Router Products Configuration Guide

© Digital Equipment Corporation 1995.
All Rights Reserved.

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual for this device, may cause interference to radio communications. This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case users at their own expense will be required to take whatever measures may be required to correct the interference.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital or an authorized sublicensor.

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

The following are trademarks of Digital Equipment Corporation: DDCMP, DEC, DECnet, DECNIS, DECserver, DECsystem, DECwindows, Digital, DNA, OpenVMS, ULTRIX, VAX, VAXstation, VMS, VMScluster, and the DIGITAL logo.

Portions of this document is used with permission of Cisco Systems, Incorporated. Copyright © 1990 - 1995, Cisco Systems, Inc.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

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

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the tn3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac software in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited.

XRemote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the Massachusetts Institute of Technology. Copyright © 1987, Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute of Technology, Cambridge, Massachusetts. All rights reserved.

THESE MANUALS AND THE SOFTWARE OF THE ABOVE-LISTED SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. DIGITAL AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Notice of Restricted Rights:

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR §52.227-19 and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS §252.227-7013. The information in this manual is subject to change without notice.

Access Without Compromise, Catalyst, CD-PAC, CiscoFusion, CiscoWorks, HyperSwitch, Internetwork Operating System, IOS, Netscape, Point and Click Internetworking, SMARTnet *The Packet*, UniverCD, Workgroup Director, and Workgroup Stack are trademarks, and Cisco, Cisco Systems and the Cisco logo are registered trademarks of Cisco Systems, Inc. All other products or services mentioned in these documents are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

TABLE OF CONTENTS

About This Manual lix

Document Objectives lix

Audience lix

Document Organization lix

Document Conventions lx

Chapter 1

Router Product Overview 1-1

IOS Software Benefits 1-1

Reliable, Adaptive Routing 1-2

WAN Optimization 1-2

Management and Security 1-2

Scalability 1-3

Supported Network Protocols 1-3

Supported IP Routing Protocols 1-4

Supported Media 1-5

Supported Platforms 1-5

Configuring the Router 1-5

Using Cisco Configuration Builder 1-5

Using the Command Interpreter 1-5

Chapter 2

Understanding the User Interface 2-1

User Interface Task List 2-1

Access Each Command Mode 2-2

User EXEC Mode 2-3

Privileged EXEC Mode 2-4

Global Configuration Mode 2-6

Interface Configuration Mode 2-7

Subinterface Configuration Mode 2-9

Controller Configuration Mode 2-10

Hub Configuration Mode 2-11

Map-List Configuration Mode 2-11

Map-Class Configuration Mode 2-12

Line Configuration Mode 2-13

Router Configuration Mode 2-14

IPX-Router Configuration Mode 2-15

Route-Map Configuration Mode 2-16

ROM Monitor Mode 2-16

Get Context-Sensitive Help 2-17

Check Command Syntax 2-19

Use the Command History Features 2-20

Set the Command History Buffer Size 2-20

Recall Commands 2-21

Disable the Command History Feature 2-21

Use the Editing Features 2-21
Enable Enhanced Editing Mode 2-22
Move Around on the Command Line 2-22
Complete a Partial Command Name 2-23
Paste in Buffer Entries 2-23
Edit Command Lines that Wrap 2-23
Delete Entries 2-24
Scroll Down a Line or a Screen 2-24
Redisplay the Current Command Line 2-25
Transpose Mistyped Characters 2-25
Control Capitalization 2-25
Designate a Keystroke as a Command Entry 2-25
Disable Enhanced Editing Mode 2-25

End a Session 2-26

Chapter 3

Loading System Images, Microcode Images, and Configuration Files 3-1
Cisco's rsh and rcp Implementation 3-1

System Image, Microcode Image, and Configuration File Load Task List 3-2

Use the AutoInstall Procedure 3-3
AutoInstall Requirements 3-4
Using a DOS-based TFTP Server 3-5
How AutoInstall Works 3-5
Acquiring the New Router's IP Address 3-6
Resolving the IP Address to the Host Name 3-7
Downloading the New Router's Host Configuration File 3-8
Perform the AutoInstall Procedure 3-9
Modify the Existing Router's Configuration 3-9
Set Up the TFTP Server 3-12
Set Up the BOOTP or RARP Server 3-13
Connect the New Router to the Network 3-14

Enter Configuration Mode 3-15
Configure the Router from the Terminal 3-15
Configure the Router from NVRAM 3-16
Configure the Router from a File on a Remote Host 3-16
Copy a Configuration File to NVRAM 3-16

Modify the Configuration Register Boot Field 3-17

Specify the System Image the Router Loads upon Restart 3-18
Load from Flash Memory 3-18
Security Precautions 3-19
Flash Memory Configuration 3-19
Use the System Image Instead of Reloading 3-21
Load from a Network Server 3-21
Load from ROM 3-22
Use a Fault-Tolerant Boot Strategy 3-23

Specify the Configuration File the Router Loads upon Restart 3-24

Download the Network Configuration File 3-24
Download the Host Configuration File 3-25

Additional Cisco 3000 and Cisco 4000 Copying and Automatic Booting Features 3-26

Change the Buffer Size for Loading Configuration Files 3-26

Compress Configuration Files 3-27

Manually Load a System Image 3-27
Manually Boot from Flash 3-28
Manually Boot from a Network File 3-29
Manually Boot from ROM 3-29
Manually Boot Using MOP 3-29

Boot Systems That Have Dual-Bank Flash Memory 3-29
Copy a Boot Image on a Cisco 4500 3-30
Verify a Boot Image's Checksum on a Cisco 4500 3-30
Erase Boot Flash Memory on a Cisco 4500 3-30

Configure a Router as a TFTP Server 3-30

Configure a Router to Support Incoming rcp Requests and rsh Commands 3-31
Configure the Router to Accept rcp Requests from Remote Users 3-32
Configure the Router to Allow Remote Users to Execute Commands Using rsh 3-33
Turn Off DNS Lookups for rcp and rsh 3-34

Configure a Router as a RARP Server 3-34

Configure the Remote Username for rcp Requests 3-35

Specify SLIP Extended BOOTP Requests 3-36

Specify MOP Server Boot Requests 3-36

Copy System Images from a Network Server to Flash Memory Using TFTP 3-37
Copy Systems Images to Flash Memory Using MOP 3-40

Copy System Images from a Network Server to Flash Memory Using rcp 3-40

Additional Cisco 3000 and Cisco 4000 Flash Upgrade Features 3-42

Copy Bootstrap Images from a Network Server to Flash Memory Using rcp or TFTP 3-42

Use Flash Load Helper to Upgrade Software on Run-from-Flash Systems 3-44
Flash Load Helper Configuration Task List 3-45
Download a File Using Flash Load Helper 3-45
Monitor Flash Load Helper 3-48

Verify the Image in Flash Memory 3-48

Partition Flash Memory Using Dual Flash Bank 3-48
Understand Relocatable Images 3-49
Dual Flash Bank Configuration Task List 3-50
Partition Flash Memory 3-51
Download a File into a Flash Partition 3-51
Manually Boot from Flash 3-52
Configure the Router to Automatically Boot from Flash Memory 3-53
Configure a Flash Partition as a TFTP Server 3-53

