link` `  default  Set a command to its defaults` `  description  Controller specific description` `  ds0  ds0 commands` `  exit  Exit from controller configuration mode` `  fdl  Specify the FDL standard for a DS1 data link` `  framing  Specify the type of Framing on a DS1 link` `  help  Description of the interactive help system` `  linecode  Specify the line encoding method for a DS1 link` `  loopback  Put the entire T1 line into loopback` `  no  Negate a command or set its defaults` `  pri-group  Configure the specified timeslots for PRI` `  shutdown  Shut down a DS1 link (send Blue Alarm)` `Router(config-controller)#`	Enter a **?** to display a list of all the controller configuration commands available for the T1 controller.
`Router(config-controller)# cas-group ?` `  <0-23>  Channel number` `Router(config-controller)# cas-group`	Enter the command that you want to configure for the controller. In this example, the **cas-group** command is used. Enter a **?** to display what you must enter next on the command line. In this example, you must enter a channel number from 0 to 23. Because a <cr> is not displayed, it indicates that you must enter more keywords to complete the command.

Table I-1 *How to Find Command Options (Continued)*

Command	Comment
`Router(config-controller)# cas-group 1 ?` `  timeslots  List of timeslots in the` `  cas-group` `Router(config-controller)# cas-group 1`	After you enter the channel number, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **timeslots** keyword. Because a <cr> is not displayed, it indicates that you must enter more keywords to complete the command.
`Router(config-controller)# cas-group 1` `timeslots ?` `  <1-24>  List of timeslots which` `  comprise the cas-group` `Router(config-controller)# cas-group 1` `timeslots`	After you enter the **timeslots** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter a list of timeslots from 1 to 24. You can specify timeslot ranges (for example, 1-24), individual timeslots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-3, 8, 17-24). The 16th time slot is not specified in the command line because it is reserved for transmitting the channel signaling. Because a <cr> is not displayed, it indicates that you must enter more keywords to complete the command.
`Router(config-controller)# cas-group 1` `timeslots 1-24 ?` `  service  Specify the type of service` `  type  Specify the type of signaling` `Router(config-controller)# cas-group 1` `timeslots 1-24`	After you enter the timeslot ranges, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **service** or **type** keyword. Because a <cr> is not displayed, it indicates that you must enter more keywords to complete the command.
`Router(config-controller)# cas-group 1` `timeslots 1-24 type ?` `  e&m-fgb  E & M Type II FGB` `  e&m-fgd  E & M Type IIFGD` `  e&m-immediate-start  E & M Immediate` `  Start` `  fxs-ground-start  FXS Ground Start` `  fxs-loop-start  FXS Loop Start` `  sas-ground-start  SAS Ground Start` `  sas-loop-start  SAS Loop Start` `Router(config-controller)# cas-group 1` `timeslots 1-24 type`	In this example, the **type** keyword is entered. After you enter the **type** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter one of the signaling types. Because a <cr> is not displayed, it indicates that you must enter more keywords to complete the command.

Continues

Table I-1 *How to Find Command Options (Continued)*

Command	Comment
`Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb ?` `  dtmf  DTMF tone signaling` `  mf  MF tone signaling` `  service  Specify the type of service` `  <cr>` `Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb`	In this example, the **e&m-fgb** keyword is entered. After you enter the **e&m-fgb** keyword, enter a **?** to display what you must enter next on the command line. In this example, you can enter the **dtmf**, **mf**, or **service** keyword to indicate the type of channel-associated signaling available for the **e&m-fgb** signaling type. Because a <cr> is displayed, it indicates that you can enter more keywords or press <cr> to complete the command.
`Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb dtmf ?` `  dnis  DNIS addr info provisioned` `  service  Specify the type of service` `  <cr>` `Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb dtmf`	In this example, the **dtmf** keyword is entered. After you enter the **dtmf** keyword, enter a **?** to display what you must enter next on the command line. In this example, you can enter the **dnis** or **service** keyword to indicate the options available for **dtmf** tone signaling. Because a <cr> is displayed, it indicates that you can enter more keywords or press <cr> to complete the command.
`Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb dtmf` `Router(config-controller)#`	In this example, enter a <cr> to complete the command.

Understanding Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you at any given time depend on which mode you are currently in. Entering a question mark (**?**) at the system prompt allows you to obtain a list of commands available for each command mode.

When you start a session on the router, you begin in user mode, often called EXEC mode. Only a limited subset of the commands are available in EXEC mode. In order to have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From privileged mode, you can enter any EXEC command or enter global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current status of something, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the router.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots. In order to get to the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your router or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter read-only memory (ROM) monitor mode.

Summary of Main Command Modes

Table I-2 summarizes the main command modes of the Cisco IOS software.

Table I-2 *Summary of Main Command Modes*

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To exit back to user EXEC mode, use the **disable** command. To enter global configuration mode, use the **configure terminal** privileged EXEC command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router (config)#`	To exit to privileged EXEC mode, use the **exit** or **end** command or press **Ctrl-Z**. To enter interface configuration mode, enter an **interface** configuration command.
Interface configuration	From global configuration mode, enter by specifying an interface with an **interface** command.	`Router (config-if)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, use the **exit** command or press **Ctrl-Z**. To enter subinterface configuration mode, specify a subinterface with the **interface** command.
Subinterface configuration	From interface configuration mode, specify a subinterface with an **interface** command.	`Router (config-subif)#`	To exit to global configuration mode, use the **exit** command. To enter privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the Break key during the first 60 seconds while the system is booting.	`>`	To exit to user EXEC mode, type **continue**.

Using the No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a function. Use the command without the keyword **no** to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** command and specify **ip routing** to re-enable it. The Cisco IOS software command references provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values. The Cisco IOS software command references describe what the **default** form of a command does if the command is not the same as the **no** form.

Saving Configuration Changes

Enter the **copy system:running-config nvram:startup-config** command to save your configuration changes to your startup configuration so that they will not be lost if there is a system reload or power outage. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this step saves the configuration to nonvolatile random-access memory (NVRAM). On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

PART

Cisco IOS Switching Paths

Chapter 1 Switching Paths Overview

Chapter 2 Configuring Switching Paths

Chapter 3 Cisco IOS Switching Commands

CHAPTER 1

Switching Paths Overview

This chapter describes switching paths that can be configured on Cisco IOS devices. It provides an overview of switching methods. For specific configuration information, refer to Chapter 2, "Configuring Switching Paths."

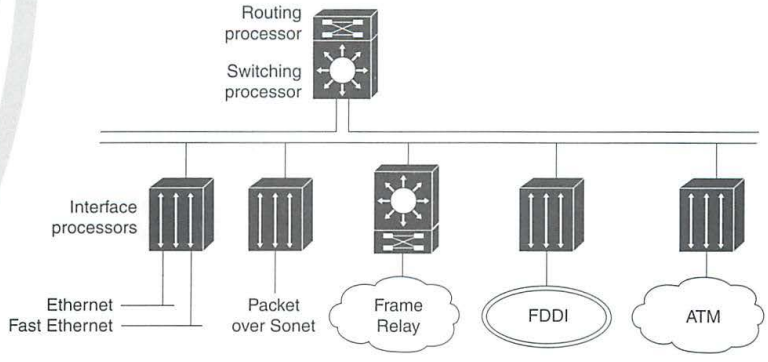
Overview of Basic Router Platform Architecture and Processes

To understand how switching works, it helps to first understand the basic router architecture and where various processes occur in the router.

Fast switching is enabled by default on all interfaces that support fast switching. If you have a situation where you need to disable fast switching and fall back to the process-switching path, understanding how various processes affect the router and where they occur will help you determine your alternatives. This understanding is especially helpful when you are troubleshooting traffic problems or need to process packets that require special handling. Some diagnostic or control resources are not compatible with fast switching or come at the expense of processing and switching efficiency. Understanding those resources can help you minimize their effect on network performance.

Figure 1-1 illustrates a possible internal configuration of a Cisco 7500 series router. In this configuration, the Cisco 7500 series router has an integrated Route/Switch Processor (RSP) and uses *route caching* to forward packets. The Cisco 7500 series router also uses Versatile Interface Processors (VIPs), a RISC-based interface processor that receives and caches routing information from the RSP. The VIP card uses the route cache to make switching decisions locally, which relieves the RSP of involvement and speeds overall throughput. This type of switching is called *distributed switching*. Multiple VIP cards can be installed in one router.

Figure 1-1 *Basic Router Architecture*



Cisco Routing and Switching Processes

The routing, or forwarding, function comprises two interrelated processes to move information in the network:

- Making a routing decision by routing
- Moving packets to the next-hop destination by switching

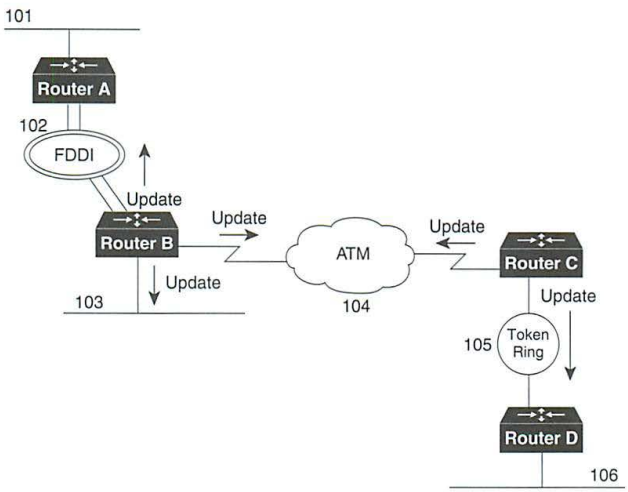
Cisco IOS platforms perform both routing and switching, and there are several types of each.

Routing

The routing process assesses the source and destination of traffic based on knowledge of network conditions. Routing functions identify the best path to use for moving the traffic to the destination from one or more of the router interfaces. The routing decision is based on a variation of criteria such as link speed, topological distance, and protocol. Each separate protocol maintains its own routing information.

Routing is more processing intensive and has a higher latency than switching as it determines path and next-hop considerations. The first packet routed requires a lookup in the routing table to determine the route. The route cache is populated after the first packet is routed by the route-table lookup. Subsequent traffic for the same destination is switched using the routing information stored in the route cache. Figure 1-2 illustrates the basic routing process.

Figure 1-2 *The Routing Process*

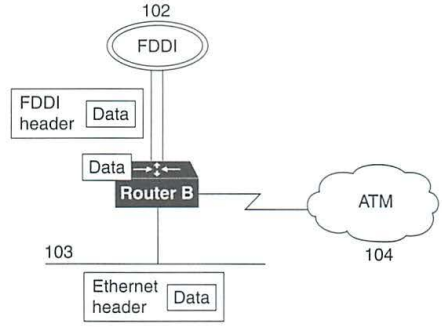


A router sends routing updates out to each of its interfaces that are configured for a particular protocol. It also receives routing updates from other attached routers. From these received updates and its knowledge of attached networks, it builds a map of the network topology.

Switching

Through the switching process, the router determines the next hop toward the destination address. Switching moves traffic from an input interface to one or more output interfaces. Switching is optimized and has a lower latency than routing because it can move packets, frames, or cells from buffer to buffer with a simpler determination of the source and destination of the traffic. It saves resources because it does not involve extra lookups. Figure 1-3 illustrates the basic switching process.

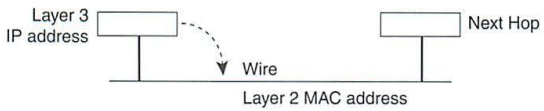
Figure 1-3 *The Switching Process*



In Figure 1-3, packets are received on the Fast Ethernet interface and destined for the FDDI interface. Based on information in the packet header and destination information stored in the routing table, the router determines the destination interface. It looks in the protocol's routing table to discover the destination interface that services the destination address of the packet.

The destination address is stored in tables, such as ARP tables for IP and AARP tables for AppleTalk. If there is no entry for the destination, the router will either drop the packet (and inform the user if the protocol provides that feature), or it must discover the destination address by some other address resolution process, such as through the ARP protocol. Layer 3 IP addressing information is mapped to the Layer 2 MAC address for the next hop. Figure 1-4 illustrates the mapping that occurs to determine the next hop.

Figure 1-4 *Layer 3-to-Layer 2 Mapping*



Basic Switching Paths

Basic switching paths are

- Process Switching
- Fast Switching
- Distributed Switching
- NetFlow Switching

Process Switching

In process switching, the first packet is copied to the system buffer. The router looks up the Layer 3 network address in the routing table and initializes the fast-switch cache. The frame is rewritten with the destination address and sent to the exit interface that services that destination. Subsequent packets for that destination are sent by the same switching path. The route processor computes the cyclic redundancy check (CRC).

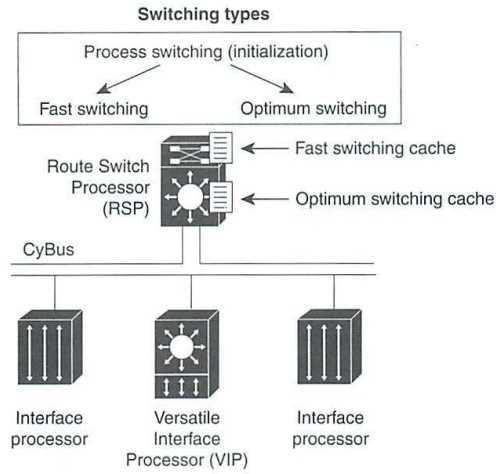
Fast Switching

When packets are fast switched, the first packet is copied to packet memory and the destination network or host is found in the fast-switching cache. The frame is rewritten and sent to the exit interface that services the destination. Subsequent packets for the same destination use the same switching path. The interface processor computes the CRC.

Distributed Switching

Switching becomes more efficient the closer to the interface the function occurs. In distributed switching, the switching process occurs on VIP and other interface cards that support switching. Figure 1-5 illustrates the distributed switching process on the Cisco 7500 series.

Figure 1-5 *Distributed Switching on Cisco 7500 Series Routers*



The VIP card installed in this router maintains a copy of the routing cache information needed to forward packets. Because the VIP card has the routing information it needs, it performs the switching locally, making the packet forwarding much faster. Router throughput is increased linearly based on the number of VIP cards installed in the router.

NetFlow Switching

NetFlow switching enables you to collect the data required for flexible and detailed accounting, billing, and chargeback for network and application resource utilization. Accounting data can be collected for both dedicated line and dial-access accounting. NetFlow switching over a foundation of VLAN technologies provides the benefits of switching and routing on the same platforms. NetFlow switching is supported over switched LAN or ATM backbones, allowing scalable inter-VLAN forwarding. NetFlow switching can be deployed at any location in the network as an extension to existing routing infrastructures. NetFlow switching is described in Chapter 8, "Configuring NetFlow Switching."

Platform and Switching Path Correlation

Depending on the routing platform you are using, availability and default implementations of switching paths varies. Table 1-1 shows the correlation between Cisco IOS switching paths and routing platforms.

Table 1-1 *Switching Paths on RSP-Based Routers*

Switching Path	Cisco 7200	Cisco 7500	Comments	Configuration Command
Process switching	Yes	Yes	Initializes switching caches	**no** *protocol* **route-cache**
Fast switching	Yes	Yes	Default (except for IP)	*protocol* **route-cache**
Distributed switching	No	Yes	Using second-generation VIP line cards	*protocol* **route-cache distributed**
NetFlow switching	Yes	Yes	Configurable per interface	*protocol* **route-cache flow**

Features That Affect Performance

Performance is derived from the switching mechanism you are using. Some Cisco IOS features require special handling and cannot be switched until the additional processing they require has been performed. This special handling is not processing that the interface processors can do. Because these features require additional processing, they affect switching performance. These features include

- Queuing
- Random Early Detection
- Compression
- Filtering
- Encryption
- Accounting

Queuing

Queuing occurs when network congestion occurs. When traffic is moving well within the network, packets are sent as they arrive at the interface. Cisco IOS software implements four different queuing algorithms:

- First-in, first-out (FIFO) queuing – Packets are forwarded in the same order in which they arrive at the interface.
- Priority queuing – Packets are forwarded based on an assigned priority. You can create priority lists and groups to define rules for assigning packets to priority queues.
- Custom queuing – You can control a percentage of interface bandwidth for specified traffic by creating protocol queue lists and custom queue lists.
- Weighted fair queuing – Weighted fair queuing provides automatic traffic priority management. Low-bandwidth sessions have priority over high-bandwidth sessions and high-bandwidth session are assigned weights. Weighted fair queuing is the default for interfaces slower than 2.048 Mbps.

Random Early Detection

Random early detection is designed for congestion avoidance. Traffic is prioritized based on type of service (TOS) or precedence. This feature is available on T3, OC-3, and ATM interfaces.

Compression

Depending on the protocol you are using, various compression options are available in Cisco IOS software.

Filtering

You can define access lists to control access to or from a router for a number of services. You could, for example, define an access list to prevent packets with a certain IP address from leaving a particular interface on a router. How access lists are used depends on the protocol.

Encryption

Encryption algorithms are applied to data to alter its appearance, making it incomprehensible to those who are not authorized to see the data.

Accounting

You can configure accounting features to collect network data related to resource usage. The information you collect (in the form of statistics) can be used for billing, chargeback, and planning resource usage.

CHAPTER 2

Configuring Switching Paths

This chapter describes how to configure switching paths on Cisco IOS devices. It provides configuration guidelines for switching paths and tuning guidelines. To find documentation of other commands, you can search online at www.cisco.com.

Fast Switching Configuration Task List

Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding. Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching.

Use the commands in these sections to configure appropriate fast switching features:

- Enabling AppleTalk Fast Switching
- Enabling IP Fast Switching
- Enabling Fast Switching on the Same IP Interface
- Enabling Fast Switching of IPX-Directed Broadcast Packets
- Disabling Banyan VINES Fast Switching
- Enabling Fast Switching of IPX-Directed Broadcast Packets

Fast Switching is not supported for the X.25 encapsulations.

Enabling AppleTalk Fast Switching

AppleTalk access lists are automatically fast switched. Access list fast switching improves the performance of AppleTalk traffic when access lists are defined on an interface.

Enabling IP Fast Switching

Fast switching involves the use of a high-speed switching cache for IP routing. Destination IP addresses are stored in the high-speed cache to expedite packet forwarding. In some cases, fast switching is inappropriate, such as when slow-speed serial links (64K and below) are being fed from higher-speed media such as T1 or Ethernet. In such a case, disabling fast switching can reduce the packet drop rate to some extent. Fast switching allows outgoing packets to be load balanced on a *per-destination* basis.

To enable or disable fast switching, use either of the following commands in interface configuration mode:

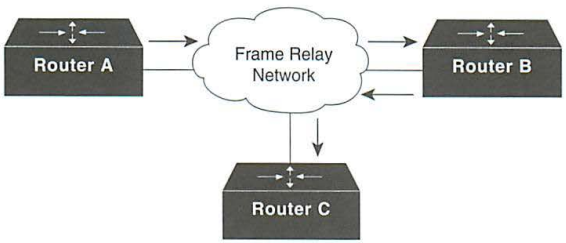
Command	Purpose
ip route-cache	Enables fast switching (use of a high-speed route cache for IP routing).
no ip route-cache	Disables fast switching and enable load balancing on a per-packet basis.

Enabling Fast Switching on the Same IP Interface

You can enable IP fast switching when the input and output interfaces are the same interface. This normally is not recommended, though it is useful when you have partially meshed media such as Frame Relay. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection.

Figure 2-1 illustrates a scenario where this is desirable. Router A has a data link connection identifier (DLCI) to Router B, and Router B has a DLCI to Router C. There is no DLCI between Routers A and C; traffic between them must go in and out of Router B through the same interface.

Figure 2-1 *IP Fast Switching on the Same Interface*



To allow IP fast switching on the same interface, use the following command in interface configuration mode:

Command	Purpose
ip route-cache same-interface	Enables the fast switching of packets out of the same interface on which they arrived.