Copy System Images from Flash Memory to a Network Server Using TFTP 3-53

Copy System Images from Flash Memory to a Network Server Using rcp 3-54

Copy a Configuration File from a Network Server to the Router Using rcp 3-56
Copy a Configuration File to NVRAM 3-56
Copy and Run the Configuration File 3-57

Copy a Configuration File from the Router to a Network Server Using TFTP 3-58

Copy a Configuration File from the Router to a Network Server Using rcp 3-58
Copy a Startup Configuration File to an rcp Server 3-59
Copy a Running Configuration File to a Network Server Using rcp 3-60

Display System Image and Configuration Information 3-60

Clear the Contents of NVRAM 3-61

Re-execute the Configuration Commands in NVRAM 3-61

Remotely Execute Commands Using rsh 3-61

Use Flash Memory as a TFTP Server 3-62
Prerequisites 3-62
Configure the Flash Server 3-63
Configure the Client Router 3-64

Load Microcode Images over the Network 3-65

Display Microcode Information 3-66

Chapter 4

Configuring Terminal Lines and Modem Support 4-1
Line Configuration Task List 4-1

Prepare to Configure Lines 4-2
Create Additional Virtual Terminal Lines 4-2
Eliminate Virtual Terminal Lines 4-3
Absolute versus Relative Line Numbers 4-3

Set Communication Parameters 4-3

Configure Automatic Baud Detection 4-4

Change the Default Privilege Level for Lines 4-4

Configure Flow Control for Communications 4-4

Define a Command String for Automatic Execution 4-5

Create Packet Dispatch Sequences 4-5

Specify the Transport Protocol for a Specific Line 4-5

Establish Terminal Session Limits 4-6

Set Up Modem Control on the Auxiliary Port 4-6
Configure Automatic Dialing 4-7
Close Modem Connections 4-8
Automatically Answer a Modem 4-9
Support a Dial-In Modem 4-10

Support Reverse Modem Connections and Prevent Incoming Calls 4-12
Support Dial-In and Dial-Out Modems 4-13
Configure a Line Timeout Interval 4-14
Configure Rotary Groups 4-15
Configure Automatic Line Disconnect 4-15
Configure High-Speed Modem Support 4-15
Configure Chat Scripts for Asynchronous Lines 4-16
Create a Chat Script 4-16
Configure the Line to Activate Chat Scripts 4-17
Start a Chat Script Manually 4-17

Support Reverse TCP Connections 4-17

Define Terminal Operation Characteristics 4-18
Specify the Terminal Type 4-18
Set the Terminal Screen Length and Width 4-19
Define Escape Character and Other Key Sequences 4-19
Specify the International Character Display 4-19
Set Character Padding 4-20
Disable Enhanced Editing Mode 4-21
Set a Terminal-Locking Mechanism 4-21
Dedicate a Line to a Particular User 4-21
Provide Line Connection Information after the Login Prompt 4-21
Enable Password Checking at Login 4-22
Create Packet Dispatch Sequences 4-22

Configure Automatic Protocol Startup 4-23

Configure Terminal Banner Messages 4-23
Configure a MOTD Banner 4-23
Configure a Line Activation Message 4-24
Configure an Incoming Message Banner 4-24
Configure an Idle Terminal Message 4-24
Enable or Disable the Display of Messages 4-24

Configure Telnet Capabilities 4-24
Generate a Hardware Break Signal 4-25
Suppress Telnet Remote Echo and Go-Ahead Options 4-25
Negotiate Speed 4-25
Send a Telnet Synchronize Signal 4-26
Set End-of-Line Control 4-26
Define Telnet Connection Failure and Success Messages 4-26
Record the Device Location 4-26
Set Pending Output Notification 4-27
Refuse a Connection 4-27
Establish and Control the EXEC Process 4-27
Display Debug Messages on the Terminal 4-27

Configuration Examples 4-28
Line Configuration Example 4-28
Creating Additional Virtual Terminal Lines Example 4-28
Eliminating Virtual Terminal Lines Example 4-28
Banner Message Example 4-29
Password Checking Examples 4-29

Chapter 5

Managing the System 5-1
Understanding System Management 5-2

Configuration Management 5-3
Customize the Router Prompt 5-3
Set the Router Name 5-4
Create and Monitor Command Aliases 5-4
Create a Command Alias 5-4
Display Command Aliases 5-4
Set the Interval for Load Data 5-4
Set the Router Time Services 5-4
Network Time Protocol 5-5
VINES Time Service 5-6
Cisco 7000 Calendar 5-6
Configure Synchronization of Logging Messages 5-6
Configure NTP 5-7
Configure NTP Authentication 5-7
Configure NTP Associations 5-8
Configure NTP Broadcast Service 5-8
Configure NTP Access Restrictions 5-8
Configure the Source IP Address for NTP Packets 5-9
Configure the System as an Authoritative NTP Server 5-9
Configure NTP to Update the Cisco 7000 Calendar 5-10
Configure VINES Time Service 5-10
Configure Time and Date Manually 5-10
Configure the Time Zone 5-11
Configure Summer Time 5-11
Set the System Clock 5-11
Set the System Calendar 5-12
Monitor Time Services 5-13
Enable the Finger Protocol 5-13
Configure SNMP Support 5-13
Configure for Both SNMPv1 and SNMP v2 5-15
Configure SNMPv2 Support 5-16
Configure SNMPv1 Support 5-19
Configure the Cisco Discovery Protocol 5-22
CDP Configuration Task List 5-22
Enable CDP on an Interface 5-22
Set the CDP Transmission Timer and Hold Time 5-22
Disable CDP for the Router 5-23
Monitor and Maintain CDP 5-23

Security Management 5-23
Establish Password Protection 5-24
Protect Access to Terminal Lines 5-24
Protect Access to Privileged EXEC Commands 5-24
Encrypt the Passwords 5-25
Configure Multiple Privilege Levels 5-25
Set the Privilege Level for a Command 5-25
Change the Default Privilege Level for Lines 5-25

Display Current Privilege Levels 5-26
Logging In To a Privilege Level 5-26
Protect Passwords over Networks 5-26
Disable Password Protection 5-26
Recover a Lost Enable Password 5-27
Recover a Lost Line Password 5-27
Create Access Lists 5-28
Establish Terminal Access Control 5-29
Enable TACACS and Extended TACACS 5-30
Set TACACS Password Protection at the User Level 5-31
Disable Password Checking at the User Level 5-31
Set Optional Password Verification 5-31
Set TACACS Password Protection at the Privileged Level 5-32
Disable Password Checking at the Privileged Level 5-32
Set Notification of User Actions 5-32
Set Authentication of User Actions 5-33
Establish the TACACS Server Host and Response Times 5-33
Set Limits on Login Attempts 5-33
Enable the Extended TACACS Mode 5-34
Enable TACACS for PPP and ARA Protocol Authentication 5-34
Configure AAA/TACACS+ 5-34
Enable AAA/TACACS+ 5-35
Enable Authentication for ARA 5-35
Enable TACACS+ Password Protection at the Privileged Level 5-36
Enable Authentication for Login 5-36
Enable an Authentication Override 5-36
Enable Authentication for PPP 5-37
Restrict Network Access 5-37
Establish Username Authentication 5-37
Enable CHAP 5-38
Enable PAP 5-39

Fault Management 5-39
Display System Information 5-39
Receiving Automatic Warning Messages 5-40
Receiving the Automatic Shutdown Message 5-40
Test Network Connectivity 5-40
Set up the TCP Keepalive Packet Service 5-41
Test Connections with the Ping Command 5-41
Trace Packet Routes 5-41
Limit TCP Transactions 5-41
Test Memory and Interfaces 5-42
Test Flash Memory 5-42
Test System Memory 5-42
Test Interfaces 5-42
Log System Error Messages 5-43
Log Errors to a UNIX Syslog Daemon 5-43
Enable Message Logging 5-44
Set the Error Message Display Device 5-44
Define the Error Message Severity Level and Facilities 5-44
Define the Syslog Facility 5-45

Enable Timestamps on Log Messages 5-46
Enable Debug Operations 5-46

System Performance Management 5-47
Configure Switching and Scheduling Priorities 5-47
Establish Queuing Strategies 5-47
Priority Queuing 5-48
Custom Queuing 5-48
Queuing Task List 5-49
Set Priority by Protocol Type 5-49
Assign a Default Priority 5-50
Set Priority by Interface Type 5-50
Specify the Maximum Packets and Bytes in the Priority Queues 5-50
Assign Priority by STUN Address 5-50
Assign a Priority Group or a Custom Queue to an Interface 5-51
Monitor the Priority and Custom Queuing Lists 5-51
Modify the System Buffer Size 5-51
Delay EXEC Startup 5-52
Handle Idle Telnet Connection 5-52

Accounting Management 5-53
Enable AAA/TACACS+ Accounting 5-53
Display Stack Utilization 5-53
Display Memory Utilization 5-54
Enable IP Accounting for Access List Violations 5-54

System Management Examples 5-54
System Configuration File Example 5-54
Clock, Calendar, and NTP Configuration Examples 5-55
Multiple Levels of Privileges Configuration Examples 5-55
Allowing Users to Clear Lines Example 5-55
Defining an Enable Password for System Operators Example 5-56
Disable a Privilege Level Example 5-56
Buffer Modification Examples 5-56
AAA/TACACS+ Authentication Examples 5-56
Username Examples 5-57

Chapter 6

Configuring Interfaces 6-1
Interface Configuration Task List 6-2

Understand Interface Configuration 6-2

Configure an Asynchronous Serial Interface 6-4
Asynchronous Serial Task List 6-4
Specify Asynchronous Serial Interface 1 6-4
Configure Asynchronous Serial Encapsulation 6-5
Configure the Addressing Method 6-5
Assign a Default Asynchronous Address 6-5
Allow an Asynchronous Address to be Assigned Dynamically 6-6
Configure Dedicated or Interactive Mode 6-6
Enable Asynchronous Routing 6-7
Connect to Remote Routers via PPP or SLIP 6-7

Configure an ATM Interface 6-7

Configure a Channelized E1 Interface 6-7
Channelized E1 Task List 6-8
Configure the E1 Controller 6-8
Define the Line Code 6-8
Define the Framing Characteristics 6-9
Define the E1 Channel Groups 6-9
Configure the E1 Interface 6-9

Configure a Channelized T1 Interface 6-9
Channelized T1 Task List 6-10
Configure the T1 Controller 6-10
Define the Line Code 6-11
Define the Framing Characteristics 6-11
Define the Clock Source 6-11
Define the T1 Channel Groups 6-12
Configure the T1 Interface 6-12

Configure a Dialer Interface 6-12

Configure an Ethernet Interface 6-12
Ethernet Interface Task List 6-13
Specify an Ethernet Interface 6-13
Configure DHCP 6-13
Configure Ethernet Encapsulation 6-14
Configure the Ethernet Network Interface Module on the Cisco 4000 6-14
Extend the 10BaseT Capability 6-15

Configure a Fiber Distributed Data Interface (FDDI) 6-15
Using Connection Management (CMT) Information 6-16
FDDI Task List 6-16
Specify an FDDI 6-17
Enable FDDI Bridging Encapsulation 6-17
Set the Token Rotation Time 6-18
Set the Transmission Valid Timer 6-18
Control the Transmission Timer 6-19
Modify the C-Min Timer 6-19
Modify the TB-Min Timer 6-19
Modify the FDDI Timeout Timer 6-19
Control SMT Frame Processing 6-19
Enable Duplicate Address Checking 6-19
Set the Bit Control 6-20
Control the CMT Microcode 6-20
Start and Stop FDDI 6-20
Control the FDDI SMT Message Queue Size 6-20
Preallocate Buffers for Bursty FDDI Traffic 6-21

Configure a High-Speed Serial Interface (HSSI) 6-21
HSSI Task List 6-21
Specify an HSSI 6-21
Specify HSSI Encapsulation 6-22
Invoke ATM on an HSSI Line 6-22
Convert HSSI to Clock Master 6-22

Configure a Hub Interface 6-22
Enable a Hub Port 6-23
Disable or Enable Automatic Receiver Polarity Reversal 6-23
Disable or Enable the Link Test Function 6-23
Enable Source Address Control 6-24

Configure an ISDN Basic BRI, MBRI, or PRI Interface 6-24

Configure a LAN Extender Interface 6-25
LAN Extender Interface Configuration Task List 6-27
Configure and Create a LAN Extender Interface 6-28
Define Packet Filters 6-28
Filter by MAC Address and Vendor Code 6-30
Filter by Protocol Type 6-30
Control Priority Queuing 6-31
Control the Sending of Commands to the LAN Extender 6-32
Shut Down and Restart the LAN Extender's Ethernet Interface 6-32
Restart the LAN Extender 6-33
Download a Software Image to the LAN Extender 6-33
Troubleshoot the LAN Extender 6-33

Configure a Loopback Interface 6-35

Configure a Null Interface 6-36

Configure a Synchronous Serial Interface 6-36
Synchronous Serial Task List 6-37
Specify a Synchronous Serial Interface 6-37
Specify Synchronous Serial Encapsulation 6-38
Configure PPP 6-38
PPP Magic Number Support 6-39
Enable PPP Encapsulation 6-39
Enable CHAP or PAP Authentication 6-39
Enable Link Quality Monitoring (LQM) 6-40
Configure Compression of PPP Data 6-41
Configure Compression of LAPB Data 6-41
Configure Compression of HDLC Data 6-42
Invoke ATM over a Serial Line 6-42
Configure the CRC 6-43
Use the NRZI Line-Coding Format 6-43
Enable the Internal Clock 6-43
Invert the Transmit Clock Signal 6-43
Set Transmit Delay 6-44
Configure DTR Signal Pulsing 6-44
Ignore DCD and Monitor DSR as Line Up/Down Indicator 6-44
Configure the Clock Rate on DCE Appliques 6-44
Specify the Serial Network Interface Module Timing 6-45
Specify G.703 Interface Options 6-45
Enable Framed Mode 6-45
Enable CRC4 Generation 6-46
Use Time Slot 16 for Data 6-46
Specify a Clock 6-46