Enabling Fast Switching of IPX-Directed Broadcast Packets

By default, Cisco IOS software switches packets that have been directed to the broadcast address. To enable fast switching of these IPX-directed broadcast packets, use the following command in global configuration mode:

Command	Purpose
ipx broadcast-fast switching	Enables fast switching of IPX directed broadcast packets.

Enabling SMDS Fast Switching

SMDS fast switching of IP, IPX, and AppleTalk packets provides faster packet transfer on serial links with speeds above 56 kbps. Use fast switching if you use high-speed, packet-switched, datagram-based WAN technologies such as Frame Relay offered by service providers.

By default, SMDS fast switching is enabled.

To re-enable fast switching, if it has been disabled, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type number*	Defines the type and unit number of the interface, and enters interface configuration mode.
2	**encapsulation smds**	Sets SMDS encapsulation.
3	**ip route-cache**	Enables the interface for IP fast switching.
4	**ipx route-cache**	Enables the interface for IPX fast switching.
5	**appletalk route-cache**	Enables the interface for AppleTalk fast switching.

Disabling Fast Switching for Troubleshooting

Fast switching uses a cache created by previous packets to achieve a higher packet throughput. Packet transfer performance is generally better when fast switching is enabled. Fast switching also provides load sharing on a per-packet basis.

By default, fast switching is enabled on all interfaces that support fast switching. However, you may want to disable fast switching to save memory space on interface cards and to help avoid congestion when high-bandwidth interfaces are writing large amounts of information to low-bandwidth interfaces. This is especially important when using rates slower than T1.

Fast switching is not supported on serial interfaces using encapsulations other than HDLC.

NOTE Turning off fast switching increases system overhead.

For some diagnostics such as debugging and packet-level tracing, you will need to disable fast switching. If fast switching is running, you will not see packets unless they pass through the route processor. Packets would otherwise be switched on the interface. You might want to turn off fast switching temporarily and bypass the route processor while you are trying to capture information.

This section includes these topics:

- Disabling AppleTalk Fast Switching
- Disabling Banyan VINES Fast Switching
- Disabling DECnet Fast Switching
- Disabling IPX Fast Switching
- Disabling ISO CLNS Fast Switching Through the Cache
- Disabling XNS Fast Switching

Disabling AppleTalk Fast Switching

To disable AppleTalk fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
no appletalk route-cache	Disables AppleTalk fast switching.

Disabling Banyan VINES Fast Switching

Fast switching is enabled by default on all interfaces on which it is supported.

To disable fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
no vines route-cache	Disables fast switching.

Disabling DECnet Fast Switching

By default, Cisco's DECnet routing software implements fast switching of DECnet packets.

To disable fast switching of DECnet packets, use the following command in interface configuration mode:

Command	Purpose
no decnet route-cache	Disables fast switching of DECnet packets on a per-interface basis.

Disabling IPX Fast Switching

To disable IPX fast switching, use the following command in interface configuration mode:

Command	Purpose
no ipx route-cache	Disables IPX fast switching.

Disabling ISO CLNS Fast Switching Through the Cache

ISO CLNS fast switching through the cache is enabled by default for all supported interfaces. To disable fast switching, use the following command in interface configuration mode:

Command	Purpose
no clns route-cache	Disables fast switching.

NOTE The cache still exists and is used after the **no clns route-cache** interface configuration command is used; the software just does not do fast switching through the cache.

Disabling XNS Fast Switching

To disable XNS fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
no xns route-cache	Disables XNS fast switching.

Controlling the Route Cache

The high-speed route cache used by IP fast switching is invalidated when the IP routing table changes. By default, the invalidation of the cache is delayed slightly to avoid excessive CPU load while the routing table is changing. To control the route cache, use the appropriate commands in these sections:

- Controlling Route Cache Invalidation for IP
- Displaying System and Network Statistics
- Adjusting the Route Cache for IPX
- Padding Odd-Length IPX Packets

Controlling Route Cache Invalidation for IP

To control route cache invalidation, use the following commands in global configuration mode as needed for your network:

Command	Purpose
no ip cache-invalidate-delay	Allows immediate invalidation of the cache.
ip cache-invalidate-delay [*minimum maximum quiet threshold*]	Delays invalidation of the cache.

NOTE This task normally should not be necessary. It should be performed only under the guidance of technical staff. Incorrect configuration can seriously degrade the performance of your router.

Displaying System and Network Statistics

You can display the contents of IP routing tables and caches. The resulting information can be used to determine resource utilization and to solve network problems.

Use the following command in privileged EXEC mode:

Command	Purpose
show ip cache [*prefix mask*] [*type number*]	Displays the routing table cache used to fast switch IP traffic.

Adjusting the Route Cache for IPX

Adjusting the route cache allows you to control the size of the route cache, reduce memory consumption, and improve router performance. You accomplish these tasks by controlling the route cache size and invalidation. The following sections describe these optional tasks:

- Controlling IPX Route Cache Size
- Controlling IPX Route Cache Invalidation

Controlling IPX Route Cache Size

You can limit the number of entries stored in the IPX route cache to free up router memory and aid router processing.

Storing too many entries in the route cache can use a significant amount of router memory, causing router processing to slow. This situation is most common on large networks that run network management applications for NetWare.

For example, if a network management station is responsible for managing all clients and servers in a very large (more than 50,000 nodes) Novell network, the routers on the local segment can become inundated with route cache entries. You can set a maximum number of route cache entries on these routers to free up router memory and aid router processing.

To set a maximum limit on the number of entries in the IPX route cache, use the following command in global configuration mode:

Command	Purpose
ipx route-cache max-size *size*	Sets a maximum limit on the number of entries in the IPX route cache.

If the route cache has more entries than the specified limit, the extra entries are not deleted. However, they may be removed if route cache invalidation is in use. See the "Controlling IPX Route Cache Invalidation" section in this chapter for more information on invalidating route cache entries.

Controlling IPX Route Cache Invalidation

You can configure the router to invalidate fast switch cache entries that are inactive. If these entries remain invalidated for 1 minute, the router purges the entries from the route cache.

Purging invalidated entries reduces the size of the route cache, reduces memory consumption, and improves router performance. Purging entries also helps ensure accurate route cache information.

You can specify the period of time that valid fast switch cache entries must be inactive before the router invalidates them. You can also specify the number of cache entries that the router can invalidate per minute.

To configure the router to invalidate fast-switch cache entries that are inactive, use the following command in global configuration mode:

Command	Purpose
ipx route-cache inactivity-timeout *period* [*rate*]	Invalidates fast switch cache entries that are inactive.

When you use the **ipx route-cache inactivity-timeout** command with the **ipx route-cache max-size** command, you can ensure a small route cache with fresh entries.

Padding Odd-Length IPX Packets

Some IPX end hosts accept only even-length Ethernet packets. If the length of a packet is odd, the packet must be padded with an extra byte so that the end host can receive it. By default, Cisco IOS pads odd-length Ethernet packets.

However, there are cases in certain topologies where non-padded Ethernet packets are being forwarded onto a remote Ethernet network. Under specific conditions, you can enable padding on intermediate media as a temporary workaround for this problem. Note that you should perform this task only under the guidance of a customer engineer or other service representative.

To enable the padding of odd-length packets, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**no ipx route-cache**	Disables fast switching.
2	**ipx pad-process-switched-packets**	Enables the padding of odd-length packets.

CHAPTER 3

Cisco IOS Switching Commands

This chapter documents commands used to configure switching features in Cisco IOS software.

NOTE Beginning with Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on Cisco 7000 series routers.

clear ip flow stats

To clear the NetFlow switching statistics, use the **clear ip flow stats** EXEC command.

clear ip flow stats

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CA.

The **show ip cache flow** command displays the NetFlow switching statistics. Use the **clear ip flow stats** command to clear the NetFlow switching statistics.

Example

The following example clears the NetFlow switching statistics on the router:

```
clear ip flow stats
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

show ip cache

encapsulation isl

Use the **encapsulation isl** subinterface configuration command to enable Inter-Switch Link (ISL). ISL is a Cisco protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.

encapsulation isl *vlan-identifier*

Syntax	Description
vlan-identifier	Virtual LAN identifier. The allowed range is 1 to 1000.

Default

Disabled

Command Mode

Subinterface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

ISL encapsulation is configurable on Fast Ethernet interfaces.

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between switches.

Example

The following example enables ISL on Fast Ethernet subinterface 2/1.20:

```
interface FastEthernet 2/1.20
 encapsulation isl 400
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

bridge-group
debug vlan
show bridge vlan
show interfaces
show vlans

encapsulation sde

Use the **encapsulation sde** subinterface configuration command to enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs. IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

encapsulation sde *said*

Syntax

Description

said

Security association identifier. This value is used as the virtual LAN identifier. The valid range is 0 through 0xFFFFFFFE.

Default

Disabled

Command Mode

Subinterface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

SDE encapsulation is configurable only on the following interface types:

IEEE 802.10 Routing	IEEE 802.10 Transparent Bridging
• FDDI	• Ethernet
	• FDDI
	• HDLC serial
	• Transparent mode
	• Token Ring

Example

The following example enables SDE on FDDI subinterface 2/0.1 and assigns a VLAN identifier of 9999:

```
interface fddi 2/0.1
 encapsulation sde 9999
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

bridge-group
debug vlans
show bridge vlan2222
show interfaces
show vlans

encapsulation tr-isl

Use the **encapsulation tr-isl** subinterface configuration command to enable TRISL, a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.

encapsulation tr-isl trbrf-vlan *vlan-id* **bridge-num** *bridge-number*

Syntax	Description
vlan-id	Number identifying the VLAN.
bridge-number	Keyword that specifies the identification number of the bridge number on the ISL trunk. Possible values are 01 to 4095.

Command Mode

Subinterface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(4)T.

Examples

In the following example, TRISL is enabled on a Fast Ethernet interface:

```
interface FastEthernet4/0.2
 encapsulation tr-isl trbrf-vlan 999 bridge-num 14
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

clear drip counters
clear vlan statistics
multiring
multiring trcrf-vlan
show drip
show vlan
source-bridge trcrf-vlan

ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** global configuration command. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

ip cache-invalidate-delay [*minimum maximum quiet threshold*]
no ip cache-invalidate-delay

Syntax	Description
minimum	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
maximum	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
quiet	(Optional) Length of quiet period (in seconds) before invalidation.
threshold	(Optional) Maximum number of invalidation requests considered to be quiet.

Defaults

minimum = 2 seconds
maximum = 5 seconds, and 3 seconds with no more than zero invalidation requests

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

All cache invalidation requests are honored immediately.

This command should typically not be used except under the guidance of technical support personnel. Incorrect settings can seriously degrade network performance.

The IP fast-switching and autonomous-switching features maintain a cache of IP routes for rapid access. When a packet is to be forwarded and the corresponding route is not present in the cache, the packet is process-switched and a new cache entry is built. However, when routing table changes occur (such as when a link or an interface goes down), the route cache must be flushed so that it can be rebuilt with up-to-date routing information.

This command controls how the route cache is flushed. The intent is to delay invalidation of the cache until after routing has settled down. Because route table changes tend to be clustered in a short period of time, and the cache may be flushed repeatedly, a high CPU load might be placed on the router.

When this feature is enabled, and the system requests that the route cache be flushed, the request is held for at least *minimum* seconds. Then the system determines whether the cache has been "quiet" (that is, less than *threshold* invalidation requests in the last *quiet* seconds). If the cache has been quiet, the cache is then flushed. If the cache does not become quiet within *maximum* seconds after the first request, it is flushed unconditionally.

Manipulation of these parameters trades off CPU utilization versus route convergence time. Timing of the routing protocols is not affected, but removal of stale cache entries is affected.

Example

The following example sets a minimum delay of 5 seconds, a maximum delay of 30 seconds, and a quiet threshold of no more than 5 invalidation requests in the previous 10 seconds:

```
ip cache-invalidate-delay 5 30 10 5
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

ip route-cache
show ip cache

ip flow-cache entries

Use the **ip flow-cache entries** global configuration command to change the number of entries maintained in the NetFlow cache. Use the **no** form of this command to return to the default number of entries.

ip flow-cache entries *number*
no ip flow-cache entries

Syntax

Description

number

Number of entries to maintain in the NetFlow cache. The valid range is 1024 to 524288 entries. The default is 65536 (64 K).

Default

65536 entries (64K)

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1 CA.

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow** command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.

CAUTION Cisco recommends that you do not change the NetFlow cache entries. Improper use of this command could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Example

The following example increases the number of entries in the NetFlow cache to 131072 (128K):

```
ip flow-cache entries 131072
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

show ip cache

ip flow-export

To enable the exporting of information in NetFlow cache entries, use the **ip flow-export** global configuration command. To disable the exporting of information, use the **no** form of this command.

ip flow-export *ip-address udp-port* [**version 1** | **version 5** [**origin-as** | **peer-as**]]
no ip flow-export

Syntax	Description
ip-address	IP address of the workstation to which you want to send the NetFlow information.
udp-port	UDP protocol-specific port number.
version 1	(Optional) Specifies that the export packet uses the version 1 format. This is the default. The version field occupies the first two bytes of the export record. The number of records stored in the datagram is a variable between 1 and 24 for version 1.
version 5	(Optional) Specifies export packet uses the version 5 format. The number of records stored in the datagram is a variable between 1 and 30 for version 5.
origin-as	(Optional) Specifies that export statistics includes the origin autonomous system (AS) for the source and destination.
peer-as	(Optional) Specifies that export statistics includes the peer AS for the source and destination.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command was modified to include the **version** keyword in Cisco IOS Release 11.1 CA.

There is a lot of information in a NetFlow cache entry. When flow switching is enabled with the **ip route-cache flow** command, you can use the **ip flow-export** command to configure the router to export the flow cache entry to a workstation when a flow expires. This feature can be useful for purposes of statistics, billing, and security.

Version 5 format includes the source and destination AS addresses, source and destination prefix masks, and a sequence number. Because this change may appear on your router as a maintenance release, support for version 1 format is maintained with the **version 1** keyword.

For more information on version 1 and version 5 data format, refer to Chapter 8, "Configuring NetFlow Switching."

Examples

The following example configures the router to export the NetFlow cache entry to UDP port 125 on the workstation at 134.22.23.7 when the flow expires, using version 1 format:

```
ip flow-export 134.22.23.7 125
```

The following example configures the router to export the NetFlow cache entry to UDP port 2048 on the workstation at 134.22.23.7 when the flow expires, using version 5 format and including the peer AS information:

```
ip flow-export 134.22.23.7 2048 version 5 peer-as
```

Related Command

You can search online at www.cisco.com to find documentation of related commands.

ip route-cache flow

ip route-cache

Use the **ip route-cache** interface configuration command to control the use of high-speed switching caches for IP routing. To disable any of these switching modes, use the **no** form of this command.

ip route-cache [**cbus**]
no ip route-cache [**cbus**]

ip route-cache same-interface
no ip route-cache same-interface

ip route-cache [**flow**]
no ip route-cache [**flow**]

ip route-cache distributed
no ip route-cache distributed

Syntax	Description
cbus	(Optional) Enables both autonomous switching and fast switching.
same-interface	Enables fast-switching packets back out the interface on which they arrived.
flow	(Optional) Enables the Route Switch Processor (RSP) to perform flow switching on the interface.
distributed	Enables Versatile Interface Processor (VIP) distributed switching on the interface. This feature can be enabled on Cisco 7500 series routers with an RSP and VIP controllers. If both **ip route-cache flow** and **ip route-cache distributed** are configured, the VIP does distributed flow switching. If only **ip route-cache distributed** is configured, the VIP does distributed switching.

Defaults

IP autonomous switching is disabled.
Fast switching varies by interface and media.
Distributed switching is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **distributed** keyword first appeared in Cisco IOS Release 11.2.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis.

The **ip route-cache** command with no additional keywords enables fast switching.

Cisco routers generally offer better packet transfer performance when fast switching is enabled, with one exception. On networks using slow serial links (64K and below), disabling fast switching to enable the per-packet load sharing is usually the best choice.

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This normally is not recommended, though it is useful when you have partially meshed media, such as Frame Relay. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection.

When the RSP is flow switching, it uses a flow cache instead of a destination network cache to switch IP packets. The flow cache uses source and destination network address, protocol, and source and destination port numbers to distinguish entries.

The flow caching option can also be used to allow statistics to be gathered with a finer granularity. The statistics include IP subprotocols, well-known ports, total flows, average number of packets per flow, and average flow lifetime.

On Cisco 7500 series routers with RSP and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

Not all switching methods are available on all platforms.

Examples

The following example enables both fast switching and autonomous switching:

```
ip route-cache cbus
```

The following example disables both fast switching and autonomous switching:

```
no ip route-cache
```

The following example turns off autonomous switching only:

```
no ip route-cache cbus
```

The following example enables VIP distributed flow switching on the interface:

```
interface ethernet 0/5/0
 ip address 17.252.245.2 255.255.255.0
 ip route-cache distributed
 ip route-cache flow
```

The following example returns the system to its defaults (fast switching enabled; autonomous switching disabled):

```
ip route-cache
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

ip cache-invalidate-delay
show ip cache

ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** interface configuration command. To disable NetFlow switching, use the **no** form of this command.

ip route-cache flow
no ip route-cache flow

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

NetFlow switching is a high-performance, network-layer switching path that captures as part of its switching function a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service information that can be used for a wide variety of purposes such as network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export** global configuration command.

NetFlow switching is supported on IP and IP encapsulated traffic over all interface types and encapsulations except for ISL/VLAN, ATM and Frame Relay interfaces when more than one input access control list is used on the interface, and ATM LANE.

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow switching, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a connection-oriented basis as part of the flow, where access list checks are bypassed and packet switching and statistics capture are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a source and destination—both defined by a network-layer IP address and transport-layer port number. Specifically, a flow is identified as the combination of the following fields:

- Source IP Address
- Destination IP Address

- Source Port Number
- Destination Port Number
- Protocol Type
- Type of Service
- Input Interface

NetFlow switching operates by creating a flow cache that contains the information needed to switch and perform the access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard fast-switching path. As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created, packets identified as belonging to an existing flow can be switched based on the cached information and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

NetFlow switching is one of the available switching modes. When you configure NetFlow on an interface, the other switching modes are not used on that interface. Also, with NetFlow switching you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow switching is based on identifying packet flows and performing switching and access list processing within a router. It does not involve any connection-setup protocol either between routers or to any other networking device or end station and does not require any change externally—either to the traffic or packets themselves or to any other networking device. Thus, NetFlow switching is completely transparent to the existing network, including end stations and application software and network devices such as LAN switches. Also, because NetFlow switching is performed independently on each internetworking device, it does not need to be operational on each router in the network. Network planners can selectively invoke NetFlow switching (and NetFlow data export) on a router/interface basis to gain traffic performance, control, or accounting benefits in specific network locations.

NOTE NetFlow consumes more memory and CPU resources than other switching modes; therefore, it is important to understand the resources required on your router before enabling NetFlow.

Examples

The following example enables NetFlow switching on the interface:

```
interface ethernet 0/5/0
 ip address 17.252.245.2 255.255.255.0
 ip route-cache flow
```

The following example returns the interface to its defaults (fast switching enabled; autonomous switching disabled):

```
interface ethernet 0/5/0
 ip route-cache
```

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

ip flow-export
show ip cache

show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** EXEC command.

show ip cache [*prefix mask*] [*type number*]

Syntax	Description
prefix	(Optional) Display only the entries in the cache that match the prefix and mask combination.
mask	(Optional) Display only the entries in the cache that match the prefix and mask combination.
type	(Optional) Display only the entries in the cache that match the interface type and number combination.
number	(Optional) Display only the entries in the cache that match the interface type and number combination.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The arguments *prefix*, *mask*, *type*, and *number* first appeared in Cisco IOS Release 10.0. The **show ip cache** display shows MAC headers up to 92 bytes.

Sample Displays

The following is sample output from the **show ip cache** command:

```
Router# show ip cache

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length       Age       Interface       MAC Header
131.108.1.1/32      0:01:09   Ethernet0/0     AA0004000134000000C0357430800
131.108.1.7/32      0:04:32   Ethernet0/0     00000C01281200000C0357430800
131.108.1.12/32     0:02:53   Ethernet0/0     00000C029FD000000C0357430800
131.108.2.13/32     0:06:22   Fddi2/0         00000C05A3E000000C035753AAAA0300
                                              00000800
131.108.2.160/32    0:06:12   Fddi2/0         00000C05A3E000000C035753AAAA0300
                                              00000800
131.108.3.0/24      0:00:21   Ethernet1/2     00000C026BC600000C03574D0800
131.108.4.0/24      0:02:00   Ethernet1/2     00000C026BC600000C03574D0800
131.108.5.0/24      0:00:00   Ethernet1/2     00000C04520800000C03574D0800
131.108.10.15/32    0:05:17   Ethernet0/2     00000C025FF500000C0357450800
131.108.11.7/32     0:04:08   Ethernet1/2     00000C010E3A00000C03574D0800
131.108.11.12/32    0:05:10   Ethernet0/0     00000C01281200000C0357430800
131.108.11.57/32    0:06:29   Ethernet0/0     00000C01281200000C0357430800
```

Table 3-1 describes significant fields shown in the sample output from the **show ip cache** command.

Table 3-1 ***show ip cache*** *Field Descriptions*

Field	Description
IP routing cache version	Version number of this table. This number is incremented any time the table is flushed.
entries	Number of valid entries.
bytes	Number of bytes of processor memory for valid entries.
hash overflows	Number of times autonomous switching cache overflowed.
minimum invalidation interval	Minimum time delay between cache invalidation request and actual invalidation.
maximum invalidation interval	Maximum time delay between cache invalidation request and actual invalidation.
quiet interval	Length of time between cache flush requests before the cache will be flushed.
threshold *n* requests	Maximum number of requests that can occur while the cache is considered quiet.
invalidation rate *n* in last *m* seconds	Number of cache invalidations during the last *m* seconds.

Continues

Table 3-1 *show ip cache Field Descriptions*

Field	Description
0 in last 3 seconds	Number of cache invalidation requests during the last quiet interval.
last full cache invalidation occurred *hh:mm:ss* ago	Time since last full cache invalidation was performed.
prefix/length	Network reachability information for cache entry.
age	Age of cache entry.
interface	Output interface type and number.
MAC Header	Layer 2 encapsulation information for cache entry.

The following is sample output from the **show ip cache** command with a prefix and mask specified:

```
Router# show ip cache 131.108.5.0 255.255.255.0

IP routing cache version 4490, 119 entries, 17464 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:11:56 ago

Prefix/Length       Age       Interface       MAC Header
131.108.5.0/24      0:00:34   Ethernet1/2     00000C04520800000C03574D0800
```

The following is sample output from the **show ip cache** command with an interface specified:

```
Router# show ip cache e0/2

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length       Age       Interface       MAC Header
131.108.10.15/32    0:05:17   Ethernet0/2     00000C025FF500000C0357450800
```

show ip cache flow

To display a summary of the NetFlow switching statistics, use the **show ip cache flow** EXEC command.

show ip cache flow

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command was modified to update the display with the latest information in Cisco IOS Release 11.1 CA.

Sample Display

The following is a sample output from the **show ip cache flow** command:

```
Router# show ip cache flow
IP packet size distribution (12718M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .554 .042 .017 .015 .009 .009 .009 .013 .030 .006 .007 .005 .004 .004

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .003 .007 .139 .019 .098 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456448 bytes
  65509 active, 27 inactive, 820628747 added
  955454490 ager polls, 0 flow alloc failures
  Exporting flows to 1.1.15.1 (2057)
  820563238 flows exported in 34485239 udp datagrams, 0 failed
  last clearing of statistics 00:00:03

Protocol         Total  Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows   /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet     2656855    4.3        86    78    372.3      49.6      27.6
TCP-FTP        5900082    9.5         9    71     86.8      11.4      33.1
TCP-FTPD       3200453    5.1       193   461   1006.3      45.8      33.4
TCP-WWW      546778274  887.3        12   325  11170.8       8.0      32.3
TCP-SMTP      25536863   41.4        21   283    876.5      10.9      31.3
TCP-X           116391    0.1       231   269     43.8      68.2      27.3
TCP-BGP          24520    0.0        28   216      1.1      26.2      39.0
TCP-Frag         56847    0.0        24   952      2.2      13.1      33.2
TCP-other     49148540   79.7        47   338   3752.6      30.7      32.2
UDP-DNS      117240379  190.2         3   112    570.8       7.5      34.7
UDP-NTP        9378269   15.2         1    76     16.2       2.2      38.7
UDP-TFTP          8077    0.0         3    62      0.0       9.7      33.2
UDP-Frag         51161    0.0        14   322      1.2      11.0      39.4
UDP-other     45502422   73.8        30   174   2272.7       8.5      37.8
ICMP          14837957   24.0         5   224    125.8      12.1      34.3
IGMP             40916    0.0       170   207     11.3     197.3      13.5
IPINIP            3988    0.0     48713   393    315.2     644.2      19.6
GRE               3838    0.0        79   101      0.4      47.3      25.9
IP-other         77406    0.1        47   259      5.9      52.4      27.0
Total:       820563238 1331.7        15   304  20633.0       9.8      33.0
```