Configure a Token Ring Interface 6-46

Token Ring Task List 6-47
Specify a Token Ring Interface 6-47
Select the Token Ring Speed 6-47
Enable Early Token Release 6-48

Configure PCbus Token Ring Interface Management 6-48

Configure a Tunnel Interface 6-48
Advantages of Tunneling 6-49
Special Considerations 6-50
IP Tunneling Task List 6-51
Specify the Tunnel Interface 6-52
Configure the Tunnel Source 6-52
Configure the Tunnel Destination 6-52
Configure the Tunnel Mode 6-52
Configure End-to-End Checksumming 6-53
Configure a Tunnel Identification Key 6-53
Configure a Tunnel Interface to Drop Out-of-Order Datagrams 6-54

Understand Subinterfaces 6-54

Configure Features Available on Any Interface 6-54
Add a Description for an Interface 6-54
Configure MOP 6-55
Control Interface Hold-Queue Limits 6-55
Set Bandwidth 6-55
Set Interface Delay 6-56
Adjust Timers 6-56
Limit Transmit Queue Size 6-56
Adjust Maximum Packet Size or MTU Size 6-56

Configure Dial Backup Service 6-57
Configure Loopback Detection 6-58

Understand Online Insertion and Removal (OIR) 6-58

Understand Fast, Autonomous, and SSE Switching Support 6-59

Monitor and Maintain the Interface 6-59
Monitor Interface Status 6-59
Monitor the Interface Port 6-60
Monitor the T1 or E1 Controller 6-60
Monitor the LAN Extender Interface 6-61
Monitor and Maintain a Hub 6-61
Shut Down the Hub Port 6-61
Reset the Hub or Clear the Hub Counters 6-61
Monitor the Hub 6-62
Monitor IP Tunnels 6-62
Clear and Reset the Interface 6-62
Shut Down and Restart the Interface 6-63
Run Interface Loopback Diagnostics 6-63
Enable Loopback Testing on the HSSI 6-64
Enable Loopback on MCI and SCI Serial Cards 6-66
Enable Loopback on MCI and MEC Ethernet Cards 6-66
Configure the Ethernet Loopback Server 6-67

Enable Loopback on the Channelized T1 Interface 6-67
Enable Loopback on the CSC-FCI FDDI Card 6-67
Enable Loopback on Token Ring Cards 6-67

Interface Configuration Examples 6-67
Examples of Enabling Interface Configuration 6-68
Example of a Dedicated Asynchronous Interface 6-68
Example of Restricting Access on the Asynchronous Interface 6-68
Example of Asynchronous Routing and Dynamic Addressing 6-69
Examples of Channelized T1 Controller and Interface 6-69
Example of Enabling Ethernet Encapsulation 6-70
Example of Enabling a LAN Extender Interface 6-70
Examples of LAN Extender Interface Access List 6-70
Example of Filtering by MAC Address 6-70
Example of Filtering by Ethernet Type Code 6-70
Examples of DHCP 6-71
Example of CHAP with an Encrypted Password 6-71
Examples of IP Tunneling 6-72
Example of Routing Two AppleTalk Networks across an IP-Only Backbone 6-72
Example of Routing a Private IP Network and a Novell Net across a Public Service Provider 6-74
Examples of Interface Descriptions 6-75
Examples of Interface Shutdown 6-75
Examples of Dial Backup Service When the Primary Line Goes Down 6-75
Examples of Dial Backup Service When the Primary Line Reaches Threshold 6-76
Examples of Dial Backup Service When the Primary Line Exceeds Threshold 6-76
Examples of Hub Configuration 6-76
Examples of Hub Port Startup 6-77
Examples of Source Address for an Ethernet Hub Port Configuration 6-77
Examples of Hub Port Shutdown 6-77

Chapter 7

Configuring ATM 7-1
Cisco's Implementation of ATM 7-1
Cisco 7000 AIP 7-3
AIP Features 7-3
AIP Interface Types 7-4
Microcode 7-4
Virtual Circuits 7-4
Cisco 4500 NPM 7-5
NPM Features 7-5
NPM ATM Interface Types 7-5
Virtual Circuits 7-6

ATM Access over a Serial Interface 7-6
ATM Serial Access Configuration Task List 7-6
Enable the Serial Interface 7-7
Enable ATM-DXI Encapsulation 7-7
Set Up the ATM-DXI PVC 7-7
Map Protocol Addresses to the ATM-DXI PVC 7-8
Monitor and Maintain the ATM-DXI Serial Interface 7-8

Cisco 7000 AIP Configuration Task List 7-8

Enable the AIP on the Cisco 7000 7-9

Customize the AIP on the Cisco 7000 7-9
Configure the Rate Queue (Cisco 7000) 7-10
Use Dynamic Rate Queues (Cisco 7000) 7-10
Configure a Permanent Rate Queue (Cisco 7000) 7-10
Configure MTU Size (Cisco 7000) 7-11
Set the SONET PLIM (Cisco 7000) 7-11
Set Loopback Mode (Cisco 7000) 7-11
Set the Exception-Queue Length (Cisco 7000) 7-11
Limit the Number of Virtual Circuits (Cisco 7000) 7-11
Limit the Message Identifiers Allowed on Virtual Circuits (Cisco 7000) 7-12
Set the Raw-Queue Size (Cisco 7000) 7-12
Configure Buffer Sizes (Cisco 7000) 7-12
Set the VCI-to-VPI Ratio (Cisco 7000) 7-13
Set the VP Filter Register (Cisco 7000) 7-13
Set the Source of the Transmit Clock (Cisco 7000) 7-13

Configure PVCs on the Cisco 7000 7-13
Create a PVC (Cisco 7000) 7-14
Map a Protocol Address to a PVC (Cisco 7000) 7-14

Configure SVCs on the Cisco 7000 7-15
Configure the PVC That Performs SVC Call Setup (Cisco 7000) 7-16
Configure the NSAP Address (Cisco 7000) 7-16
Change QOS Values (Cisco 7000) 7-17
Configure SSCOP (Cisco 7000) 7-19
Set the Poll Timer (Cisco 7000) 7-19
Set the Keepalive Timer (Cisco 7000) 7-19
Set the Connection Control Timer (Cisco 7000) 7-19
Set the Transmit and Receive Windows (Cisco 7000) 7-20
Close an SVC (Cisco 7000) 7-20

Configure ATM Subinterfaces for SMDS Networks on the Cisco 7000 7-20

Configure Transparent Bridging over ATM on the Cisco 7000 7-21
Enable Transparent Bridging for SMDS Subinterfaces 7-22
Enable Transparent Bridging for SNAP PVCs 7-22

Cisco 4500 ATM Configuration Task List 7-23

Enable the ATM Interface on the Cisco 4500 7-23

Configure PVCs on the Cisco 4500 7-24
Create a PVC (Cisco 4500) 7-24
Map a Protocol Address to a PVC (Cisco 4500) 7-24
Configure Transmission of Loopback Cells to Verify Connectivity (Cisco 4500) 7-25

Configure SVCs on the Cisco 4500 7-25
Configure the PVC That Performs SVC Call Setup (Cisco 4500) 7-26
Configure the NSAP Address (Cisco 4500) 7-27
Change QOS Values (Cisco 4500) 7-28
Configure SSCOP (Cisco 4500) 7-30
Set the Poll Timer (Cisco 4500) 7-30
Set the Keepalive Timer (Cisco 4500) 7-30

Set the Connection Control Timer (Cisco 4500) 7-30
Set the Transmit and Receive Windows (Cisco 4500) 7-31
Close an SVC (Cisco 4500) 7-31

Customize the NPM on the Cisco 4500 7-31
Configure the Rate Queue (Cisco 4500) 7-31
Use Dynamic Rate Queues (Cisco 4500) 7-32
Configure a Permanent Rate Queue (Cisco 4500) 7-32
Configure MTU Size (Cisco 4500) 7-32
Set the SONET PLIM (Cisco 4500) 7-32
Set Loopback Mode (Cisco 4500) 7-33
Set the VCI-to-VPI Ratio (Cisco 4500) 7-33
Set the Source of the Transmit Clock (Cisco 4500) 7-33

Configure Transparent Bridging for ATM on the Cisco 4500 7-33

Monitor and Maintain the ATM Interface 7-34

ATM Access over a Serial Interface Example 7-35

Cisco 7000 ATM Configuration Examples 7-35
PVC with AAL5 and LLC/SNAP Encapsulation Examples (Cisco 7000) 7-35
PVCs in a Fully Meshed Network Example (Cisco 7000) 7-36
SVCs in a Fully Meshed Network Example (Cisco 7000) 7-37
PVC with AAL3/4 and SMDS Encapsulation Examples (Cisco 7000) 7-38
Dynamic Rate Queue Examples (Cisco 7000) 7-39
Transparent Bridging on an AAL5-SNAP PVC Example (Cisco 7000) 7-39
Transparent Bridging on an SMDS Subinterface Example (Cisco 7000) 7-39

Cisco 4500 ATM Configuration Examples 7-39
PVC with AAL5 and LLC/SNAP Encapsulation Examples (Cisco 4500) 7-40
PVCs in a Fully Meshed Network Example (Cisco 4500) 7-40
SVCs in a Fully Meshed Network Example (Cisco 4500) 7-42
Dynamic Rate Queue Examples (Cisco 4500) 7-42
Transparent Bridging on an AAL5-SNAP PVC Example (Cisco 4500) 7-43

Chapter 8

Configuring DDR 8-1
Cisco's Implementation of Dial Backup and DDR 8-1
Fast Call Rerouting for ISDN 8-2
Placing Calls Using DDR 8-2
Chat Scripts on the Auxiliary Port 8-2
V.25bis over Synchronous Interfaces 8-3
DTR Dialing for Synchronous Interfaces 8-4
Controlling Access for DDR 8-4

Dial Backup Configuration Task List 8-5
Select Backup Line 8-5
Define the Traffic Load Threshold 8-5
Define Backup Line Delays 8-6

DDR Configuration Task Overview 8-6

Configure an Interface to Place Calls 8-7
Create Chat Scripts for Asynchronous Interfaces 8-7

Suggested Chat Script Naming Conventions 8-7
Specify Chat Scripts for DDR 8-8
Configure Calls to a Single Site 8-8
Configure Calls to Multiple Sites 8-9
Calling on a Single Line or Multiple Lines 8-9
Configure Calling from Dialer Rotary Groups 8-10

Configure an Interface to Receive Calls 8-13
Configure an Interface to Receive Calls from a Single Site 8-13
Configure an Interface to Receive Calls from Multiple Sites 8-13
Configure an Interface to Receive Calls on a Single Line or Multiple Lines 8-13
Configure an Interface to Receive Calls on a Dialer Rotary Group 8-13

Configure an Interface to Place and Receive Calls 8-16
Place and Receive Calls from a Single Site 8-17
Place and Receive Calls from Multiple Sites 8-17

Configure Snapshot Routing 8-19
Configure the Client Router 8-20
Configure the Server Router 8-21

Configure DDR over LAPB 8-21

Configure DDR over X.25 8-22

Configure DDR over Frame Relay 8-22
Configuration Restrictions 8-23
Configuration Overview 8-23

Configure DDR for Routed Protocols 8-23
Configure DDR for AppleTalk 8-24
Configure DDR for Banyan VINES 8-24
Configure DDR for DECnet 8-25
Configure DDR for IP 8-25
Configure ISO CLNS over DDR 8-26
Configure DDR for Novell IPX 8-26
Configure XNS over DDR 8-27

Configure DDR for Transparent Bridging 8-28
Define the Protocols to Bridge 8-28
Specify the Bridging Protocol 8-28
Control Access for Bridging 8-29
Permit All Bridge Packets 8-29
Control Bridging Access by Ethernet Type Codes 8-29
Configure an Interface for Bridging 8-29
Specify the Interface 8-30
Configure the Destination 8-30
Assign the Interface to a Bridge Group 8-30

Customize the DDR Network 8-30
Set Line-Idle Time 8-31
Set Idle Time for Busy Interfaces 8-31
Set Line-Down Time 8-31
Set Carrier-Wait Time 8-31
Control Access to a DDR Interface 8-32

Set Dialer Interface Priority 8-33
Configure a Dialer Hold Queue 8-33
Configure Bandwidth on Demand 8-33

Monitor DDR Connections and Snapshot Routing 8-34

DDR Configuration Examples 8-34
Dial Backup Using the Auxiliary Port Example 8-35
Dial Backup Using DDR and ISDN Example 8-35
Configuring DDR in an IP Environment Example 8-36
Configuring Multiple Destination Dial Strings Example 8-37
Configuring Dialer Rotary Groups Example 8-37
Dialing a Single Site or Multiple Sites Example 8-37
Using Chat Scripts Example 8-38
Writing and Implementing Chat Scripts Example 8-39
Chat Scripts and Dialer Mapping Example 8-39
System Scripts and Modem Scripts Example 8-40
Dial-on-Demand PPP Configuration Example 8-41
DTR Dialing Configuration Example 8-42
Snapshot Routing Examples 8-43
LAPB Support Configuration Example 8-43
X.25 Support Configuration Example 8-43
Frame Relay Support Examples 8-44
In-Band Dialing (V.25bis) and Static Map 8-44
ISDN Dialing and Dynamic Maps 8-44
ISDN Dialing and Subinterfaces 8-45
AppleTalk Configuration Example 8-46
Banyan VINES Configuration Example 8-46
DECnet Configuration Example 8-47
ISO CLNS Configuration Example 8-47
XNS Configuration Example 8-47
DDR for Transparent Bridging Examples 8-48

Chapter 9

Configuring Frame Relay 9-1
Cisco's Implementation of Frame Relay 9-1

Frame Relay Hardware Configurations 9-2

Frame Relay Configuration Task List 9-3

Enable Frame Relay Encapsulation 9-4

Configure Dynamic or Static Address Mapping 9-4
Configure Dynamic Mapping 9-4
Configure Static Mapping 9-4