```
SrcIf     SrcIPaddress    DstIf     DstIPaddress    Pr SrcP DstP Pkts B/Pk Active
Fd0/0     80.0.0.3        Hs1/0     200.1.9.1       06 0621 0052    7   87    5.9
Fd0/0     80.0.0.3        Hs1/0     200.1.8.1       06 0620 0052    7   87    1.8
Hs1/0     200.0.0.3       Fd0/0     80.1.10.1       06 0052 0621    6   58    1.8
Hs1/0     200.0.0.3       Fd0/0     80.1.1.1        06 0052 0620    5   62    5.9
Fd0/0     80.0.0.3        Hs1/0     200.1.3.1       06 0723 0052   16   68    0.3
HS1/0     200.0.0.3       Fd0/0     80.1.2.1        06 0052 0726    6   58   11.8
Fd0/0     80.0.0.3        Hs1/0     200.1.5.1       06 0726 0052    6   96    0.3
Hs1/0     200.0.0.3       Fd0/0     80.1.4.1        06 0052 0442    3   76    0.3
Hs1/0     200.0.0.3       Fd0/0     80.1.7.1        06 0052 D381   11 1171    0.6
```

Table 3-2 describes the fields in the packet size distribution lines of the output from the **show ip cache flow** command.

Table 3-2 *Packet Size Distribution Field Descriptions*

Field	Description
IP packet size distribution	The two lines below this banner show the percentage distribution of packets by size range. In this display, 55.4% of the packets fall in the size range 33 to 64 bytes.

Table 3-3 describes the fields in the flow switching cache lines of the output from the **show ip cache flow** command.

Table 3-3 *Flow Switching Cache Display Field Descriptions*

Field	Description
bytes	Number of of bytes of memory the NetFlow cache uses.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command was entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to expire entries (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
exporting flows	IP address and UDP port number of the workstation to which flows are exported.
flows exported in udp datagrams	Total number of flows exported and the total number of UDP datagrams used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the **clear ip flow stats** command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 3-4 describes the fields in the activity-by-protocol lines of the output from the **show ip cache flow** command.

Table 3-4 *Activity-by-Protocol Display Field Descriptions*

Field	Description
Protocol	IP protocol and the "well known" port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to Total Packets for this protocol or number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol) or the total number of seconds for this summary period).
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, time-out, and so forth) in seconds or total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time this command was entered, in seconds or total flows for this protocol for this summary period.

Table 3-5 describes the fields in the current flow lines of the output from the **show ip cache flow** command.

Table 3-5 *Current Flow Display Field Descriptions*

Field	Description
SrcIf	Internal port name for the source interface.
SrcIPaddress	Source IP address for this flow.
DstIf	Router's internal port name for the destination interface.
DstIPaddress	Destination IP address for this flow.
Pr	IP protocol; for example, 6=TCP, 17=UDP, … as defined in RFC 1340.
SrcP	Source port address, TCP/UDP "well known" port number, as defined in RFC 1340.
DstP	Destination port address, TCP/UDP "well known" port number, as defined in RFC 1340.
Pkts	Number of packets observed for this flow.
B/Pkt	Average observed number of bytes per packet for this flow.
Active	Number of seconds between first and last packet of a flow.

CISCO SYSTEMS, INC. IPR2024-00540 Ex. 1010, p. 62 of 135
FORTINET, INC.

Related Commands

You can search online at www.cisco.com to find documentation of related commands.

ip route-cache
clear ip flow stats

PART VII

Virtual LANs

Chapter 17 Routing Between Virtual LANs Overview

Chapter 18 Configuring Routing Between VLANs with ISL Encapsulation

Chapter 19 Configuring Routing Between VLANs with IEEE 802.10 Encapsulation

Chapter 20 LAN Emulation Overview

Chapter 21 Configuring LAN Emulation

Chapter 22 LAN Emulation Commands

Chapter 23 MPOA Overview

Chapter 24 Configuring the MPOA Client

Chapter 25 Configuring the MPOA Server

Chapter 26 MPOA Commands

CHAPTER 17

Routing Between Virtual LANs Overview

This chapter provides an overview of virtual LANs (VLANs). It describes the encapsulation protocols used for routing between VLANs and provides some basic information about designing VLANs.

What Is a Virtual LAN?

A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. None of the switches within the defined group bridge any frames, not even broadcast frames, between two VLANs. Several key issues need to be considered when designing and building switched LAN internetworks.

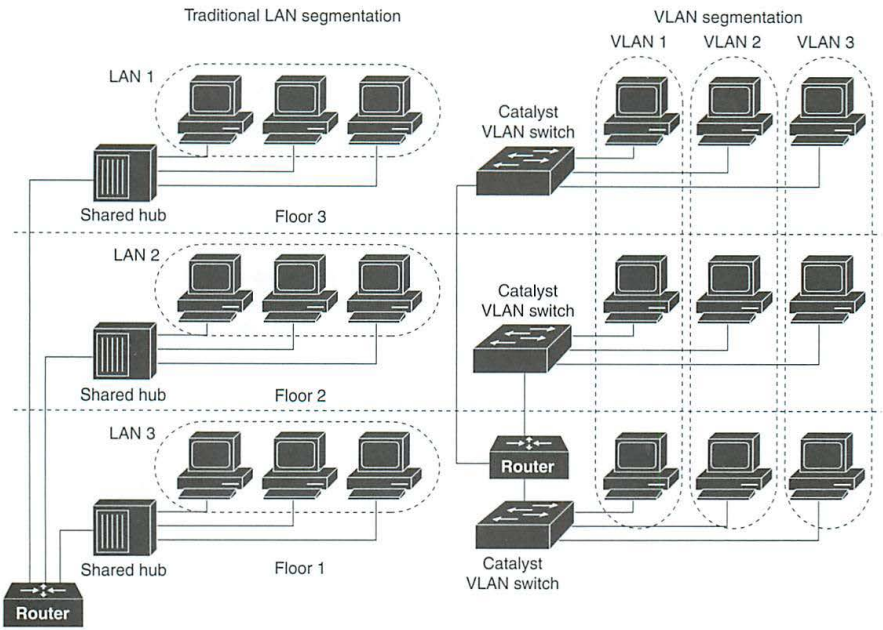
- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

LAN Segmentation

VLANs allow logical network topologies to overlay the physical, switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN sent only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth—a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.

Figure 17-1 illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation.

Figure 17-1 *LAN Segmentation and VLAN Segmentation*



Security

VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Just as switches isolate collision domains for attached hosts and forward appropriate traffic through a particular port, VLANs provide complete isolation between VLANs. A VLAN is a bridging domain and all broadcast and multicast traffic is contained within it.

Performance

The logical grouping of users allows an accounting group to make intensive use of a networked accounting system assigned to a VLAN that contains just that accounting group and its servers. That group's work does not affect other users. The VLAN configuration improves general network performance by not slowing down other users sharing the network.

Network Management

The logical grouping of users allows easier network management. It is not necessary to pull cables to move a user from one network to another. Adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.

Communication Between VLANs

Communication between VLANs is accomplished through routing, and the traditional security and filtering functions of the router can be used. Cisco IOS software provides network services such as security filtering, QoS, and accounting on a per-VLAN basis. As switched networks evolve to distributed VLANs, Cisco IOS provides key inter-VLAN communications and allows each network to scale.

VLAN Colors

VLAN switching is accomplished through *frame tagging*, where traffic originating and contained within a particular virtual topology carries a unique VLAN identifier (VLAN ID) as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions based on the embedded VLAN ID. Each VLAN is differentiated by a *color*, or VLAN identifier. The unique VLAN ID determines the *frame coloring* for the VLAN. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN (by the VLAN ID).

The VLAN ID allows VLAN switches and routers to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color. If you are using a Cisco network management product such as VlanDirector, you can actually color-code the VLANs and monitor VLAN graphically.

Why Implement VLANs?

Network managers can logically group networks that span all major topologies, including high-speed technologies such as ATM, FDDI, and Fast Ethernet. By creating VLANs, system and network administrators can control traffic patterns, react quickly to relocations, and keep up with constant changes in the network due to moving requirements and node relocation just by changing the VLAN member list in the router configuration. They can add, remove, or move devices or make other changes to network configuration by using software to make the changes.

Issues regarding benefits of creating VLANs should have been addressed when you developed your network design. Issues to consider include

- Scalability
- Performance improvements
- Security
- Network additions, moves, and changes

Communicating Between VLANs

Cisco IOS provides full-feature routing at Layer 3, and translation at Layer 2 between VLANs. There are three different protocols available for routing between VLANs:

- Inter-Switch Link (ISL)
- IEEE 802.10
- ATM LAN emulation

All three of these technologies are based on OSI Layer 2 bridge-multiplexing mechanisms.

ISL Protocol

ISL protocol is used to interconnect two VLAN-capable Fast Ethernet devices, such as the Catalyst 5000 or 3000 switches and Cisco 7500 routers. The ISL protocol is a packet-tagging protocol that contains a standard Ethernet frame and the VLAN information associated with that frame. The packets

on the ISL link contain a standard Ethernet, FDDI, or Token Ring frame and the VLAN information associated with that frame. ISL is currently supported only over Fast Ethernet links, but a single ISL link, or trunk, can carry different protocols from multiple VLANs.

IEEE 802.10 Protocol

The IEEE 802.10 protocol provides connectivity between VLANs. Originally developed to address the growing need for security within shared LAN/MAN environments, it incorporates authentication and encryption techniques to ensure data confidentiality and integrity throughout the network. Additionally, by functioning at Layer 2, it is well suited to high-throughput, low-latency switching environments. IEEE 802.10 protocol can run over any LAN or HDLC serial interface.

ATM LANE Protocol

The ATM LAN Emulation (LANE) protocol provides a way for legacy LAN users to take advantage of ATM benefits without requiring modifications to end-station hardware or software. LANE emulates a broadcast environment like IEEE 802.3 Ethernet on top of an ATM network that is a point-to-point environment.

LANE makes ATM function like a LAN. LANE allows standard LAN drivers such as NDIS and ODI to be used. The VLAN is transparent to applications. Applications can use normal LAN functions without dealing with the underlying complexities of the ATM implementation. For example, a station can send broadcasts and multicasts, even though ATM is defined as a point-to-point technology and doesn't support any-to-any services.

To accomplish this, special low-level software is implemented on an ATM client workstation, called the LAN Emulation Client, or LEC. The client software communicates with a central control point called a LAN Emulation Server, or LES. A Broadcast and Unknown Server (BUS) acts as a central point to distribute broadcasts and multicasts. The LAN Emulation Configuration Server (LECS) holds a database of LECs and the ELANs they belong to. The database is maintained by a network administrator.

VLAN Interoperability

Cisco IOS features bring added benefits to the VLAN technology. Enhancements to ISL, IEEE 802.10, and ATM LANE implementations enable routing of all major protocols between VLANs. These enhancements allow users to create more robust networks incorporating VLAN configurations by providing communications capabilities between VLANs.

Inter-VLAN Communications

The Cisco IOS software supports full routing of several protocols over ISL and ATM LANE virtual LANs. IP, Novell IPX, and AppleTalk routing are supported over IEEE 802.10 VLANs. Standard routing attributes, such as network advertisements, secondaries, and help addresses are applicable and VLAN routing is fast switched. Table 17-1 shows protocols supported for each VLAN encapsulation format and corresponding Cisco IOS releases.

Table 17-1 *Inter-VLAN Routing Protocol Support*

Protocol	ISL	ATM LANE	IEEE 802.10
IP	Release 11.1	Release 10.3	Release 11.1
Novell IPX (default encapsulation)	Release 11.1	Release 10.3	Release 11.1
Novell IPX (configurable encapsulation)	Release 11.3	Release 10.3	Release 11.3
AppleTalk Phase II	Release 11.3	Release 10.3	
DECnet	Release 11.3	Release 11.0	
Banyan VINES	Release 11.3	Release 11.2	
XNS	Release 11.3	Release 11.2	

VLAN Translation

VLAN translation refers to the ability of the Cisco IOS software to translate between different virtual LANs or between VLAN and non-VLAN encapsulating interfaces at Layer 2. Translation is typically used for selective inter-VLAN switching of non-routable protocols and to extend a single VLAN topology across hybrid switching environments. It is also possible to bridge VLANs on the main interface; the VLAN encapsulating header is preserved. Topology changes in one VLAN domain do not affect a different VLAN.

Designing Switched VLANs

By the time you are ready to configure routing between VLANs, you will have already defined them through the switches in your network. Issues related to network design and VLAN definition should be addressed during your network design:

- Sharing resources between VLANs
- Load balancing
- Redundant links
- Addressing
- Segmenting networks with VLANs

Segmenting the network into broadcast groups improves network security. Use router access lists based on station addresses, application types, and protocol types.

- Routers and their role in switched networks

  In switched networks, routers perform broadcast management and route processing and distribution, and they provide communications between VLANs. Routers provide VLAN access to shared resources and connect to other parts of the network that are either logically segmented with the more traditional subnet approach or require access to remote sites across wide-area links.

CHAPTER 18

Configuring Routing Between VLANs with ISL Encapsulation

This chapter describes the ISL protocol and provides guidelines for configuring ISL and Token Ring ISL (TRISL) features. To locate documentation of other commands that appear in this chapter, you can search online at www.cisco.com.

Overview of ISL Protocol

ISL is a Cisco protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full-wire speed performance on Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment and supports up to 1,000 VLANs. You can define as many logical networks as are necessary for your environment.

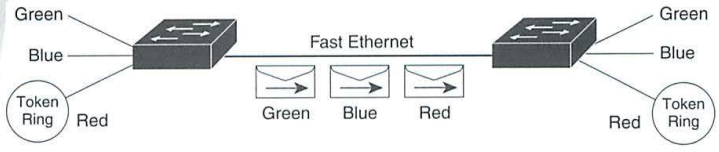
This chapter describes how to configure routing between VLANs using ISL encapsulation.

Frame Tagging in ISL

With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header that contains a 10-bit VLAN ID is prepended to the Ethernet frame.

A VLAN ID is added to the frame only when the frame is destined for a nonlocal network. Figure 18-1 illustrates VLAN packets traversing the shared backbone. Each VLAN packet carries the VLAN ID within the packet header.

Figure 18-1 *VLAN Packets Traversing the Shared Backbone*



ISL Encapsulation Configuration Task List

You can configure routing between any number of VLANs in your network. This section documents the configuration tasks for each protocol supported with ISL encapsulation. The basic process is the same, regardless of the protocol being routed. It involves

- Enabling the protocol on the router.
- Enabling the protocol on the interface.
- Defining the encapsulation format as ISL or TRISL.
- Customizing the protocol according to the requirements for your environment.

The configuration processes documented in this chapter include the following:

- Configuring AppleTalk Routing over ISL
- Configuring Banyan VINES Routing over ISL
- Configuring DECnet Routing over ISL
- Configuring Hot Standby Router Protocol over ISL
- Configuring IP Routing over TRISL
- Configuring IPX Routing over TRISL
- Configuring VIP Distributed Switching over ISL
- Configuring XNS Routing over ISL

Refer to the "ISL Encapsulation Configuration Examples" section at the end of this chapter for sample configurations.

Configuring AppleTalk Routing over ISL

AppleTalk can be routed over VLAN subinterfaces by using the ISL and IEEE 802.10 VLAN encapsulation protocols. The AppleTalk routing over ISL and IEEE 802.10 VLANs feature provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.

To route AppleTalk over ISL or IEEE 802.10 between VLANs, customize the subinterface to create the environment in which it will be used by performing these tasks in the order in which they appear:

- Enabling AppleTalk Routing
- Defining the VLAN Encapsulation Format
- Configuring AppleTalk on the Subinterface

Enabling AppleTalk Routing

To enable AppleTalk routing on either ISL or 802.10 interfaces, use this command in global configuration mode:

Command	Purpose
appletalk routing [**eigrp** *router-number*]	Enables AppleTalk routing globally.

Defining the VLAN Encapsulation Format

To define the VLAN encapsulation format as either ISL or 802.10, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface the VLAN will use.
2	**encapsulation isl** *vlan-identifier* **encapsulation sde** *said*	Defines the encapsulation format as either ISL (**isl**) or IEEE 802.10 (**sde**), and specifies the VLAN identifier or security association identifier, respectively.

Configuring AppleTalk on the Subinterface

After you enable AppleTalk globally and define the encapsulation format, you need to enable it on the subinterface by specifying the cable range and naming the AppleTalk zone for each interface. To enable the AppleTalk protocol on the subinterface, use the following commands in interface configuration mode:

Command	Purpose
appletalk cable-range *cable-range* [*network.node*]	Assigns the AppleTalk cable range and zone for the subinterface.
appletalk zone *zone-name*	Assigns the AppleTalk zone for the subinterface.

Configuring Banyan VINES Routing over ISL

Banyan VINES can be routed over VLAN subinterfaces by using the ISL encapsulation protocol. The Banyan VINES routing over ISL VLANs feature provides full-feature Cisco IOS software Banyan VINES support on a per-VLAN basis, allowing standard Banyan VINES capabilities to be configured on VLANs.

To route Banyan VINES over ISL between VLANs, configure ISL encapsulation on the subinterface by performing these tasks in the order in which they appear:

- Enabling Banyan VINES Routing
- Defining the VLAN Encapsulation Format
- Configuring Banyan VINES on the Subinterface

Enabling Banyan VINES Routing

To begin the VINES routing configuration, use the following command in global configuration mode:

Command	Purpose
vines routing [*address*]	Enables Banyan VINES routing globally.

Defining the VLAN Encapsulation Format

To define the VINES routing encapsulation format, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which ISL will be used.
2	**encapsulation isl** *vlan-identifier*	Defines the encapsulation format as ISL (**isl**), and specifies the VLAN identifier.

Configuring Banyan VINES on the Subinterface

After you enable Banyan VINES globally and define the encapsulation format, you need to enable VINES on the subinterface by specifying the VINES routing metric. To enable the Banyan VINES protocol on the subinterface, use the following command in interface configuration mode:

Command	Purpose
vines metric [*whole* [*fractional*]]	Enables VINES routing on an interface.

Configuring DECnet Routing over ISL

DECnet can be routed over VLAN subinterfaces using the ISL VLAN encapsulation protocols. The DECnet routing over ISL VLANs feature provides full-feature Cisco IOS software DECnet support on a per-VLAN basis, allowing standard DECnet capabilities to be configured on VLANs.

To route DECnet over ISL VLAN, configure ISL encapsulation on the subinterface by performing these tasks in the order in which they appear:

- Enabling DECnet Routing
- Defining the VLAN Encapsulation Format
- Configuring DECnet on the Subinterface

Enabling DECnet Routing

To begin the DECnet routing configuration, use the following command in global configuration mode:

Command	Purpose
decnet [*network-number*] **routing** [*decnet-address*]	Enables DECnet on the router.

Defining the VLAN Encapsulation Format

To define the encapsulation format, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which ISL will be used.
2	**encapsulation isl** *vlan_identifier*	Defines the encapsulation format as ISL (**isl**), and specifies the VLAN identifier.

Configuring DECnet on the Subinterface

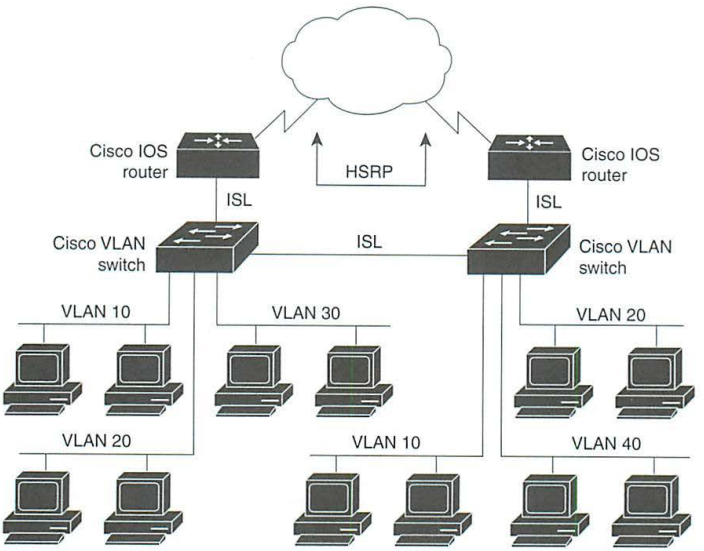
To configure DECnet routing on the subinterface, use the following command in interface configuration mode:

Command	Purpose
decnet cost [*cost-value*]	Enables DECnet routing on an interface.

Configuring Hot Standby Router Protocol over ISL

Hot Standby Router Protocol (HSRP) provides fault tolerance and enhanced routing performance for IP networks. HSRP allows Cisco IOS routers to monitor each other's operational status and very quickly assume packet forwarding responsibility in the event that the current forwarding device in the HSRP group fails or is taken down for maintenance. The standby mechanism remains transparent to the attached hosts and can be deployed on any LAN type. With multiple hot standby groups, routers can simultaneously provide redundant backup and perform load sharing across different IP subnets. Figure 18-2 illustrates HSRP in use with ISL providing routing between several VLANs.

Figure 18-2 *HSRP in VLAN Configurations*



A separate HSRP group is configured for each VLAN subnet so that Cisco IOS router A can be the primary and forwarding router for VLANs 10 and 20. At the same time, it acts as backup for VLANs 30 and 40. Conversely, Router B acts as the primary and forwarding router for ISL VLANs 30 and 40, as well as the secondary and backup router for distributed VLAN subnets 10 and 20.

Running HSRP over ISL allows users to configure redundancy between multiple routers that are configured as front ends for VLAN IP subnets. By configuring HSRP over ISLs, users can eliminate situations in which a single point of failure causes traffic interruptions. This feature inherently provides some improvement in overall networking resilience by providing load balancing and redundancy capabilities between subnets and VLANs.

To configure HSRP over ISLs between VLANs, create the environment in which it will be used by performing these tasks in the order in which they appear:

- Defining the Encapsulation Format
- Defining the IP Address
- Enabling HSRP

Defining the Encapsulation Format

To define the encapsulation format as ISL, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which ISL will be used.
2	**encapsulation isl** *vlan-identifier*	Defines the encapsulation format, and specify the VLAN identifier.

Defining the IP Address

After you have specified the encapsulation format, define the IP address over which HSRP will be routed. Use the following command in interface configuration mode:

Command	Purpose
ip address *ip-address mask* [**secondary**]	Specifies the IP address for the subnet on which ISL will be used.

Enabling HSRP

To enable HSRP on an interface, enable the protocol, and then customize it for the interface. Use the following command in interface configuration mode:

Command	Purpose
standby [*group-number*] **ip** [*ip-address* [**secondary**]]	Enables HSRP.

To customize hot standby group attributes, use one or more of the following commands in interface configuration mode:

Command	Purpose
standby [*group-number*] **timers** *hellotime holdtime*	Configures the time between hello packets and the hold time before other routers declare the active router to be down.
standby [*group-number*] **priority** *priority*	Sets the hot standby priority used to choose the active router.
standby [*group-number*] **preempt**	Specifies that if the local router has priority over the current active router, the local router should attempt to take its place as the active router.

Command	Purpose
standby [*group-number*] **track** *type-number* [*interface-priority*]	Configures the interface to track other interfaces, so that if one of the other interfaces goes down, the hot standby priority for the device is lowered.
standby [*group-number*] **authentication** *string*	Selects an authentication string to be carried in all HSRP messages.

Configuring IP Routing over TRISL

The IP routing over TRISL VLANs feature extends IP routing capabilities to include support for routing IP frame types in VLAN configurations.

Enabling IP Routing

IP routing is automatically enabled in the Cisco IOS software for routers. To re-enable IP routing if it has been disabled, use the following command in global configuration mode:

Command	Purpose
ip routing	Enables IP routing on the router.

When you have IP routing enabled on the router, you can customize the characteristics to suit your environment.

Defining the VLAN Encapsulation Format

To define the encapsulation format as TRISL, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which TRISL will be used.
2	**encapsulation tr-isl trbrf-vlan** *vlanid* **bridge-num** *bridge-number*	Defines the encapsulation for TRISL.

The DRiP database is automatically enabled when TRISL encapsulation is configured, and at least one TrBRF is defined, and the interface is configured for SRB or for routing with RIF.

Assigning IP Address to Network Interface

An interface can have one primary IP address. To assign a primary IP address and a network mask to a network interface, use the following command in interface configuration mode:

Command	Purpose
ip address *ip-address mask*	Sets a primary IP address for an interface.

A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a *subnet mask*.

NOTE TRISL encapsulation must be specified for a subinterface before an IP address can be assigned to that subinterface.

Configuring IPX Routing over ISL

The IPX routing over ISL VLANs feature extends Novell NetWare routing capabilities to include support for routing all standard IPX encapsulations for Ethernet frame types in VLAN configurations. Users with Novell NetWare environments can now configure any one of the four IPX Ethernet encapsulations to be routed using the ISL encapsulation across VLAN boundaries. IPX encapsulation options now supported for VLAN traffic include

- *novell-ether* (Novell Ethernet_802.3)
- *sap* (Novell Ethernet_802.2)
- *arpa* (Novell Ethernet_II)
- *snap* (Novell Ethernet_Snap)

NetWare users can now configure consolidated VLAN routing over a single VLAN trunking interface. With configurable Ethernet encapsulation protocols, users have the flexibility of using VLANs regardless of their NetWare Ethernet encapsulation. Configuring Novell IPX encapsulations on a per-VLAN basis facilitates migration between versions of Netware. NetWare traffic can now be routed across VLAN boundaries with standard encapsulation options (*arpa*, *sap*, and *snap*) previously unavailable.

NOTE Only one type of IPX encapsulation can be configured per VLAN (subinterface). The IPX encapsulation used must be the same within any particular subnet: A single encapsulation must be used by all NetWare systems that belong to the same virtual LAN.

To configure Cisco IOS software on a router with connected VLANs to exchange different IPX framing protocols, perform these tasks in the order in which they are appear:

- Enabling NetWare Routing
- Defining the VLAN Encapsulation Format
- Configuring NetWare on the Subinterface

Enabling NetWare Routing

To enable IPX routing on ISL interfaces, use the following command in global configuration mode:

Command	Purpose
ipx routing [*node*]	Enables IPX routing globally.

Defining the VLAN Encapsulation Format

To define the encapsulation format as ISL, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which ISL will be used.
2	**encapsulation isl** *vlan-identifier*	Defines the encapsulation format and specify the VLAN identifier.

Configuring NetWare on the Subinterface

After you enable NetWare globally and define theVLAN encapsulation format, you need to enable the subinterface by specifying the NetWare network number (if necessary) and the encapsulation type. Use this command in interface configuration mode:

Command	Purpose
ipx network *network* **encapsulation** *encapsulation-type*	Specifies the IPX encapsulation.

NOTE The default IPX encapsulation format for Cisco IOS routers is *novell-ether* (Novell Ethernet_802.3). If you are running Novell Netware 3.12 or 4.0, the new Novell default encapsulation format is Novell Ethernet_802.2 and you should configure the Cisco router with the IPX encapsulation format *sap*.

Configuring IPX Routing over TRISL

The IPX routing over ISL VLANs feature extends Novell NetWare routing capabilities to include support for routing all standard IPX encapsulations for Ethernet frame types in VLAN configurations. Users with Novell NetWare environments can configure either *sap* or *snap* encapsulations to be routed using the TRISL encapsulation across VLAN boundaries. The *sap* (Novell Ethernet_802.2) IPX encapsulation is supported for VLAN traffic.

NetWare users can now configure consolidated VLAN routing over a single VLAN trunking interface. With configurable Ethernet encapsulation protocols, users have the flexibility of using VLANs regardless of their NetWare Ethernet encapsulation. Configuring Novell IPX encapsulations on a per-VLAN basis facilitates migration between versions of Netware. NetWare traffic can now be routed across VLAN boundaries with standard encapsulation options (*sap* and *snap*) previously unavailable.

NOTE Only one type of IPX encapsulation can be configured per VLAN (subinterface). The IPX encapsulation used must be the same within any particular subnet: A single encapsulation must be used by all NetWare systems that belong to the same LANs.

To configure Cisco IOS software to exchange different IPX framing protocols on a router with connected VLANs, perform these tasks in the order in which they appear:

- Enabling NetWare Routing
- Defining the VLAN Encapsulation Format
- Configuring NetWare on the Subinterface

Enabling NetWare Routing

To enable IPX routing on TRISL interfaces, use the following command in global configuration mode:

Command	Purpose
ipx routing [*node*]	Enables IPX routing globally.

Defining the VLAN Encapsulation Format

To define the encapsulation format as TRISL, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which TRISL will be used.
2	**encapsulation tr-isl trbrf-vlan** *trbrf-vlan* **bridge-num** *bridge-num*	Defines the encapsulation for TRISL.

Configuring NetWare on the Subinterface

After you enable NetWare globally and define the VLAN encapsulation format, you need to enable the subinterface by specifying the NetWare network number (if necessary) and the encapsulation type. Use the following command in interface configuration mode:

Command	Purpose
ipx network *network* **encapsulation** *encapsulation-type*	Specifies the IPX encapsulation.

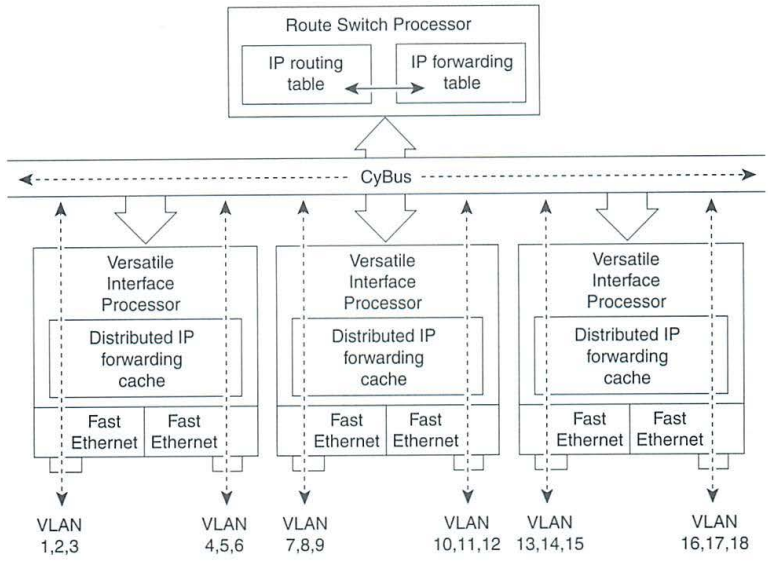
NOTE The default IPX encapsulation format for Cisco IOS routers is *novell-ether* (Novell Ethernet_802.3). If you are running Novell Netware 3.12 or 4.0, the new Novell default encapsulation format is Novell Ethernet_802.2 and you should configure the Cisco router with the IPX encapsulation format *sap*.

Configuring VIP Distributed Switching over ISL

With the introduction of the VIP Distributed ISL feature, ISL encapsulated IP packets can be switched on VIP controllers installed on Cisco 7500 series routers.

The VIP2 provides distributed switching of IP encapsulated in ISL in VLAN configurations. Where an aggregation route performs inter-VLAN routing for multiple VLANs, traffic can be switched autonomously on-card or between cards rather than through the central RSP. Figure 18-3 shows the VIP distributed architecture of the Cisco 7500 series router.

Figure 18-3 *Cisco 7500 Distributed Architecture*



This distributed architecture allows incremental capacity increases by installing additional VIP cards. Using VIP cards for switching the majority of IP VLAN traffic in multiprotocol environments significantly increases routing performance for the other protocols since the RSP offloads IP and can then be dedicated to switching the non-IP protocols.

VIP distributed switching offloads switching of ISL VLAN IP traffic to the VIP card, removing involvement from the main CPU. Offloading ISL traffic to the VIP card significantly improves networking performance. Because you can install multiple VIP cards in a router, VLAN routing capacity is increased linearly according to the number of VIP cards installed in the router.

To configure distributed switching on the VIP, you must first configure the router for IP routing by performing these tasks in the order in which they appear:

- Enabling IP Routing
- Enabling VIP Distributed Switching
- Configuring ISL Encapsulation on the Subinterface

Enabling IP Routing

To enable IP routing, use the following command in global configuration mode:

Command	Purpose
ip routing	Enables IP routing on the router.

When you have IP routing enabled on the router, you can customize the characteristics to suit your environment.

Enabling VIP Distributed Switching

To enable VIP distributed switching, use the following commands beginning in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port-adapter/port*	Specifies the interface and enters interface configuration mode.
2	**ip route-cache distributed**	Enables VIP distributed switching of IP packets on the interface.

Configuring ISL Encapsulation on the Subinterface

To configure ISL encapsulation on the subinterface, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port-adapter/port*	Specifies the interface and enters interface configuration mode.
2	**encapsulation isl** *vlan-identifier*	Defines the encapsulation format as ISL and specifies the VLAN identifier.

Configuring XNS Routing over ISL

XNS can be routed over VLAN subinterfaces using the ISL VLAN encapsulation protocol. The XNS routing over ISL VLANs feature provides full-feature Cisco IOS software XNS support on a per-VLAN basis, allowing standard XNS capabilities to be configured on VLANs.

To route XNS over ISL VLANs, configure ISL encapsulation on the subinterface by performing these tasks in the order in which they appear:

- Enabling XNS Routing
- Defining the VLAN Encapsulation Format
- Configuring XNS on the Subinterface

Enabling XNS Routing

Begin the XNS routing configuration by using the following commands in global configuration mode:

Command	Purpose
xns routing [*address*]	Enables XNS routing globally.

Defining the VLAN Encapsulation Format

To define the VLAN encapsulation format, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface on which ISL will be used.
2	**encapsulation isl** *vlan-identifier*	Defines the encapsulation format as ISL (**isl**, and specifies the VLAN identifier.

Configuring XNS on the Subinterface

Enable XNS on the subinterface by specifying the XNS network number. Use the following command in interface configuration mode:

Command	Purpose
xns network [*number*]	Enables XNS routing on the subinterface.

ISL Encapsulation Configuration Examples

This section provides configuration examples for each of the protocols described in this chapter. It includes these examples:

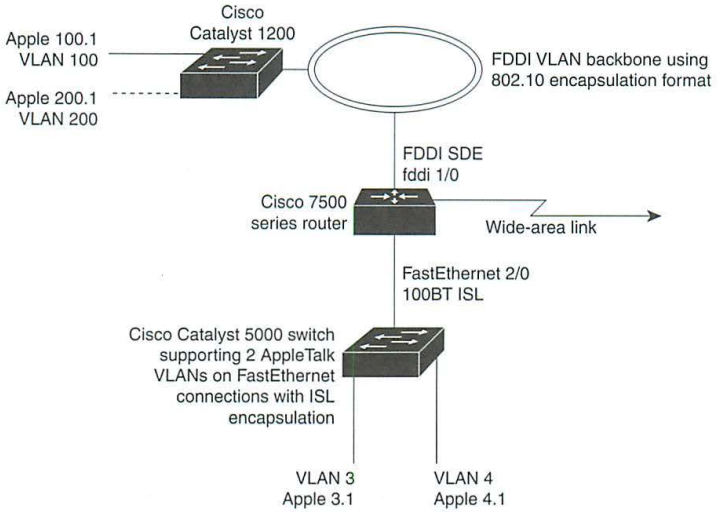
- AppleTalk routing over ISL configuration example
- Banyan VINES routing over ISL configuration example

- DECnet routing over ISL configuration example
- HSRP over ISL configuration example
- IP routing over RIF between TrBRF VLANs
- IP routing between a TRISL VLAN and an Ethernet ISL VLAN
- IPX routing over ISL configuration example
- Routing with RIF between a TRISL VLAN and a Token Ring interface
- VIP distributed switching over ISL configuration example
- XNS routing over ISL configuration example

AppleTalk Routing over ISL Configuration Example

The configuration example illustrated in Figure 18-4 shows AppleTalk being routed between different ISL and IEEE 802.10 VLAN encapsulating subinterfaces.

Figure 18-4 *Routing AppleTalk over VLAN encapsulations*



As shown in Figure 18-4, AppleTalk traffic is routed to and from switched VLAN domains 3, 4, 100, and 200 to any other AppleTalk routing interface. This example shows a sample configuration file for the Cisco 7500 series router with the commands entered to configure the network shown in Figure 18-4:

```
!
appletalk routing
interface Fddi 1/0.100
 encapsulation sde 100
 appletalk cable-range 100-100 100.2
 appletalk zone 100
!
interface Fddi 1/0.200
 encapsulation sde 200
 appletalk cable-range 200-200 200.2
 appletalk zone 200
!
interface FastEthernet 2/0.3
 encapsulation isl 3
 appletalk cable-range 3-3 3.2
 appletalk zone 3
!
interface FastEthernet 2/0.4
 encapsulation isl 4
 appletalk cable-range 4-4 4.2
 appletalk zone 4
!
```

Banyan VINES Routing over ISL Configuration Example

To configure routing of the Banyan VINES protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows Banyan VINES configured to be routed over an ISL trunk:

```
vines routing
interface fastethernet 0.1
 encapsulation isl 100
 vines metric 2
```

DECnet Routing over ISL Configuration Example

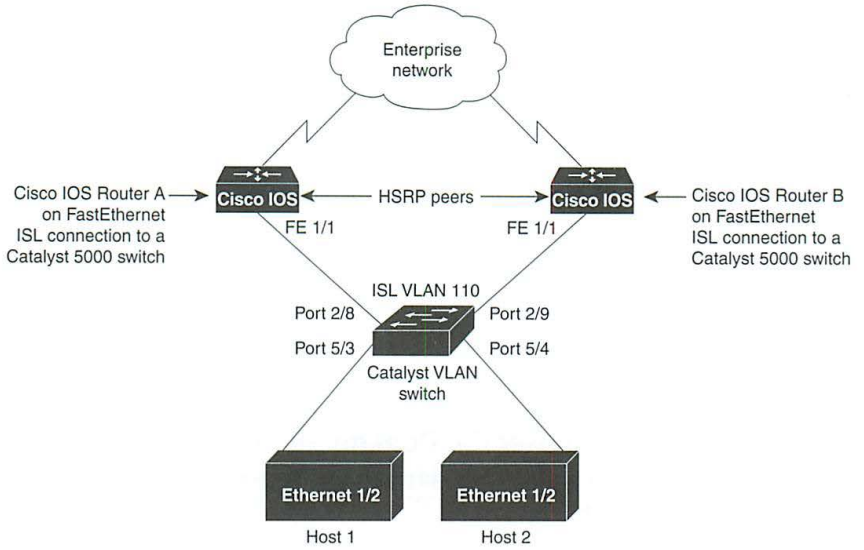
To configure routing the DECnet protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows DECnet configured to be routed over an ISL trunk:

```
decnet routing 2.1
interface fastethernet 1/0.1
 encapsulation isl 200
 decnet cost 4
```

HSRP over ISL Configuration Example

The configuration example shown in Figure 18-5 shows HSRP being used on two VLAN routers sending traffic to and from ISL VLANs through a Catalyst 5000 switch. Each router forwards its own traffic and acts as a standby for the other.

Figure 18-5 *HSRP Sample Configuration*



The topology shown in Figure 18-5 illustrates a Cisco Catalyst VLAN switch supporting Fast Ethernet connections to two routers running HSRP. Both routers are configured to route HSRP over ISLs.

The standby conditions are determined by the standby commands used in the configuration. Traffic from Host 1 is forwarded through Router A. Because the priority for the group is higher, Router A is the active router for Host 1. Because the priority for the group serviced by Host 2 is higher in Router B, traffic from Host 2 is forwarded through Router B, making Router B its active router.

In the configuration shown in Figure 18-5, if the active router becomes unavailable, the standby router assumes active status for the additional traffic and automatically routes the traffic normally handled by the router that has become unavailable.

The following is the Host 1 configuration:

```
interface Ethernet 1/2
 ip address 110.1.1.25 255.255.255.0
 ip route 0.0.0.0 0.0.0.0 110.1.1.101
```

The following is the Host 2 configuration:

```
interface Ethernet 1/2
 ip address 110.1.1.27 255.255.255.0
 ip route 0.0.0.0 0.0.0.0 110.1.1.102
!
```

The following is the Router A configuration:

```
interface FastEthernet 1/1.110
 encapsulation isl 110
 ip address 110.1.1.2 255.255.255.0
 standby 1 ip 110.1.1.101
 standby 1 preempt
 standby 1 priority 105
 standby 2 ip 110.1.1.102
 standby 2 preempt

!
end

!
```

The following is the Router B configuration:

```
interface FastEthernet 1/1.110
 encapsulation isl 110
 ip address 110.1.1.3 255.255.255.0
 standby 1 ip 110.1.1.101
 standby 1 preempt
 standby 2 ip 110.1.1.102
 standby 2 preempt
 standby 2 priority 105
router igrp 1
!
network 110.1.0.0
network 120.1.0.0
!
```

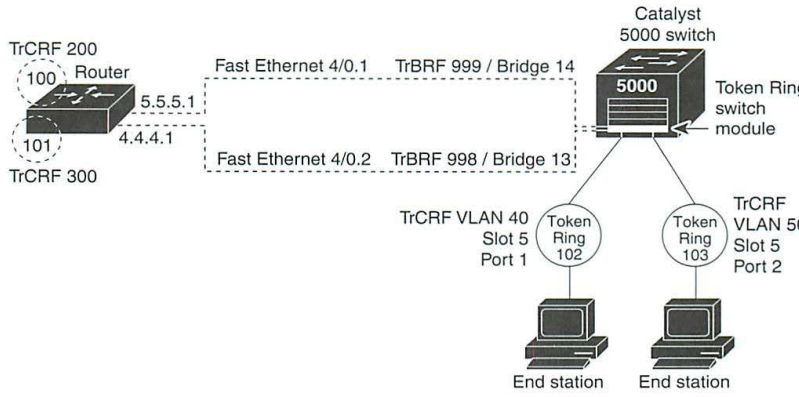
The following is the VLAN switch configuration:

```
set vlan 110 5/4
set vlan 110 5/3
set trunk 2/8 110
set trunk 2/9 110
```

IP Routing with RIF Between TrBRF VLANs

Figure 18-6 illustrates IP routing with RIF between two TrBRF VLANs.

Figure 18-6 *IP Routing with RIF Between TrBRF VLANs*



The following is the configuration for the router:

```
interface FastEthernet4/0.1
  ip address 5.5.5.1 255.255.255.0
  encapsulation tr-isl trbrf-vlan 999 bridge-num 14
  multiring trcrf-vlan 200 ring 100
  multiring all
!
  interface FastEthernet4/0.2
  ip address 4.4.4.1 255.255.255.0
  encapsulation tr-isl trbrf-vlan 998 bridge-num 13
  multiring trcrf-vlan 300 ring 101
  multiring all
```

The following is the configuration for the Catalyst 5000 switch with the Token Ring switch module in slot 5. In this configuration, the Token Ring port 102 is assigned with TrCRF VLAN 40 and the Token Ring port 103 is assigned with TrCRF VLAN 50:

```
#vtp
set vtp domain trisl
set vtp mode server
set vtp v2 enable
#drip
set set tokenring reduction enable
set tokenring distrib-crf disable
#vlans
set vlan 999 name trbrf type trbrf bridge 0xe stp ieee
set vlan 200 name trcrf200 type trcrf parent 999 ring 0x64 mode srb
set vlan 40 name trcrf40 type trcrf parent 999 ring 0x66 mode srb
set vlan 998 name trbrf type trbrf bridge 0xd stp ieee
set vlan 300 name trcrf300 type trcrf parent 998 ring 0x65 mode srb
set vlan 50 name trcrf50 type trcrf parent 998 ring 0x67 mode srb
#add token port to trcrf 40
```

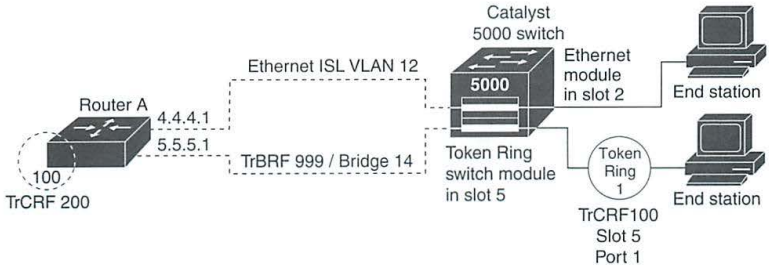
CISCO SYSTEMS, INC. IPR2024-00540 Ex. 1010, p. 92 of 135
FORTINET, INC.

```
set vlan 40   5/1
#add token port to trcrf 50
set vlan 50   5/2
set trunk 1/2 on
```

IP Routing Between a TRISL VLAN and an Ethernet ISL VLAN

Figure 18-7 illustrates IP routing between a TRISL VLAN and an Ethernet ISL VLAN.

Figure 18-7 *IP Routing Between a TRISL VLAN and an Ethernet ISL VLAN*



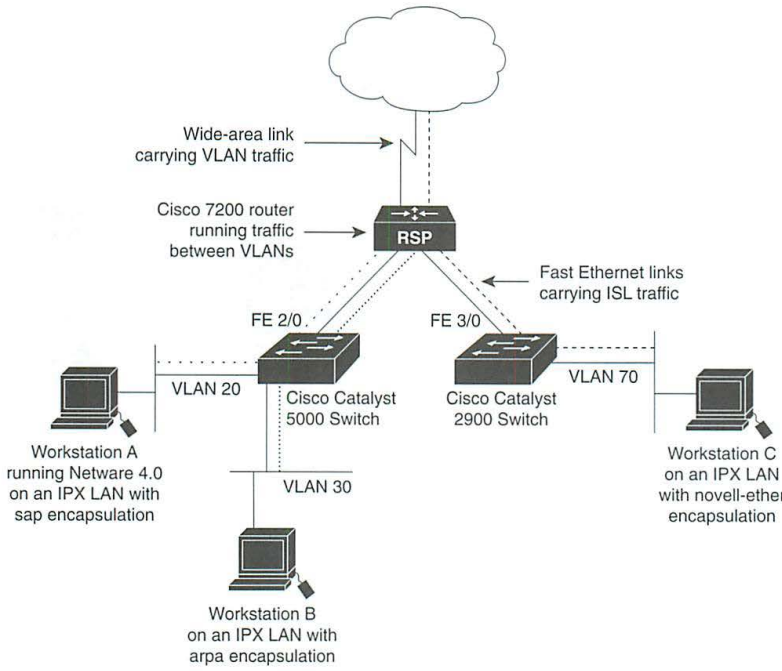
The following is the configuration for the router:

```
interface FastEthernet4/0.1
 ip address 5.5.5.1 255.255.255.0
 encapsulation tr-isl trbrf-vlan 999 bridge-num 14
 multiring trcrf-vlan 20 ring 100
 multiring all
!
interface FastEthernet4/0.2
 ip address 4.4.4.1 255.255.255.0
 encapsulation isl 12
```

IPX Routing over ISL Configuration Example

Figure 18-8 shows IPX interior encapsulations configured over ISL encapsulation in VLAN configurations. Note that three different IPX encapsulation formats are used. VLAN 20 uses *sap* encapsulation, VLAN 30 uses *arpa*, and VLAN 70 uses *novell-ether*. Prior to the introduction of this feature, only the default encapsulation format, *novell-ether*, was available for routing IPX over ISL links in VLANs.

Figure 18-8 *Configurable IPX Encapsulations Routed over ISL in VLAN Configurations*



The following is the VLAN 20 configuration:

```
ipx routing
interface FastEthernet 2/0
 no shutdown
interface FastEthernet 2/0.20
 encapsulation isl 20
 ipx network 20 encapsulation sap
```

The following is the VLAN 30 configuration:

```
ipx routing
interface FastEthernet 2/0
 no shutdown
interface FastEthernet 2/0.30
 encapsulation isl 30
 ipx network 30 encapsulation arpa
```

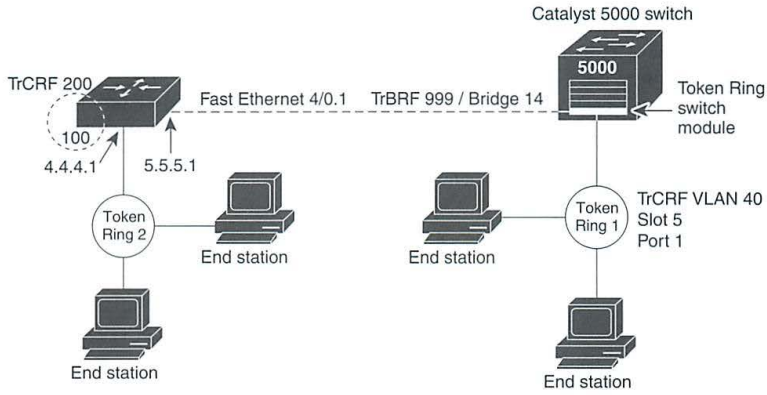
The following is the VLAN 70 configuration:

```
ipx routing
interface FastEthernet 3/0
 no shutdown
interface Fast3/0.70
 encapsulation isl 70
 ipx network 70 encapsulation novell-ether
```

Routing with RIF Between a TRISL VLAN and a Token Ring Interface

Figure 18-9 illustrates routing with RIF between a TRISL VLAN and a Token Ring interface.

Figure 18-9 *Routing with RIF Between a TRISL VLAN and a Token Ring Interface*



The following is the configuration for the router:

```
source-bridge ring-group 100
!
interface TokenRing 3/1
  ip address 4.4.4.1 255.255.255.0
!
interface FastEthernet4/0.1
  ip address 5.5.5.1 255.255.255.0
  encapsulation tr-isl trbrf 999 bridge-num 14
  multiring trcrf-vlan 200 ring-group 100
  multiring all
```

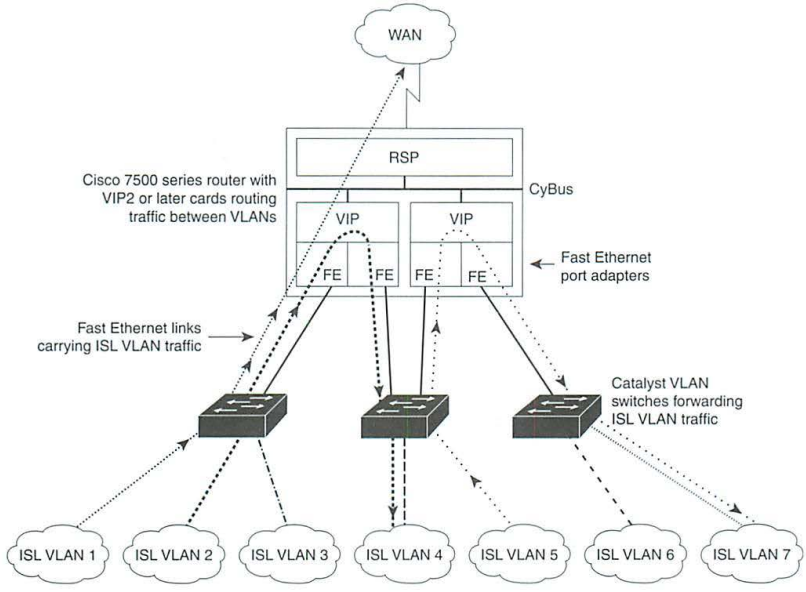
The following is the configuration for the Catalyst 5000 switch with the Token Ring switch module in slot 5. In this configuration, the Token Ring port 1 is assigned to the TrCRF VLAN 40:

```
#vtp
set vtp domain trisl
set vtp mode server
set vtp v2 enable
#drip
set set tokenring reduction enable
set tokenring distrib-crf disable
#vlans
set vlan 999 name trbrf type trbrf bridge 0xe stp ieee
set vlan 200 name trcrf200 type trcrf parent 999 ring 0x64 mode srt
set vlan 40 name trcrf40 type trcrf parent 999 ring 0x1 mode srt
#add token port to trcrf 40
set vlan 40   5/1
set trunk 1/2 on
```

VIP Distributed Switching over ISL Configuration Example

Figure 18-10 illustrates a topology in which Catalyst VLAN switches are connected to routers forwarding traffic from a number of ISL VLANs. With the VIP distributed ISL capability in the Cisco 7500 series router, each VIP card can route ISL-encapsulated VLAN IP traffic. The inter-VLAN routing capacity is increased linearly by the packet-forwarding capability of each VIP card.

Figure 18-10 *VIP Distributed ISL VLAN Traffic*



In Figure 18-10, the VIP cards forward the traffic between ISL VLANs or any other routing interface. Traffic from any VLAN can be routed to any of the other VLANs, regardless of which VIP card receives the traffic.

These commands show the configuration for each of the VLANs shown in Figure 18-10:

```
interface FastEthernet1/0/0
 ip address 20.1.1.1 255.255.255.0
 ip route-cache distributed
 full-duplex

interface FastEthernet1/0/0.1
 ip address 22.1.1.1 255.255.255.0
 encapsulation isl 1

interface FastEthernet1/0/0.2
 ip address 22.1.2.1 255.255.255.0
 encapsulation isl 2

interface FastEthernet1/0/0.3
 ip address 22.1.3.1 255.255.255.0
 encapsulation isl 3

interface FastEthernet1/1/0
 ip route-cache distributed
 full-duplex

interface FastEthernet1/1/0.1
 ip address 77.1.1.1 255.255.255.0
 encapsulation isl 4

interface FastEthernet 2/0/0
 ip address 30.1.1.1 255.255.255.0
 ip route-cache distributed
 full-duplex

interface FastEthernet2/0/0.5
 ip address 33.1.1.1 255.255.255.0
 encapsulation isl 5

interface FastEthernet2/1/0
 ip address 40.1.1.1 255.255.255.0
 ip route-cache distributed
 full-duplex

interface FastEthernet2/1/0.6
 ip address 44.1.6.1 255.255.255.0
 encapsulation isl 6

interface FastEthernet2/1/0.7
 ip address 44.1.7.1 255.255.255.0
 encapsulation isl 7
```

XNS Routing over ISL Configuration Example

To configure routing of the XNS protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows XNS configured to be routed over an ISL trunk:

```
xns routing 0123.4567.adcb
interface fastethernet 1/0.1
 encapsulation isl 100
 xns network 20
```

CHAPTER 19

Configuring Routing Between VLANs with IEEE 802.10 Encapsulation

This chapter describes the required and optional tasks for configuring routing between VLANs with IEEE 802.10 encapsulation. For a complete description of VLAN commands used in this chapter, refer to Chapter 3, "Cisco IOS Switching Commands." For documentation of other commands that appear in this chapter, you can search online at www.cisco.com.

The IEEE 802.10 standard provides a method for secure bridging of data across a shared backbone. It defines a single frame type known as the Secure Data Exchange (SDE), a MAC-layer frame with an IEEE 802.10 header inserted between the MAC header and the frame data. A well-known Logical Link Control Service Access Point notifies the switch of an incoming IEEE 802.10 frame. The VLAN ID is carried in the 4-byte Security Association Identifier (SAID) field.

HDLC serial links can be used as VLAN trunks in IEEE 802.10 virtual LANs to extend a virtual topology beyond a LAN backbone.

Configure AppleTalk Routing over IEEE 802.10

AppleTalk can be routed over VLAN subinterfaces by using the ISL or IEEE 802.10 VLAN encapsulation protocols. The AppleTalk Routing over IEEE 802.10 Virtual LANs feature provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.

AppleTalk users can now configure consolidated VLAN routing over a single VLAN trunking interface. Prior to introduction of this feature, AppleTalk could be routed only on the main interface on a LAN port. If AppleTalk routing was disabled on the main interface or if the main interface was shut down, the entire physical interface would stop routing any AppleTalk packets. With this feature enabled, AppleTalk routing on subinterfaces will be unaffected by changes in the main interface with the main interface in the "no-shut" state.

To route AppleTalk over IEEE 802.10 between VLANs, create the environment in which it will be used by customizing the subinterface by performing these tasks in the order in which they appear:

- Enabling AppleTalk Routing
- Configuring AppleTalk on the Subinterface
- Defining the VLAN Encapsulation Format

Enabling AppleTalk Routing

To enable AppleTalk routing on IEEE 802.10 interfaces, use the following command in global configuration mode:

Command	Purpose
appletalk routing [**eigrp** *router-number*]	Enables AppleTalk routing globally.

Configuring AppleTalk on the Subinterface

After you enable AppleTalk globally and define the encapsulation format, you need to enable it on the subinterface by specifying the cable range and naming the AppleTalk zone for each interface. To enable the AppleTalk protocol on the subinterface, use the following commands in interface configuration mode:

Command	Purpose
appletalk cable-range *cable-range* [*network.node*]	Assigns the AppleTalk cable range and zone for the subinterface.
appletalk zone *zone-name*	Assigns the AppleTalk zone for the subinterface.

Defining the VLAN Encapsulation Format

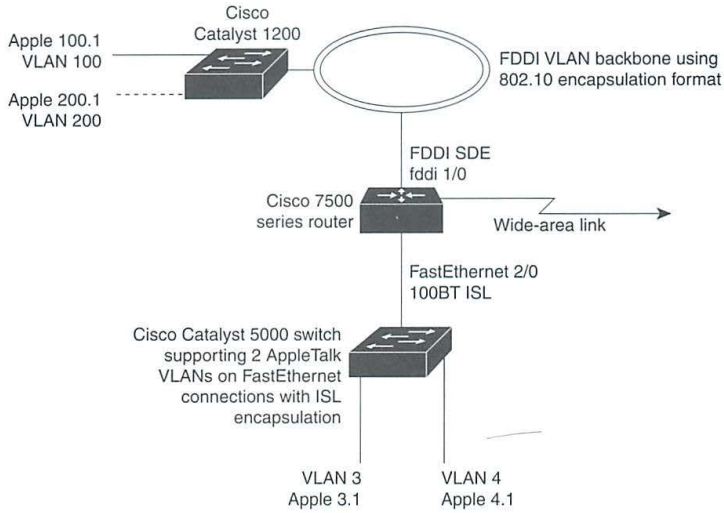
To define the VLAN encapsulation format as either ISL or 802.10, use the following commands in interface configuration mode:

Step	Command	Purpose
1	**interface** *type slot/port.subinterface-number*	Specifies the subinterface the VLAN will use.
2	**encapsulation sde** *said*	Defines the encapsulation format as IEEE 802.10 (**sde**) and specifies the VLAN identifier or security association identifier, respectively.

Routing AppleTalk over IEEE 802.10 Configuration Example

The configuration example illustrated in Figure 19-1 shows AppleTalk being routed between different ISL and IEEE 802.10 VLAN encapsulating subinterfaces.

Figure 19-1 *Routing AppleTalk over VLAN Encapsulations*



As shown in Figure 19-1, AppleTalk traffic is routed to and from switched VLAN domains 3, 4, 100, and 200 to any other AppleTalk routing interface. This example shows a sample configuration file for the Cisco 7500 series router with the commands entered to configure the network shown in Figure 19-1:

```
!
interface Fddi 1/0.100
 encapsulation sde 100
 appletalk cable-range 100-100 100.2
 appletalk zone 100
!
interface Fddi 1/0.200
 encapsulation sde 200
 appletalk cable-range 200-200 200.2
 appletalk zone 200
!
interface FastEthernet 2/0.3
 encapsulation isl 3
 appletalk cable-range 3-3 3.2
 appletalk zone 3
!
interface FastEthernet 2/0.4
 encapsulation isl 4
 appletalk cable-range 4-4 4.2
 appletalk zone 4
!
```

Numerics

802.10 standard. *See* IEEE 802.10
  standard, 241

A

access lists
  extended, 176
  MLS, 164
    affects, 166
    configuring, 175
    flow mask impact, 167
accounting, switching, 9
across-path traffic engineering, 96
address templates, LANE ATM
  addressing, 258
addresses
  ATM LANE, 257
    automatic assignment, 257
    clients, 299, 308
    configuration servers, 262
    defaults, 262, 340
    fixed LANE, 315
    LANE BUS, 305
    servers, 319, 326
  IP, mapping Layer 3 to Layer 2, 5
  LAN MAC, LANE resolution, 249
  LANE ATM. *See* ATM LANE
  LECS, 317
  NDE, specifying, 173
adjacency tables, 42
  clearing, 55
adjacency tables, Continued
  discovery, 43
  resolution, 43
  unresolved adjacencies, 43
AppleTalk
  configuring
    cable ranges, 217
    over encapsulating VLAN interfaces, 230
    routing, 241
    zones, 217
  fast switching, 11, 14
  routing
    IEEE 802.10 interfaces, 216, 242
    over ISL, 216, 230–231
    subinterfaces, 242
    VLANs, 243
    zones, 242
appletalk cable-range command, 217, 242
appletalk route-cache command, 13
appletalk routing command, 217, 242
appletalk routing eigrp command, 217
appletalk zone command, 217, 242
ATM
  addresses
    LANE BUS, 305
    LANE servers, 326
    MPC defaults, 382
    prefixes, LANE configuration, 282
  LANE, 253
    address templates, 258
    addresses, 257
    automatic server addresses, 303
    client addresses, 308

ATM, Continued
configuration servers, 262
configuring switch prefix, 261
defaults, 340
interface assignment rules, 259
servers, 319
tag bindings, summary information, 118-120
atm address command, 261
ATM interfaces
attaching MPCs, 372
attaching MPSs, 374
LANE, 245
ATM LANE protocol
configuration server addresses, 310
VLAN communications, 211
atm lecs-address command, 263
atm lecs-address-default command, 263
ATM networks
control addresses, overriding for MPOA, 365
MPOA connections, 351
atm pvc ilmi command, 262
atm pvc qsaal command, 262
ATM TDP database, 114–115
atm-address command, 355, 361, 365

B

backup paths, traffic engineering, 98
backups, LANE configuration servers, 280
Banyan VINES
encapsulation, 218
fast switching, 14
Banyan VINES, Continued
over ISL encapsulation, 217
routing
metric, 218
over ISL, 217, 231
BGP (Border Gateway Protocol), 78
binding LECs
to named MPCs, 369
to named MPSs, 370
binding tags, Tag Switching, 88
broadcast control, VLANs, 209
BUS (Broadcast and Unknown Server), LANE, 211, 246, 254
ATM addresses, 305
configuring, 270
enabling, 321
packet flooding, 249
redundancy, 273
viewing data, 331

C

cable ranges, AppleTalk routing, 217
cache
MLS, 161
MPC. *See* egress cache, ingress cache, 366
NetFlow, 78
controlling number of entries, 24
customizing number of entries, 82
exporting entries, 84
exporting entry data, 26
candidate packets, MLS, 162

CAR (Committed Access Rate), 168
CEF (Cisco Express Forwarding), 41
  accounting, 52
  adjacency tables, 42-43
    clearing, 55
  central CEF mode, 44
  counters, clearing, 57
  dCEF, enabling, 45, 50
  distributed tunnel switching, 53
  enabling, 49–50
    on route processor cards, 57–58
  FIB (Forwarding Information Base), 42
  GSRs, compatibility, 46
  load balancing, 50
  network accounting, 52
  per destination load balancing, 51
  per packet load balancing, 51
central CEF mode, 44
Cisco 12000 Gigabit Switched Router.
  See GSR, 187
Cisco Express Forwarding. *See* CEF
Cisco IOS 12.0 Reference Library, xvi–xvii
  book conventions, xviii
  command syntax, xix
Cisco IOS 12.0 Switching Services document
  overview, xv
clear adjacency command, 56
clear atm vc command, 295
clear cef linecard command, 57
clear ip cef prefix-statistics command, 57
clear ip flow stats command, 19, 83
clear ip mds forwarding command, 188, 191
clear ip mroute command, 188
clear ip pim interface count command, 188, 192
clear lane le-arp command, 296–297
clear lane server command, 297-299
clear mpoa client cache command, 355, 366
clear mpoa server cache command, 362, 367
clearing
  CEF
    adjacency table, 55
    counters, 57
  line cards, 55–56
  NetFlow switching statistics, 19
client-atm-address command, 299–300
client-atm-address name command, 268
clients
  emulated LANs, 271
  LANE, 246, 254, 271
    adding address to database, 299
    ATM addresses, 308
    clearing LE ARP table, 296
    clearing server, 297
    configuring, 269
    default emulated LAN names, 302
    displaying LE ARP table, 341
    joining emulated LANs, 248
    LE ARP table, 249
    MAC addresses, 257
    MPOA, 272
    multicast traffic, 249
    starting, 307
    static LE ARP table entries, 318
    viewing data, 333

clients, Continued
MPC, 347
MPOA, configuring, 353
command modes, xxiv
Global configuration, xxv
Interface configuration, xxv
Privileged EXEC, xxv
ROM monitor, xxv
Subinterface configuration, xxv
User EXEC, xxv
commands
appletalk cable-range, 217, 242
appletalk route-cache, 13
appletalk routing, 217, 242
appletalk zone, 217, 242
atm address, 261
atm lecs-address, 263
atm lecs-address-default, 263
atm pvc ilmi, 262
atm pvc qsaal, 262
atm-address, 355, 361, 365
clear atm vc, 295
clear ip flow stats, 19, 83
clear ip mds forwarding, 188, 191
clear ip mroute, 188
clear ip pim interface count, 188, 192
clear lane le-arp, 296–297
clear lane server, 297, 299
clear mpoa client cache, 355, 366
clear mpoa server cache, 362, 367
client-atm-address, 299–300
commands, Continued
client-atm-address name, 268
copy system, 261
decnet cost, 219
decnet routing, 219
default-name, 265, 302
defaults, xxvi
displaying syntax, xxi, xxiii
encapsulation isl, 20, 217
encapsulation sde, 21, 217, 242
encapsulation smds, 13
encapsulation tr-isl trbrf-vlan bridge-num, 222, 226
EXEC
clear cef linecard, 57
clear cef linecard command, 57
show adjacency, 64-66
show cef, 66–67
show cef interface, 68–69
show cef linecard, 70–71
show ip cef, 72–74
show tag-switching interfaces, 123–124
global configuration
clear adjacency, 56
ip cef, 49, 58
ip cef accounting, 60
ip cef traffic-statistics, 61
router traffic-engineering, 107
tag-switching advertise-tags, 135–136
tag-switching atm allocation-mode, 136
tag-switching atm maxhops, 139
tag-switching atm vc-merge, 140
tag-switching ip, 142

commands, Continued
tag-switching tag-range downstream, 145
tag-switching tdp discovery, 146
tag-switching tdp holdtime, 148
tag-switching tsp-tunnels, 149
holding-time, 361
holding-time (MPS), 368
interface, 13
interface atm, 262, 354, 361
interface configuration
ip load-sharing, 62
ip route-cache cef, 63–64
tag-switching atm control-vc, 137
tag-switching atm vpi, 141
tag-switching ip, 143
tag-switching mtu, 144
tag-switching tsp-tunnels, 150
tunnel mode tag-switching, 153
tunnel tsp-hop, 154
interface mul, 354
ip address, 221
ip cache-invalidate-delay, 16, 23
ip cef, 49
ip flow-cache entries, 24, 82
ip flow-export, 26, 82–84
ip flow-export version 5, 82
ip mroute-cache, 193
ip mroute-cache distributed, 188
ip multicast-routing, 194
ip multicast-routing distributed, 188
ip route-cache, 12–13, 27
ip route-cache distributed, 83, 188, 228
ip route-cache flow, 30, 82–83

commands, Continued
ip route-cache same-interface, 12
ip routing, 222
ipx broadcast-fastswitching, 13
ipx network encapsulation, 224–226
ipx pad-process-switched-packets, 18
ipx route-cache, 13
ipx route-cache inactivity-timeout, 17
ipx route-cache max-size, 17
ipx routing, 224
keepalive-time, 361
keepalive-time command (MPS), 368
lane auto-config-atm-address, 303
lane bus-atm-address, 305–306
lane client, 270, 307
lane client mpoa client name, 354, 369
lane client mpoa server name, 361, 370
lane client-atm-address, 308
lane config auto-config-atm-address, 269
lane config config-atm-address, 269
lane config database, 269
lane config fixed-config-atm-address command, 269
lane config-atm-address, 310–311
lane database, 264–266, 313
lane fixed-config-atm-address, 315–316
lane global-lecs-address, 317
lane le-arp, 318
lane server-atm-address, 319
lane server-bus, 270, 321, 360
lane server-bus ethernet, 354

commands, Continued
MDS configuration, 191
mls ip vlan-id, 180
mls rp ip, 169–170, 177
mls rp management-interface, 170, 178
mls rp nde-address, 173, 179
mls rp vip-domain, 170
mls rp vlan-id, 170
mls rp vtp-domain, 181
mpoa client config name, 354–355, 371
mpoa client name, 354, 372
mpoa server config name, 361, 373
mpoa server name, 361, 374
mpoa server name trigger ip-address, 362, 374
name elan-id, 354, 360
name elan-id LANE, 322
name local-seg-id, 265–266, 324
name preempt, 276
name preempt LANE, 323
name server-atm-address, 265–266, 326
name server-atm-address restricted, 267
network-id, 361
network-id (MPS), 375
no form, xxvi
no ip route-cache, 12
privileged EXEC
show ip traffic-engineering, 108–111
show ip traffic-engineering configuration, 111–112
show ip traffic-engineering routes, 113

commands, Continued
show tag-switching atm-tdp bindings, 114–116
show tag-switching atm-tdp capability, 116–117
show tag-switching atm-tdp summary, 118–120
show tag-switching forwarding-table, 120–122
show tag-switching tdp bindings, 125–127
show tag-switching tdp discovery, 128
show tag-switching tdp neighbors, 129–131
show tag-switching tdp parameters, 131–133
show tag-switching tsp-tunnels, 133–134
router configuration
traffic-engineering filter, 151
traffic-engineering route, 152–153
set configserver, 263
set local, 261
shortcut-frame-count, 355
shortcut-frame-count (MPC), 376
shortcut-frame-time, 355
shortcut-frame-time (MPC), 377
show interface stats, 189, 195
show ip cache, 16, 32–33
show ip cache flow, 34–37
show ip mcache, 189, 196–197
show ip mds forwarding, 189, 198–199
show ip mds interface, 189, 199
show ip mds stats, 189, 200–201
show ip mds summary, 189, 201–203
show ip pim interface, 189
show ip pim interface count, 203

commands, Continued
show ip route flow, 83
show ip traffic-engineering configuration, 105
show lane, 327–330
show lane bus, 276, 331–332
show lane client, 277, 333–335
show lane config, 277, 336–338
show lane database, 277, 338–339
show lane default-atm-addresses, 262, 277, 341
show lane le-arp, 278, 341–342
show lane name, 276
show lane server, 278, 343–345
show mls rp, 182–183
show mls rp vtp-domain, 183
show mpoa client, 355, 378–379
show mpoa client cache, 355, 379–380
show mpoa client statistics, 355, 381
show mpoa default-atm-address, 355
show mpoa default-atm-addresses, 361, 382–383
show mpoa server, 362, 384–385
show mpoa server cache, 385
show mpoa server statistics, 387–388
show tag-switching atm-tdp bindings, 100
show tag-switching forwarding-table, 101
show tag-switching interfaces, 102
show tag-switching tdp bindings, 100
show tag-switching tdp neighbors, 103
show tag-switching tsp tunnels, 104
commands, Continued
standby authentication, 222
standby ip, 221
standby preempt, 221
standby priority, 221
standby timers, 221
standby track, 222
syntax example, xix
tag-switching advertise-tags, 94
tr-isl, 22
vines metric, 218
vines routing, 218
xns network, 229
xns routing, 229
communications between VLANs, 209–210
ATM LANE protocol, 211
IEEE 802.10 protocol, 211
ISL, 210
compatibility, CEF, 46
compression, switching, 9
configuration
CEF
load balancing, 50
network accounting, 52
per destination load balancing, 51
per packet load balancing, 51
databases, LANE, 313
configuration mode
atm-address command, 355
mpoa client config name command, 355
MPS
holding-time command, 368

configuration mode, Continued
keepalive-time command, 368
network-id command, 375
shortcut-frame-count command, 376
shortcut-frame-time command, 377
See also MPS configuration mode
shortcut-frame-count command, 355
shortcut-frame-time command, 355
configuration servers, LANE, 246, 268
ATM
addresses, 262, 310
automatic addressing, 303
backups, 280
BUS redundancy, 273
database, 264, 338
redundant, 273
server associations, 312
viewing data, 336
configuring, 152
AppleTalk
cable ranges, 217
routing over ISL, 216
zones, 217
downstream unicast tag allocation, 145
emulated LANs, 279
IP multicast fast switching, 193
LANE, 259–260, 278, 283
ATM address prefixes, 282
ATM switch prefix, 261
BUS, 270
clients, 269–271
command reference, 295
default address display, 262
configuring, Continued
ELAN IDs, 322
fault tolerance, 280
ILMI PVCs, 262
implementation issues, 273–274
restricted memberships, 284–286
servers, 269
signaling PVCs, 261
source-route bridging, 287–288
unrestricted memberships, 281
MDS, 187–193
MLS
extended access lists, 176
routers, 169–170
standard access lists, 175
without access lists, 173
MPCs, 351–357
MPOA, 356, 362
clients, 353
ELAN IDs, 354
MPS, 351, 360–363
ELAN IDs, 360
variables, 361
NDE, 172–173
NetFlow switching, 81–84
routers, LANE, 264
routing, VLANs, 241
saving changes, xxvi
switching paths, 11
Tag Switching, 91, 98
incremental, 99
peer device links, 137
subset of destinations, 99

configuring, Continued
TDP holdtime, 148
traffic engineering, 104, 107
TR-LANE, source-route bridging, 289–290
TSP tunnels, 103
VIP distributed switching, 227
control ATM addresses, overriding for MPOA, 365
controlling
NetFlow cache entries, 24
TC-ATM, tag binding requests, 136
TDP tag distribution, 135–136
copy system command, 261
counters, CEF, clearing, 57
custom queuing, 8

D

database configuration mode
client-atm-address command, 299–300
default-name command, 302
name elan-id command, 354
name elan-id LANE command, 322
name local-seg-id command, 324
name preempt command, 276
name preempt LANE command, 323
name server-atm-address command, 326
databases
ATM TDP, entries, displaying, 114–115
LANE
configuration, 313
databases, Continued
configuration server, 264
restricted-membership emulated LANs, 267
unrestricted emulated LANs, 265
dCEF (distributed CEF mode), 45
enabling, 50
load balancing, 51–52
DECnet
encapsulation, 219
fast switching, disabling, 14
over ISL encapsulation, 218
routing
over ISL, 218–219, 231
subinterface, 219
decnet cost command, 219
decnet routing command, 219
default emulated LAN names, 302
default-name command, 265, 302
defaults
commands, xxvi
emulated LAN names, LANE clients, 302
LANE
addresses, 262
component ATM, 340
MPC ATM addresses, 382
defining
MPCs, 371
MPS, 373
designing VLANs, 212
devices, TSP tunneling, 148

directed broadcast packets (IPX), fast switching, 13
disabling
fast switching, 13
AppleTalk, 14
Banyan VINES, 14
DECnet, 14
IPX, 15
ISO CLNS, 15
XNS, 15
MLS, 170
discard adjacencies, 43
discovery
adjacency tables, 43
TDP, status, displaying, 128
displaying
ATM tag bindings
summary information, 118–120
TDP database entries, 114–115
interfaces, 123–124
TDP
discovery status, 128
session status, 129–130
TFIB contents, 120–122
TIB contents, 125–127
traffic engineering statistics, 108–111
TSP tunnel statistics, 133–134
See also viewing
distributed CEF mode. *See* dCEF
distributed switching, 3, 6–7
CEF tunneling, 53
VIP, 83
domains
MPS, shortcuts, 360
VTP MLS, 172, 181
downstream unicast tag allocation, tag space configuration, 145
DRiP database, enabling, 222
drop adjacencies, 43

E

egress cache
MPCs
clearing, 366
viewing entries, 379
MPOA servers, viewing, 385
MPS, clearing, 367
ELAN IDs
configuring (LANE), 322
MPOA, 354
MPS configuration, 360
emulated LANs
clients, 271
configuring, 279
LANE
clients, 248
preempt, 323
enabler packets, MLS, 163
encapsulation
Banyan VINES, 218
DECnet, 219
defining, 217, 221–225
HSRP, 221

encapsulation, Continued
IEEE 802.10, 21, 217
IPX, 224–226
ISL, 217-218, 221–225, 228
Novell Ethernet 802.2, 225
SAP, 225
SDE, 217
TRISL, 222
VIP distributed switching, 228
VLANs, 217, 242
XNS, 229
encapsulation isl command, 20, 217–221, 224, 228–229
encapsulation sde command, 21, 217, 242
encapsulation sde | isl command, 217
encapsulation smds command, 13
encapsulation tr-isl command, 22
encapsulation tr-isl trbrf-vlan bridge-num command, 222, 226
encryption, switching, 9
ESI field (end-system identifier), LANE ATM addresses, 257
ESI templates, LANE, 258
Ethernet
configuring LANE, 279–280
routing to Token Ring, 292
EXEC commands
clear cef linecard, 57
clear cef linecard command, 57
show adjacency, 64–66
show cef, 66–67
EXEC commands, Continued
show cef interface, 68–69
show cef linecard, 70–71
show ip cef, 72–74
show tag-switching interfaces, 123–124
EXEC mode
clear atm vc command, 295
clear ip mds forwarding command, 191
clear ip pim interface count command, 192
clear lane le-arp command, 296–297
clear lane server command, 297–299
clear mpoa client cache command, 355, 366
clear mpoa server cache command, 362, 367
mpoa server name trigger ip-address command, 362, 374
show interface stats command, 195
show ip mcache command, 196
show ip mds forwarding command, 198–199
show ip mds interface command, 199
show ip mds stats command, 200
show ip mds summary command, 201
show ip pim interface count command, 203
show lane bus command, 276, 331–332
show lane client command, 277, 333–335
show lane command, 327–330
show lane config command, 277, 336–338
show lane database command, 277, 338–339
show lane default-atm-addresses command, 277, 341
show lane le-arp command, 278, 341–342
show lane name command, 276

EXEC mode, Continued
show lane server command, 278, 343–345
show mls rp command, 182
show mls rp vtp-domain command, 183
show mpoa client cache command, 355, 379
show mpoa client command, 355, 378
show mpoa client statistics command, 355, 381
show mpoa default-atm-address command, 355
show mpoa default-atm-addresses command, 361, 382
show mpoa server cache command, 362, 385
show mpoa server command, 362, 384
show mpoa server statistics command, 387
export datagrams, NetFlow data, 78
exporting NetFlow cache entries, 26, 84
extended access lists, MLS, 164, 176
external routers, MLS guidelines, 166

F

fast switching, 3, 6
AppleTalk, 11, 14
Banyan VINES, 14
configuring, 11
DECnet, 14
disabling, 13
Fast Ethernet switching, 5
IP, 11
routing table cache, 32
same IP interface, 12
fast switching, Continued
IPX, 13–15
ISO CLNS, 15
SMDS, 13
troubleshooting, 13
XNS, 15
fault tolerance, LANE, 272, 280
FDDI switching, 5
FIB (Forwarding Information Base), 42
FIFO (first-in, first-out) queuing, 8
filtering
switching, 9
traffic engineering, 104
statistics, displaying, 111–113
TSP tunnels, 89
fixed ATM addresses, LANE, 315
flapping, emulated LANs, 275
flow
MLS, 161
network, 78
forwarding. *See* routing
frames
coloring, VLANs, 209
SDE, 241
tagging
ISL, 215
VLANs, 209
functions of tags in Tag Switching, 87

G

glean adjacencies, 43
global configuration command mode, xxv
global configuration commands
atm address command, 261
atm lecs-address-default command, 263
clear adjacency, 56
default-name command, 265
interface atm command, 262
ip cef, 49, 58
ip cef accounting, 60
ip cef traffic-statistics, 61
ip multicast-routing command, 194
lane client command, 270
lane database command, 264, 266, 313
lane server-bus command, 270
mls rp ip command, 177
mls rp nde-address command, 179
mpoa client config name command, 354, 371
mpoa server config name command, 373
name local-seg-id command, 265–266
name server-atm-address command, 265–266
router traffic-engineering, 107
show lane default-atm-addresses command, 262
tag-switching advertise-tags, 135–136
tag-switching atm allocation-mode, 136
tag-switching atm maxhops, 139
tag-switching atm vc-merge, 140
tag-switching ip, 142
global configuration commands, Continued
tag-switching tag-range downstream, 145
tag-switching tdp discovery, 146
tag-switching tdp holdtime, 148
tag-switching tsp-tunnels, 149
GSR (Gigabit Switched Router)
CEF compatibility, 46
MDS configuration, 187, 194

H

hardware
LANE support, 256
MLS requirements, 166
headend routers, traffic engineering tunnels, 89
hello messages, TDP discovery intervals, 146
help system, displaying command syntax, xx–xxiii
holding-time command, 361
holding time command (MPS), 368
holding times, MPS-p7 variable (MPS), 368
hop counts, 139
hops, Tag Switching tunnels, 154
HSRP (Hot Standby Router Protocol), 219
configuration over ISLs, 221, 232
encapsulation, 221
group attributes, customizing, 221
routing
IP addresses, 221
over ISL, 219, 232
standby group attributes, 221

IDs (identifiers), VLANs, 209
IEEE 802.10, 241
AppleTalk routing, 216, 241–242
encapsulation, 21
VLANs
communications, 211
encapsulation, 217
ILMI PVC, LANE, 262
implementing MLS, 162
incremental Tag Switching, 92–93, 99
ingress cache
MPCs
clearing, 366
viewing entries, 379
MPOA servers, viewing, 385
MPS, clearing, 367
interface atm command, 262, 354, 361
interface command, 13, 217, 221–229
interface configuration command mode, xxv
interface configuration commands
atm lecs-address command, 263
atm pvc ilmi command, 262
atm pvc qsaal command, 262
atm-address command, 365
interface atm command, 354
interface mul command, 354
ip load-sharing, 62
ip mroute-cache command, 193
ip route-cache cef, 63–64
lane auto-config-atm-address command, 303
lane bus-atm-address command, 305–306
interface configuration commands, Continued
lane client command, 307
lane client mpoa client name command, 354, 369
lane client mpoa server name command, 370
lane client-atm-address command, 308
lane config-atm-address command, 310–311
lane fixed-config-atm-address command, 315–316
lane global-lecs-address command, 317
lane le-arp command, 318
lane server-atm-address command, 319
lane server-bus command, 321, 360
lane server-bus ethernet command, 354
mls ip vlan-id command, 180
mls rp management-interface command, 178
mls rp vtp-domain command, 181
mpoa client name command, 354, 372
mpoa server name command, 374
name elan-id command, 360
tag-switching atm control-vc, 137
tag-switching atm vpi, 141
tag-switching ip, 143
tag-switching mtu, 144
tag-switching tsp-tunnels, 150
tunnel mode tag-switching, 153
tunnel tsp-hop, 154
interface mul command, 354
interfaces
ATM
attaching MPCs, 372
attaching MPSs, 374

interfaces, Continued
LAN emulation, 245
LANE assignment rules, 259
IPv4 Tag Switching, 143
LANE, viewing data, 327
MDS, viewing status, 199
MLS
monitoring, 171
viewing for VTP domains, 183
MLSP, management, 178
MTUs, overriding, 144
NetFlow switching, 81
physical, attaching MPCs/MPSs, 351
statistics display, 195
Tag Switching statistics, 123–124
TC-ATM, tag binding requests, 136
TSP tunneling, 150
viewing Tag Switching data, 102
VIP, distributed switching, 83
Inter-Switch Link protocol. *See* ISL
invalidation
IP route cache, 16, 23
IPX route cache, 17
IP
accounting, MLS, 167
addresses
defining, 221
mapping Level 3 to Level2, 5
fast switching, 11
routing table cache, 32
same IP interface, 12
IP, Continued
multicast fast switching, 193
displaying cache contents, 196
multicast routing, 194
route cache, controlling invalidation, 16, 23
router commands, MLS restrictions, 165
routing
between TrBRF VLANs, 233
between TRISL and Ethernet ISL VLANs, 235
NetFlow switching, 30
switching caches, 27
routing tables, viewing contents, 16
subnets, defining, 221
switching, CEF, 41–45
ip address command, 221
IP addresses
HSRP routing, 221
TRISL, primary, 223
ip cache-invalidate-delay command, 16, 23
ip cef accounting command, 52, 60
ip cef command, 49, 58
ip cef traffic-statistics command, 61
ip flow-cache entries command, 24, 82
ip flow-export command, 26, 82–84
ip flow-export version 5 command, 82
ip load-sharing command, 62
ip load-sharing per-packet command, 52
ip mroute-cache command, 193
ip mroute-cache distributed command, 188
ip multicast-routing command, 194
ip multicast-routing distributed command, 188

ip route-cache cef command, 50, 63–64
ip route-cache command, 12–13, 27
ip route-cache distributed command, 83, 188, 228
ip route-cache flow command, 30, 82–83
ip route-cache same-interface command, 12
IP routing
  NetFlow switching configuration, 82
  over TRISL, 222
  VIP distributed switching, 228
ip routing command, 222, 228
IPv4 packets, Tag Switching, 142
IPX, 224
  configuration
    encapsulation formats, 223
    example, 235
  encapsulation, 224–226
    Ethernet V2, 223
    IEEE 802.2, 223
    novell-ether, 223
    SAP, 223
    SNAP, 223
  fast switching, 13–15
  packets, padding odd-length, 18
  route cache
    invalidation options, 17
    size options, 17
  routing
    over ISL, 223–235
    over TRISL, 225
    subinterface, 226
  SAP, 225
IPX, Continued
  virtual LANs, TRISL, configuring NetWare, 225–226
ipx broadcast-fast-switching command, 13
ipx network encapsulation command, 224–226
ipx pad-process-switched-packets command, 18
ipx route-cache command, 13
ipx route-cache inactivity-timeout command, 17
ipx route-cache max-size command, 17
ipx routing command, 224–225
ISL protocol (Inter-Switch Link), 20, 210, 215
  AppleTalk routing, 216, 230–231
  Banyan VINES
    encapsulation, 217
    routing, 231
  configuring on subinterfaces, 228
  DECnet
    encapsulation, 218
    routing, 218, 231
  enabling, 20
  encapsulation
    configuration tasks, 216
    VLANs, 215–217
  frame tagging, 215
  HSRP
    routing, 219–221, 232
    VLAN encapsulation, 221
  IP routing between TrBRF VLANs, 233
  IPX
    encapsulations, 223
    routing, 223, 235
  overview, 215

ISL protocol, Continued
VIP distributed switching, 226, 238–239
VLAN
communications, 210
identifier, 215
traffic, distributed on VIP card, 226
XNS encapsulation/ routing, 228
ISO CLNS fast switching, 15

J-K

keepalive time values, MPS-p1 variable, 368
keepalive-time command, 361
keepalive-time command (MPS), 368
key features of MLS, 160

L

LAN MAC addresses, LANE resolution, 249
LANE (LAN Emulation), 245, 253
addressing, 256–257
resolution, 249
ATM addresses
displaying default, 340
templates, 258
automatic server addresses, 303