Configure the LMI 9-5
Set the LMI Type 9-5
Set the LMI Keepalive Interval 9-6
Set the LMI Polling and Timer Intervals 9-6

Customize Frame Relay for Your Network 9-7
Understand and Define Frame Relay Subinterfaces 9-7
Define Frame Relay Subinterfaces 9-9

Associate a DLCI with a Subinterface 9-9
Configure Dynamic or Static Address Mapping 9-10
Configure a Backup Interface for a Subinterface 9-11
Configure Frame Relay Switching 9-11
Enable Frame Relay Switching 9-12
Configure a Frame Relay DTE Device, DCE Switch, or NNI Support 9-12
Specify the Static Route 9-13
Disable or Reenable Frame Relay Inverse ARP 9-13
Create a Broadcast Queue for an Interface 9-14
Configure TCP/IP Header Compression 9-14
Configure an Individual IP Map for TCP/IP Header Compression 9-15
Configure an Interface for TCP/IP Header Compression 9-15
Disable TCP/IP Header Compression 9-16
Configure Discard Eligibility 9-16
Monitor the Frame Relay Connections 9-17
Frame Relay Configuration Examples 9-17
IETF Encapsulation Examples 9-17
Static Address Mapping Examples 9-18
Two Routers in Static Mode Example 9-18
AppleTalk Routing Example 9-18
DECnet Routing Example 9-19
IPX Routing Example 9-19
Subinterface Examples 9-19
Basic Subinterface Examples 9-19
IPX Routes over Frame Relay Subinterfaces Example 9-20
Unnumbered IP over a Point-to-Point Subinterface Example 9-20
Transparent Bridging Using Subinterfaces Example 9-21
Configuration Providing Backward Compatibility Example 9-21
Booting from a Network Server over Frame Relay Example 9-22
Frame Relay Switching Examples 9-23
PVC Switching Configuration Example 9-23
Pure Frame Relay DCE Example 9-24
Hybrid DTE/DCE PVC Switching Example 9-26
Switching over an IP Tunnel Example 9-27
TCP/IP Header Compression Examples 9-28
IP Map with Inherited TCP/IP Header Compression Example 9-28
Using an IP Map to Override TCP/IP Header Compression Example 9-29
Disabling TCP/IP Header Compression Examples 9-29
Disabling Inherited TCP/IP Header Compression Example 9-29
Disabling Explicit TCP/IP Header Compression Example 9-30

Chapter 10

Configuring ISDN 10-1
Cisco's Implementation of ISDN 10-3
ISDN Channels 10-3
Network-Customer Premises Boundary 10-3
ISDN Task List 10-4
Understand Line Configuration Requirements 10-5

Configure an ISDN BRI 10-5
Check the Buffers 10-6
Select the ISDN Switch Type 10-6
Define ISDN TEI Negotiation 10-7
Specify an ISDN Basic Rate Interface 10-7
Define ISDN Service Profile Identifiers (SPIDs) 10-7
Configure Calling Line Identification Screening 10-8
Configure Called Party Number Verification 10-8
Configure ISDN Calling Number Identification 10-9
Configure the Line Speed for Calls Not ISDN End-To-End 10-9

Configure an ISDN PRI 10-10
Configure Channelized T1 ISDN PRI 10-10
Configure Channelized E1 ISDN PRI 10-10

Configure Encapsulation for Frame Relay or X.25 Networks 10-11

Configure Network Addressing 10-11

Configure Semipermanent Connections 10-12

Perform Configuration Self-Tests 10-13

Monitor and Maintain ISDN Interfaces 10-13

Chapter 11

Configuring SMDS 11-1
Cisco's Implementation of SMDS 11-1
SMDS Addresses 11-2
SMDS Hardware Requirements 11-3

SMDS Configuration Task List 11-3

Enable SMDS on the Interface 11-3
Set SMDS Encapsulation 11-4
Specify the SMDS Address 11-4
Establish Address Mapping 11-4
Map a Multicast Address to an SMDS Address 11-5
Enable ARP 11-5
Enable Broadcast ARP Messages 11-6

Customize Your SMDS Network 11-6
Configure Specific Protocols 11-7
ARP and IP 11-7
DECnet 11-7
CLNS 11-7
XNS and IPX 11-7
AppleTalk 11-8
Banyan VINES 11-8
Enable Transparent Bridging 11-8
Configure SMDS Subinterfaces for Multiple Logical IP Subnetworks 11-8
Reenable the Data Exchange Interface Version 3.2 with Heartbeat Support 11-9
Configure Pseudobroadcasting 11-9
Enable IP Fast Switching 11-10

Monitor the SMDS Connection 11-10

SMDS Configuration Examples 11-10
Typical Multiprotocol Configuration Example 11-11
Remote Peer on the Same Network Example 11-11
AppleTalk Configuration Examples 11-12
Nonextended Appletalk Network Example 11-12
Extended AppleTalk Network Example 11-12
MultiLIS over SMDS Example 11-13
Pseudobroadcasting Example 11-14

Chapter 12

Configuring X.25 and LAPB 12-1
Cisco's Implementation of LAPB and X.25 12-1
LAPB Configuration Task List 12-2
Configure a LAPB Datagram Transport 12-3
Modify LAPB Protocol Parameters 12-4
Configure LAPB Priority and Custom Queuing 12-5
X.25 Configuration Task List 12-6
Configure an X.25 Interface 12-6
Set the X.25 Mode 12-7
Set the Virtual Circuit Ranges 12-7
Set the Packet Numbering Modulo 12-8
Set the X.121 Address 12-9
Set the Default Flow Control Values 12-9
Set Default Window Sizes 12-9
Set Default Packet Sizes 12-10
Configure Additional X.25 Interface Parameters 12-10
Configure the X.25 Level 3 Timers 12-11
Configure X.25 Addresses 12-11
Understand Normal X.25 Addressing 12-11
Understand X.25 Subaddresses 12-12
Configure an Interface Alias Address 12-12
Suppress or Replace the Calling Address 12-12
Suppress the Called Address 12-13
Establish a Default Virtual Circuit Protocol 12-13
Disable Packet-Level Protocol Restarts 12-13
Modify LAPB Protocol Parameters 12-13
Configure an X.25 Datagram Transport 12-15
Configure Subinterfaces 12-15
Point-to-Point and Multipoint Subinterfaces 12-16
Creating and Configuring X.25 Subinterfaces 12-16
Map Protocol Addresses to X.121 Addresses 12-17
Protocol Encapsulation for Single-Protocol and Multiprotocol Virtual Circuits 12-17
Protocol Identification 12-17
Map Datagram Addresses to X.25 Hosts 12-18
Establish an Encapsulation PVC 12-20
Set X.25 TCP Header Compression 12-20

Configure X.25 Bridging 12-21

Configure Additional X.25 Datagram Transport Features 12-21
Configure X.25 Payload Compression 12-21
Configure the Encapsulation Virtual Circuit Idle Time 12-22
Increase the Number of Virtual Circuits Allowed 12-23
Configure the Ignore Destination Time 12-23
Establish the Packet Acknowledgment Policy 12-23
Configure X.25 User Facilities 12-23
Define the Virtual Circuit Packet Hold Queue Size 12-25
Restrict Map Usage 12-25

Configure X.25 Routing 12-25
Enable X.25 Routing 12-26
Configure a Local X.25 Route 12-27
Configure an XOT (Remote) X.25 Route 12-27
Configure a Locally Switched PVC 12-27
Configure an XOT (Remote) PVC 12-28

Configure Additional X.25 Routing Features 12-28
Configure XOT to Use Interface Default Flow Control Values 12-28
Substitute Addresses in a Local X.25 Route 12-29
Configure XOT Alternate Destinations 12-29

Configure CMNS Routing 12-30
Enable CMNS on an Interface 12-30
Specify a CMNS Static Map of Addresses 12-31

Configure DDN or BFE X.25 12-31
DDN X.25 Dynamic Mapping 12-31
BFE IP Address Conventions 12-32
Enable DDN X.25 12-32
Define IP Precedence Handling 12-33
Configure Blacker Front-End X.25 12-33

Monitor and Maintain LAPB and X.25 12-35

X.25 Facility Handling 12-35
Facility Handling in Encapsulated X.25 Virtual Circuits 12-35
Facility Handling in Routed X.25 Virtual Circuits 12-35
Standard (1984 X.25) Facilities 12-36
ITU-T-Specified Marker Facilities 12-37
Local Marker Facilities Specified for DDN or BFE X.25 12-37

X.25 and LAPB Configuration Examples 12-38
Typical LAPB Configuration Example 12-38
Typical X.25 Configuration Example 12-39
Virtual Circuit Ranges Example 12-40
PVC Switching on the Same Router Example 12-40
X.25 Route Address Pattern Matching Example 12-40
X.25 Routing Example 12-41
PVC Used to Exchange IP Traffic Example 12-42
Point-to-Point Subinterface Configuration Example 12-42
Simple Remote PVC Tunneling Example 12-42
Remote PVC Tunneling Example 12-43

CMNS Configured for X.121 and MAC Addresses Example 12-44
CMNS Switched over a PDN Example 12-44
CMNS Switched over Leased Lines Example 12-46
DDN X.25 Configuration Example 12-48
Blacker Emergency Mode Example 12-48
X.25 Configured to Allow Ping Support over Multiple Lines Example 12-48
Booting from a Network Server over X.25 Example 12-50

Chapter 13

Configuring Apollo Domain 13-1
Cisco's Implementation of Apollo Domain 13-1
Apollo Domain Addresses 13-2
Apollo Domain Configuration Task List 13-2
Enable Apollo Domain Routing 13-2
Enable Apollo Domain Routing on the Router 13-3
Enable Apollo Domain Routing on an Interface 13-3
Control Access to the Apollo Domain Network 13-3
Tune Apollo Domain Network Performance 13-4
Configure Static Routes 13-4
Set Routing Table Update Timers 13-4
Set the Maximum Paths 13-4
Configure Apollo Domain over WANs 13-5
Monitor the Apollo Domain Network 13-5
Apollo Domain Configuration Examples 13-5
Configuring Apollo Domain Routing Example 13-5
Access List Example 13-6
Routing Table Update Timer Example 13-6

Chapter 14

Configuring AppleTalk 14-1
Cisco's Implementation of AppleTalk 14-1
Standard AppleTalk Services 14-2
Enhancements to Standard AppleTalk 14-2
AppleTalk Phase 1 and Phase 2 14-3
AppleTalk Addresses 14-4
Configuration Guidelines and Compatibility Rules 14-5
AppleTalk Configuration Task List 14-5
Enable AppleTalk Routing 14-6
Enable AppleTalk Routing on the Router 14-6
Manually Configure an Interface 14-6
Dynamically Configure an Interface 14-7
Dynamically Configure a Nonextended Interface 14-7
Dynamically Configure an Extended Interface 14-8
Configure Transition Mode 14-8

Create an AppleTalk Routing Process 14-9

Control Access to AppleTalk Networks 14-9
Create Access Lists 14-11
Create Filters 14-12
Create Data Packet Filters 14-12
Create Routing Table Update Filters 14-13
Create GetZoneList (GZL) Filters 14-14
Enable ZIP Reply Filters 14-15
Enable Partial Zone Filters 14-16

Configure the Name Display Facility 14-16

Set up Special Configurations 14-17
Configure AURP 14-17
Configure Free-Trade Zones 14-18
Configure SNMP in AppleTalk Networks 14-18
Configure AppleTalk Tunneling 14-19
Configure AppleTalk MacIP 14-20
Configure IPTalk 14-22
Configure IP Encapsulation of AppleTalk Packets 14-23
Specify the UDP Port Ranges 14-24

Configure AppleTalk Control Protocol for PPP 14-25

Tune AppleTalk Network Performance 14-25
Control Routing Updates 14-25
Disable the Processing of Routed RTMP Packets 14-26
Disable the Transmission of Routing Updates 14-26
Prevent the Advertisement of Routes to Networks with No Associated Zones 14-26
Set Routing Table Update Timers 14-27
Assign Proxy Network Numbers 14-27
Disable Checksum Generation and Verification 14-28
Control the AppleTalk ARP Table 14-28
Control the Delay between ZIP Queries 14-29
Log Significant Network Events 14-29
Disable Fast Switching 14-29

Configure AppleTalk Enhanced IGRP 14-29
Cisco's Enhanced IGRP Implementation 14-29
Enhanced IGRP Configuration Task List 14-31
Enable AppleTalk Enhanced IGRP 14-31
Configure Miscellaneous AppleTalk Enhanced IGRP Parameters 14-31
Disable Redistribution of Routing Information 14-32
Adjust the Interval between Hello Packets and the Hold Time 14-32
Disable Split Horizon 14-32

Configure AppleTalk Interenterprise Routing 14-33
Enable AppleTalk Interenterprise Routing 14-34
Remap Network Numbers 14-35
Control Hop Count 14-35

Configure AppleTalk over WANs 14-35

Monitor and Maintain the AppleTalk Network 14-36

Monitor and Maintain the AppleTalk Network Using Router Commands 14-36
Monitor the AppleTalk Network Using Network Monitoring Packages 14-37

AppleTalk Configuration Examples 14-38
Configuring an Extended AppleTalk Network Example 14-39
Configuring a Nonextended AppleTalk Network Example 14-39
Configuring a Nonextended Network in Discovery Mode Example 14-40
Transition Mode Example 14-40
AppleTalk Access List Examples 14-41
Defining an Access List to Filter Data Packets 14-41
Defining an Access List to Filter Incoming Routing Table Updates 14-42
Comparison of Alternative Segmentation Solutions 14-43
Configuring Partial Zone Advertisement 14-44
GZL and ZIP Reply Filter Examples 14-45
Hiding and Sharing Resources with Access List Examples 14-46
Establishing a Free-Trade Zone Example 14-46
Restricting Resource Availability 14-48
Implicit Configuration of the Admin and Test-Lab Zones 14-50
MacIP Examples 14-50
SNMP Example 14-51
Proxy Network Number Example 14-51
AppleTalk Enhanced IGRP Example 14-52
AppleTalk Interenterprise Routing Example 14-52
Configure AppleTalk Control Protocol Example 14-53
AppleTalk over DDR Example 14-53
IPTalk Example 14-54