backup configuration servers, 280
BUS, 211, 246, 254
ATM addresses, 305
configuring, 270
enabling, 321
packet flooding, 249
viewing data, 331
LANE, Continued
clients, 246, 254, 271, 302
adding address to database, 299
ATM addresses, 308
configuring, 269
joining emulated LANs, 248
LE ARP table, 249, 341
MAC addresses, 257
MPOA, 272
multicast traffic, 249
starting, 307
viewing data, 333
components, interface assignment rules, 259
configuration server
ATM addresses, 310
BUS redundancy, 273
viewing data, 336
viewing database, 338
configuration servers, 246, 254, 268
ATM addresses, 262
database, 264
redundant, 273
configuration table, server associations, 312
configuring, 259–260, 283
ATM address prefixes, 282
ATM switch prefix, 261
command reference, 295
default address display, 262
ELAN IDs, 322
examples, 278
fault tolerance, 280
ILMI PVCs, 262
implementation issues, 273–274
restricted memberships, 284–286

LANE, Continued
routing between Token Ring and Ethernet emulated LANs, 291–292
signaling PVCs, 261
source-route bridging, 287–288
unrestricted memberships, 281
database configuration mode
name elan-id command, 354
name preempt command, 276
emulated LAN preempt, 323
ESI templates, 258
fault tolerance, 272
fixed ATM addresses, 315
hardware supported, 256
LE ARP table
adding static entries, 318
clearing, 296
LECS, 211
addresses, 317
local segment IDs, 324
monitoring, 276
MPOA interaction, 350
multiple emulated LAN example, 251
named configuration databases, 313
network features supported, 255
planning worksheets, 260
prefix templates, 258
restricted-membership emulated LANs, 267
ring numbers, 324
servers, 246, 254
ATM addresses, 319, 326
configuring, 269
dropping clients, 297
LANE, Continued
enabling, 321
viewing data, 343
simple server redundancy, 254, 272
single emulated LAN example, 250
SSRP, reducing network flap, 275
SVCs, 247, 295
switches, 256
unrestricted emulated LAN databases, 265
VCCs, 247
viewing component or interface data, 327
lane auto-config-atm-address command, 303
lane bus-atm-address command, 305–306
lane client command, 270, 307
lane client mpoa client name command, 369
lane client mpoa server name command, 361, 370
lane client-atm-address command, 308
lane config auto-config-atm-address command, 269
lane config config-atm-address command, 269
lane config database command, 269
lane config fixed-config-atm-address command, 269
lane config-atm-address command, 310–311
lane database command, 264–266, 313
lane fixed-config-atm-address command, 315–316
lane global-lecs-address command, 317
lane le-arp command, 318
lane server-atm-address command, 319

lane server-bus command, 270, 321, 360
lane server-bus ethernet command, 354
LANs
  emulated, configuring, 279
  segmentation, VLAN design, 208
Layer 2, mapping Layer 3, 5
Layer 3
  IP addresses, mapping to Layer 2, 5
  switching. *See* MLS
LE ARP table (LANE ARP), LANE clients, 249
  adding entries, 318
  clearing, 296
  displaying, 341
LECSs (LAN Emulation Configuration Server), 211, 254, 317
  binding
    to named MPC, 369
    to named MPS, 370
  MPC/MPS relationship, 350
LightStream ATM switch, LANE example, 250
limiting tag distribution, Tag Switching, 94
line cards
  clearing, 55–56
    packet counts, 192
  MDS
    maintenance, 188
    monitoring, 189
    statistics, 200
    viewing MFIB table/forwarding data, 198
  MFIB table, clearing routes, 191
local segment IDs (LANE), 324

M

MAC addresses, LANE clients, 257
maintenance of MDS, 188
management interface, MLSP, 178
managing VLANs, 209
MDS (Multicast Distributed Switching), 187
  configuring, 187–193
  GSR, 194
  interface, viewing status, 199
  line card statistics, 200
  MFIB table, summary display, 201
  monitoring, 188–189
  switching, statistics display, 200, 203
  viewing line card forwarding data, 198
MFIB table
  clearing routes, 191
  MDS summary display, 201
  viewing, 198
MLS (Multilayer Switching), 169
  access lists, 167
  cache, 161
  candidate packets, 162
  CAR affects, 168
  configuring
    extended access lists, 176
    routers, 169–170
    standard access lists, 175
    without access lists, 173
  disabling, 170
  enabler packets, 163
  enabling, 177

MLS, Continued
extended access lists, 164
external router guidelines, 166
flows, 161
implementing, 162
interfaces, viewing for VTP domains, 183
IP
accounting, 167
router command restrictions, 165
key features, 160
monitoring, 170
specific interfaces, 171
VTP domains, 172
MTU sizes, 168
NAT affects, 168
NDE addresses, 179
overview, 159
policy route-maps, 168
standard access lists, 164
system requirements, 166
TCP intercept feature, 168
viewing data, 182
VLAN IDs, 180
VTP domains, 181
mls ip vlan-id command, 180
mls rp ip command, 169–170, 177
mls rp management-interface command, 170, 178
mls rp nde-address command, 173, 179
mls rp vip-domain command, 170
mls rp vlan-id command, 170
mls rp vtp-domain command, 181
MLSP (Multilayer Switching Protocol), 160
enabling, 177
management interface, 178
MLS-RP (Multilayer Switching-Route Processor), 160
MLS-SE (Multilayer Switching-Switching Engine), 160
monitoring
LANE, 276
MDS, 188–189
MLS, 170
specific interfaces, 171
VTP domains, 172
MPCs, 355
MPS, 361
MPCs (MPOA clients), 347, 353
ATM
address defaults, 382
attaching to interfaces, 372
overriding control address, 365
binding LECs, 369
clearing ingress/egress caches, 366
configuration mode commands, 355
configuring, 351–357
ingress/egress cache entries, 379
LEC relationship, 350
monitoring, 355
MPOA message flow, 348
naming, 371
physical interfaces, 351
shortcut-frame counts, 376
shortcut-setup frame times, 377

MPCs, Continued
statistics display, 381
summary data, 378
MPOA (Multiprotocol over ATM), 347, 365
ATM network connections, 351
configuring, 356, 362
clients, 353
ELAN IDs, 354
LANE
clients, 272
interactions, 350
message flow between MPS and MPC, 348
NBMA network functionality, 348
overriding control ATM address, 365
platform support, 348
servers, viewing ingress/egress cache, 385
traffic flow, 349
triggers, 374
mpoa client config name command, 354–355, 371
mpoa client name command, 354, 372
mpoa server config name command, 361, 373
mpoa server name command, 361, 374
mpoa server name trigger ip-address command, 362, 374
MPS (MPOA server), 347
attaching to ATM interfaces, 374
binding LECs, 370
clearing ingress/egress caches, 367
configuration mode
atm-address command, 361
holding-time command, 361
MPS, Continued
keepalive-time command, 361, 368
mpoa server config name command, 361
network-id command, 361
configuring, 351, 362–363
ELAN IDs, 360
variables, 361
holding-time command, 368
LEC relationship, 350
monitoring, 361
MPOA
message flow, 348
triggers, 374
MPS-p1 variable, keepalive time values, 368
MPS-p7 variable, holding time, 368
naming, 373
network IDs, 375
NHRP routing interaction, 359
overview of functionality, 359
physical interfaces, 351
shortcut domains, 360
statistics display, 387
viewing data, 384
MPS-p1 variable, keepalive time values, 368
MPS-p7 variable, holding time, 368
MTUs (Maximum Transmission Units)
MLS sizes, 168
overriding, 144
multicast fast switching
configuring, 193
cache, displaying contents, 196
multicast routing, 194

multicast traffic, LANE clients, 249
multiple emulated LANs, LANE example, 251

N

name elan-id command, 354, 360
name elan-id LANE command, 322
name local-seg-id command, 265–266, 324
name preempt command, 276
name preempt LANE command, 323
name server-atm-address, 326
name server-atm-address command, 265–266
name server-atm-address restricted command, 267
naming
  MPCs, 371
  MPSs, 373
NAT (Network Address Translation), 168
NBMA (nonbroadcast multiaccess) networks, 347–348
NDE (NetFlow Data Export), 159
  addresses
    MLS, 179
    specification, 173
  configuring, 172
NetFlow
  cache, 78
    controlling number of entries, 24, 82
    exporting entry data, 26
  data formats, 78–80
  flow data
    UDP datagrams, 78
NetFlow, Continued
    version 1 flow record format, 79
    version 1 header format, 79
    version 5 flow record format, 80
    version 5 header format, 80
  switching, 77, 81–82
    configuring, 84
    exporting cache entries, 84
    statistics options, 83
    traffic statistics, 77
    VIP controllers, 83
  switching, 7
    IP routing, 30
    statistics display, 19, 34
NetWare IPX routing. *See* IPX routing
network IDs, MPS, 375
network masks, TRISL, 223
network-id command, 361
network-id command (MPS), 375
networks
  ATM
    LAN emulation, 245
    MPOA connections, 351
  configuring
    accounting configuration, CEF, 52
    MPCs, 354
  flow, 78
  LANE
    flapping, 275
  MPOA, 347
  NBMA, 347–348
  Tag Switching
    incremental, 92–93

networks, Continued
limiting tag distribution, 94
subset of destinations, 93
traffic engineered paths, 95
VLANs, 209
NFFC (NetFlow Feature Card), 159
NHRP (Next Hop Routing Protocol), MPS routing interaction, 359
no form of commands, xxvi
no ip load-sharing per-destination command, 51
no ip route-cache command, 12
Novell Ethernet 802.2 encapsulation formats, 225
null adjacencies, 43

O

odd-length IPX packets, padding, 18
online support, xix
organization of Cisco IOS Switching Services document, xv
overriding MTUs, 144
overview of Cisco IOS 12.0 Switching Services document, xv

P

packets
candidate, MLS, 162
counts, line cards, clearing, 192
enabler, MLS, 163
IPv4 Tag Switching, 142
IPX, padding odd-length, 18
statistics display, 195
parameters for TDP, displaying, 131, 133
paths, switching, 6
peer devices, Tag Switching, link configuration, 137
per destination load balancing, CEF configuration, 51
per packet load balancing, CEF configuration, 51
performance factors for switching, 8
physical interfaces, MPC/MPS attachments, 351
planning worksheets, LANE, 260
platform support, MPOA, 348
policy route-maps, MLS, 168
prefix templates, LANE, 258
primary IP addresses, TRISL, 223
priority queuing, 8
privileged EXEC command mode, xxv
privileged EXEC commands
show ip traffic-engineering, 108–111
show ip traffic-engineering configuration, 111–112
show ip traffic-engineering routes, 113
show tag-switching atm-tdp bindings, 114, 116

privileged EXEC commands, Continued
show tag-switching atm-tdp capability, 116–117
show tag-switching atm-tdp summary, 118, 120
show tag-switching forwarding-table, 120–122
show tag-switching tdp bindings, 125–127
show tag-switching tdp discovery, 128
show tag-switching tdp neighbors, 129–131
show tag-switching tdp parameters, 131–133
show tag-switching tsp-tunnels, 133–134
process switching, 6
protocols
BGP, 78
HSRP, 219
IEEE 802.10, 21
ISL, 20, 210, 215
MLSP, 160, 177
SSRP, 272
TDP, 103
TRISL, 22
UDP, 79
VLAN routing, 212
punt adjacencies, 43
PVCs, LANE configuration, 261

Q-R

queuing, switching, 8
random early detection, switching, 9
redundancy
between multiple routers, 220
HSRP, 220
redundant LANE BUSes, 273
redundant LANE configuration servers, 273
reference texts for Cisco IOS 12.0, xvi–xvii
book conventions, xviii
command syntax, xix
resolution, adjacency tables, 43
restricted LANE memberships, 284–286
restricted-membership emulated LANs, LANE, 267
restricting Tag Switching, hop counts, 139
RIF routing between TRISL VLAN and Token Ring interface, 237
ring numbers, LANE, 324
ROM monitor command mode, xxv
route cache
IP, controlling invalidation, 16
IPX, 17
route caching, 3
route processor cards, CEF, 57–58
router commands, MLS restrictions, 165
router configuration commands
traffic-engineering filter, 151
traffic-engineering route, 152–153
router traffic-engineering command, 107

routers
configuring
LANE, 264, 279–283, 295
LANE source-route bridging, 287–288
MLS, 169–170, 173
restricted LANE memberships, 285–286
Tag Switching, 98
TR-LANE source-route bridging, 289–290
external, MLS guidelines, 166
headend, traffic engineering, 89
LANE
fault tolerance, 280
support, 256
Tag Switching, 88
routes
MFIB table, clearing, 191
traffic engineering, 104
routing, 5
AppleTalk, 241
cable lengths, 217
IEEE 802.10 interfaces, 216, 242
over ISL, 230–231
subinterfaces, 242
VLANs, 243
zones, 217, 242
Banyan VINES over ISL, 217, 231
DECnet
over ISL, 218, 231
subinterface, 219
HSRP, 221
IP addresses, 221
over ISL, 219, 232
IP
between TrBRF VLANs, 233
between TRISL and Ethernet ISL VLANs, 235
NetFlow switching, 30
over TRISL, 222
switching caches, 27
IPX
over ISL, 223, 235
over TRISL, 225
subinterfaces, 224–226
LANE, between Token Ring and Ethernet emulated LANs, 291–292
MPS, NHRP interaction, 359
process overview, 4–5
RIF, between TRISL VLAN and Token Ring interface, 237
subinterfaces, 224
Tag Switching, 88
VLANs, 207, 241
ISL encapsulation, 215
protocols, 212
XNS
over ISL, 228
subinterface, 229
routing metric, Banyan VINES, 218
routing platforms, switching paths, 7
routing tables
IP
fast switching, 32
viewing contents, 16
RSM (Route Switch Module), 159

RSP (Route/Switch Processor) route caching, 3
MDS, 193
multicast fast switching, 193

S

SAIDs (Security Association Identifiers), 241
saving configuration changes, xxvi
SDE (Secure Data Exchange) frame type, 241
security, VLANs, 209
segmentation of LANs, VLAN design, 208
servers
LANE, 246, 254
ATM addresses, 319, 326
clearing clients, 297
configuration, 268–269
enabling, 321
viewing data, 343
MPOA, viewing ingress/egress cache, 385
MPS, 347
sessions, TDP
holdtime, configuring, 148
status, displaying, 129–130
set configserver command, 263
set local command, 261
shortcut domains, MPS, 360
shortcut-frame-count command, 355
shortcut-frame-count command (MPC), 376
shortcut-frame counts, MPCs, 376
shortcut-frame-time command, 355
shortcut-frame-time command (MPC), 377
shortcut-setup frame times, MPCs, 377
show, 108, 123
show adjacency command, 64–66
show cef command, 66–67
show cef interface command, 68–69
show cef linecard command, 70–71
show interface stats command, 189, 195
show ip cache command, 16, 32–33
show ip cache flow command, 34–37
show ip cef command, 72–74
show ip mcache command, 189, 196–197
show ip mds forwarding command, 189, 198–199
show ip mds interface command, 189, 199
show ip mds stats command, 189, 200–201
show ip mds summary command, 189, 201–203
show ip pim interface command, 189
show ip pim interface count command, 203
show ip route flow command, 83
show ip route profile command, 53
show ip traffic-engineering command, 108–111
show ip traffic-engineering configuration command, 105, 111–112
show ip traffic-engineering routes command, 113
show lane bus command, 276, 331–332
show lane client command, 277, 333–335
show lane command, 327–330
show lane config command, 277, 336–338
show lane database command, 277, 338–339
show lane default-atm-addresses command, 262, 277, 341
show lane le-arp command, 278, 341–342

show lane name command, 276
show lane server command, 278, 343–345
show mls rp command, 182–183
show mls rp vtp-domain command, 183
show mpoa client cache command, 355, 379–380
show mpoa client command, 355, 378–379
show mpoa client statistics command, 355, 381
show mpoa default-atm-address command, 355
show mpoa default-atm-addresses command, 361, 382–383
show mpoa server cache command, 385
show mpoa server command, 362, 384–385
show mpoa server statistics command, 387–388
show tag-switching atm-tdp bindings command, 100, 114–116
show tag-switching atm-tdp capability command, 116–117
show tag-switching atm-tdp summary command, 118–120
show tag-switching forwarding-table command, 101, 120–122
show tag-switching interfaces command, 102, 123–124
show tag-switching tdp bindings command, 100, 125–127
show tag-switching tdp discovery command, 128
show tag-switching tdp neighbors command, 103, 129–131
show tag-switching tdp parameters command, 131–133
show tag-switching tsp tunnels command, 104
show tag-switching tsp-tunnels command, 133–134
signaling PVC, LANE, 261
simple server redundancy, LANE, 254, 272
single emulated LANs, LANE example, 250
size options, IPX route cache, 17
SMDS, fast switching, 13
software, MLS requirements, 166
source-route bridging
    LANE, 287–288
    TR-LANE, 289–290
SSRP protocol, reducing network flap, 272, 275
standard access lists, MLS, 164
standby authentication command, 222
standby group attributes, HSRP, 221
standby ip command, 221
standby preempt command, 221
standby priority command, 221
standby timers command, 221
standby track command, 222
starting LANE clients, 307
statistics
    interfaces, 195
    MPCs, 381
    MPS, 387
    NetFlow switching, 77, 83
subinterface configuration command mode, xxv
subinterface routing, DECnet, 219
subinterfaces
    AppleTalk routing, 242
    IPX routing, 224–226

subinterfaces, Continued
Tag Switching
enabling, 141
peer device links, 137
VIP distributed switching, encapsulation, 228
XNS routing, 229
subnets, IP, 221
subset destination Tag Switching, 93, 99
summary data, MPCs, 378
SVCs (switched virtual circuits), LANE, 247, 295
switching, 3
ATM, LANE address prefix, 261
CEF (Cisco Express Forwarding), 41
adjacency tables, 42–43
central CEF mode, 44
dCEF, 45
enabling, 49–50
FIB, 42
load balancing, configuration, 50
network accounting, configuration, 52
per destination load balancing, 51
per packet load balancing, 51
route processor cards, 57–58
compression, 9
distributed, 3
distributed switching, 6–7
distributed tunnel switching, 53
Fast Ethernet, 5
fast switching, 3, 6
FDDI, 5
switching, Continued
ISL VLAN traffic, 226
LANE, 256
configuration server ATM addresses, 262
MDS, viewing statistics, 200, 203
NetFlow, 7, 77, 81–82
clearing statistics, 19
configuring, 84
exporting cache entries, 84
statistics options, 83
traffic statistics, 77
performance factors, 8
process switching, 6
queuing, 8
Tag Switching, 87
VIP
controllers, 83
distributed, 226–228
VLANs, 209
switching caches, IP routing, 27
switching paths, 7, 11
switching statistics, NetFlow, 34
syntax of commands, displaying help examples, xxi–xxiii
system requirements, MLS, 166

T

tag bindings
  ATM summary information, 118–120
  TC-ATM requests, 136
Tag Switching, 87
  binding tags, 88
  configuring, 91, 99
  displaying Tag Information Base, 100
  functions of tags, 87
  hop counts, limiting, 139
  incremental, 92–93
  IPv4 packets, 142
  limiting tag distribution, 94
  peer devices, links, configuring, 137
  restricting, 139
  routing, 88
  statistics, displaying, 123–124
  subinterfaces, enabling, 141
  subset of destinations, 93
  tag bindings, 88
  TDP binding data, 100
  traffic engineering, 88
    paths, 95
  TSP tunnels, 103
    viewing data, 104
  tunnels, hops, 154
  viewing
    interface data, 102
    TDP neighbor data, 103
    TFIB, 101
Tag Switching statistics, 123–124
tags, 87
    binding, routing, switching, 88
    TDP distribution, controlling, 135–136
tag-switching advertise-tags command, 94, 135–136
tag-switching atm allocation-mode command, 136
tag-switching atm control-vc command, 137
tag-switching atm maxhops command, 139
tag-switching atm vc-merge command, 140
tag-switching atm vpi command, 141
tag-switching ip command, 142–143
tag-switching mtu command, 144
tag-switching tag-range downstream command, 145
tag-switching tdp discovery command, 146
tag-switching tdp holdtime command, 148
tag-switching tsp-tunnels command, 149–150
TAXIs (Transparent Asynchronous Transmitter/Receiver Interfaces), 256
TC-ATM interfaces, tag binding requests, 136
TCP (Transmission Control Protocol), intercept feature, MLS affects, 168
TDP (Tag Distribution Protocol), 103
    binding data, Tag Switching, 100
    discovery status, displaying, 128
    hello message interval, configuring, 146
    parameters, displaying, 131–133
    session status, displaying, 129–130

TDP, Continued
tags, distribution, 135–136
viewing neighbor data, 103
templates, LANE, 258
TFIB (Tag Forwarding Information Base)
contents, displaying, 120–122
viewing, 101
TIB (Tag Information Base), 100, 125–127
Token Ring
interfaces, RIF routing, 237
LANE. *See* TR-LANE
routing to Ethernet, 292
Token Ring ISL. *See* TRISL
traffic engineering, 95
across paths, 96
backup paths, 98
configuring routes and filters, 104
filters, 89, 111–113
routing process, 107
statistics
displaying, 108–111
filters, 111–113
Tag Switching, 88
tunnels, 89
viewing configuration data, 105
traffic flow, MPOA, 349
traffic statistics, NetFlow switching, 77
traffic-engineering filter command, 151
traffic-engineering route command, 152–153
translation, VLANs, 212
TrBRF VLANs, IP routing, 233
triggering IP addresses (MPOA), 374
TRISL (Token Ring ISL)
configuration
RIF, 233, 237
TrBRF VLANs, 233
TRISL and Ethernet VLANs, 235
TRISL VLAN and Token Ring, 237
enabling, 22, 222
encapsulation, 222
IP routing, 222
IPX
encapsulation, 226
routing, 225
network masks, 223
primary IP addresses, 223
VLANs, RIF routing to Token Ring interface, 237
TR-LANE, configuring source-route bridging, 289–290
troubleshooting fast switching, AppleTalk, 13–14
TSP (Tag Switched path) tunnels, 88, 149
configuring, 103
filters, 89
statistics, displaying, 133–134
viewing data, 104
TSRs (Tag Switching routers), 88
tunnel mode tag-switching command, 153
tunnel tsp-hop command, 154
tunnels
filters, routes, configuring, 152–153

tunnels, Continued
Tag Switching
enabling, 153
hops, defining, 154
TSP, 89
enabling, 149
statistics, displaying, 133–134

U

UDP (User Datagram Protocol), 78–79
unicast tag VCs, VC merge, 140
unrestricted emulated LANs, databases, 265
unrestricted LANE memberships, 281
user EXEC command mode, xxv

V

variables
MPCs, 355
MPSs, 361
VCCs (virtual channel connections), LANE, 247
VCs (Virtual Circuits), unicast tag, VC merge, 140
Versatile Interface Processor. *See* VIP
version 1 flow record format, NetFlow data, 79
version 1 header format, NetFlow data, 79
version 1flow records, 79
version 1headers, 79
version 5 flow record format, NetFlow data, 80
version 5 flow records, 80
version 5 header format, NetFlow data, 80
version 5 headers, 80
viewing
ATM TDP database entries, 114–115
ingress/egress cache entries, MPCs, 379
interface statistics, 195
IP routing table contents, 16
LANE BUS data, 331
LANE
client data, 333
component/interface data, 327
configuration server data, 336
configuration server database, 338
server data, 343
line cards, MDS forwarding data, 198
MDS
interface status, 199
switching statistics, 200, 203
MFIB table, 198
MLS data, 182
MPC data, 381, 384
MPS statistics, 387
multicast fast-switching cache contents, 196
NetFlow switching statistics, 34
Tag Information Base, 100
Tag Switching interface data, 102
TDP neighbor data, Tag Switching, 103
TFIB, 101
traffic engineering
configuration data, 105
statistics, 108–109, 111
TSP tunnel data, 104
vines metric command, 218

vines routing command, 218
VINES. *See* Banyan VINES
VIPs (Versatile Interface Processors)
distributed switching, 3, 83
between ISL VLANs, 227, 239
enabling, 228
IP routing, 228
ISL encapsulation, 228
ISL VLAN traffic, 226, 238
over ISL, 226, 238–239
scalability, 227, 238
VLAN configuration example, 239
NetFlow switching, 83
virtual LANs. *See* VLANs
VLANs (virtual LANs), 207
advantages/benefits, 210
AppleTalk
over ISL encapsulation, 216
routing, 241, 243
ATM LANE protocol, 211
Banyan VINES over ISL encapsulation, 217
broadcast control, 209
communications between, 209–210
DECnet over ISL encapsulation, 218
designing, 212
encapsulation, 217, 242
frame coloring, 209
frame tagging, 209
IDs (identifiers), 209
IEEE 802.10 protocol, 211
IP
routing, 222
over TRISL, 222
IPX routing, 225
ISL, 210
frame tagging, 215
LAN segmentation, 208
managing, 209
MLS IDs, 180
network performance, 209
packets traversing shared backbone, 215
routing, 207, 212, 241
between, 238
ISL encapsulation, 215
Novell IPX, 223
protocols, 212
routing protocols, 212
security, 209
switching, 209
translation, 212
TrBRF, IP routing, 233
TRISL, RIF routing to Token Ring interface, 237
VIP distributed switching, 239
XNS over ISL encapsulation, 228
VTP domains
MLS, 181
MLS monitoring, 172
viewing MLS interfaces, 183

W

weighted fair queuing, 8
worksheets for LANE planning, 260

X

XNS
    encapsulation, 229
    fast switching, 15
    over ISL encapsulation, 228
    routing
        over ISL, 228
        subinterface, 229
xns network command, 229
xns routing command, 229

Y-Z

zones, AppleTalk routing, 217, 242

Cisco IOS™ 12.0 Switching Services

- Discover techniques for optimizing performance and scalability in your network with Cisco Express Forwarding
- Identify the appropriate command syntax and usage in the integrated command reference
- Learn the Cisco IOS 12.0 switching paths for IP
- Find out how to configure routing between virtual LAN environments

Cisco IOS 12.0 Switching Services provides guidelines detailing available Cisco IOS switching alternatives—from fast switching and NetFlow switching to LAN Emulation. You will find general guidelines for configuring switching of various protocols, NetFlow accounting, routing between VLANs, and LAN Emulation, as well as corresponding configuration guidelines for the specific technology or set of features. This book also offers system optimization techniques, which can help increase performance and scalability in your network through Cisco Express Forwarding.

Cisco Systems, Inc., is the leading global supplier of internetworking solutions that include Cisco IOS 12.0 software, routers, LAN and ATM switches, dial-up access servers, and network management software. This book is the result of a collaboration of multiple authors who have developed the definitive guides to Cisco Internetwork Operating System software.

*This book is part of the **Cisco IOS 12.0 Reference Library**, which targets network practitioners and offers strategic configuration and implementation expertise, guidance, and initiatives.*

Category: Internet—Networking
Covers: Cisco IOS version 12.0
User Level: Accomplished—Expert

Cisco Systems
Cisco Press
www.ciscopress.com

$40.00 USA
$59.95 CAN

ISBN 1-57870-157-0

CISCO SYSTEMS, INC.
FORTINET, INC.
IPR2024-00540
Ex. 1010, p. 135 of 135