Chapter 15

Configuring Banyan VINES 15-1
Cisco's Implementation of VINES 15-1

VINES Addresses 15-1

VINES Configuration Task List 15-2

Configure VINES Routing 15-2
Enable VINES Routing on the Router 15-3
Enable VINES Routing on an Interface 15-3
Enable VINES on Serverless Networks 15-4

Control Access to the VINES Network 15-4

Configure VINES Network Parameters 15-5
Select an Encapsulation Type 15-6
Control the Display of Host Addresses 15-6
Control the Base of Host Addresses 15-6
Control RTP Routing Updates 15-6
Control RTP and SRTP Routing Updates 15-7
Disable Fast Switching 15-8
Set the Time 15-8
Configure Static Routes 15-9
Configure Static Paths 15-9
Control the Forwarding of Broadcast Packets 15-9

Configure VINES over WANs 15-10

Monitor and Maintain the VINES Network 15-10

VINES Configuration Examples 15-11
Typical VINES Network Configuration Example 15-11
Serverless Network Configuration Example 15-11
Access List Example 15-14
Time-of-Day Service Example 15-15

Chapter 16

Configuring DECnet 16-1
Cisco's Implementation of DECnet 16-1

DECnet Configuration Task List 16-2

Enable DECnet Routing 16-3
Enable DECnet Phase IV Routing 16-3
Enable DECnet Phase IV Prime Routing 16-4
Assign a DECnet Cost to Each Interface 16-5
Specify the DECnet Node Type 16-6

Configure DECnet on Token Rings 16-6

Configure Address Translation 16-7
Make a "Poor Man's Routing" Connection 16-8

Specify Name-to-DECnet Address Mapping 16-8

Enable Phase IV-to-Phase V Conversion 16-8

Propagate Phase IV Areas through an OSI Backbone 16-9

Establish the Routing Table Size 16-9

Configure Level 1 Routers 16-10
Set Areas as Unreachable 16-10

Configure Level 2 Routers 16-10
Set Areas as Unreachable 16-10

Specify Designated Routers 16-11

Configure Static Routing 16-11
Configure a Static Route 16-11
Configure a Static Route for an Interface 16-12
Configure a Default Static Route 16-12
Configure a Default Static Route for an Interface 16-12
Configure DECnet Static Route Propagation 16-12

Control Access to DECnet Networks 16-13
Create an Access List Based on Source Addresses 16-13
Create an Access List Based on Source and Destination Addresses 16-13
Add Filters to Access Lists 16-13
Configure Access Groups 16-14
Configure Routing Filters 16-14

Enhance DECnet Performance 16-14
Set Maximum Equal-Cost Paths 16-14

Establish Selection for Paths of Equal Cost 16-15
Set Maximum Visits 16-15
Adjust the Hello Timer 16-15
Disable Fast Switching 16-16
Set the Congestion Threshold 16-16
Adjust the Broadcast Routing Timer 16-16

Configure DECnet over DDR 16-16

Configure DECnet over WANs 16-17

Monitor and Maintain the DECnet Network 16-17

DECnet Configuration Examples 16-17
Enabling DECnet Example 16-18
Phase IV-to-Phase V Conversion Example 16-18
Configuring Phase IV Areas through an OSI Backbone Example 16-19
Configuring Address Translation Example 16-20
Configuring DECnet Phase IV Prime Examples 16-22

Chapter 17

Configuring IP 17-1
Cisco's Implementation of IP 17-1

IP Configuration Task List 17-1

Assign IP Addresses to Network Interfaces 17-2
Assign Multiple IP Addresses to Network Interfaces 17-3
Enable Use of Subnet Zero 17-4
Enable Classless Routing Behavior 17-4
Enable IP Processing on a Serial Interface 17-6

Configure Address Resolution Methods 17-6
Establish Address Resolution 17-7
Define a Static ARP Cache 17-7
Set ARP Encapsulations 17-8
Disable Proxy ARP 17-8
Configure Local-Area Mobility 17-9
Map Host Names to IP Addresses 17-9
Map IP Addresses to Host Names 17-10
Specify the Domain Name 17-10
Specify a Name Server 17-11
Disable the DNS 17-11
Use the DNS to Discover ISO CLNS Addresses 17-11
Configure HP Probe Proxy Name Requests 17-11
Configure the Next Hop Resolution Protocol 17-12
Cisco's Implementation of NHRP 17-12
Modes of Operation 17-14
NHRP Configuration Task List 17-14
Enable NHRP on an Interface 17-15
Configure a Station's Static IP-to-NBMA Address Mapping 17-15
Statically Configure a Next Hop Server (Server Mode) 17-16
Configure NHRP Authentication 17-16
Control NHRP Initiation 17-16

Suppress Forward and Reverse Record Options 17-17
Specify the NHRP Responder Address 17-17
Change the Time Period NBMA Addresses Are Advertised as Valid 17-17
Configure a GRE Tunnel for Multipoint Operation 17-18

Disable IP Routing 17-18
Routing Assistance When IP Routing Is Disabled 17-18
Proxy ARP 17-18
Default Gateway 17-19
Router Discovery Mechanism 17-19

Configure a Routing Process 17-20

Configure Broadcast Packet Handling 17-20
Enable Directed Broadcast-to-Physical Broadcast Translation 17-21
Forward UDP Broadcast Packets and Protocols 17-22
Establish an IP Broadcast Address 17-22
Flood IP Broadcasts 17-23
Speed Up Flooding of UDP Datagrams 17-24

Configure IP Services 17-24
Disable ICMP Protocol Unreachable Messages 17-25
Disable ICMP Redirect Messages 17-25
Understand Path MTU Discovery 17-25
Set the MTU Packet Size 17-27
Enable ICMP Mask Reply Messages 17-27
Disable IP Source Routing 17-27
Configure Simplex Ethernet Interfaces 17-28

Filter IP Packets 17-28
Create Standard and Extended Access Lists 17-29
Apply an Access List to an Interface or Terminal Line 17-30

Configure the Hot Standby Protocol 17-30

Configure Basic IP Security Options 17-32
Enable IPSO and Set the Security Classifications 17-32
Specify How IP Security Options Are Processed 17-32
Default Values for Command Keywords 17-33

Configure Extended IP Security Options 17-33
Configure Global Default Settings 17-34
Attach ESOs to an Interface 17-34
Attach AESOs to an Interface 17-34

Configure the DNSIX Audit Trail Facility 17-34
Enable the DNSIX Audit Trail Facility 17-35
Specify Hosts to Receive Audit Trail Messages 17-35
Specify Transmission Parameters 17-35

Configure IP Accounting 17-35

Configure Performance Parameters 17-36
Compress TCP Packet Headers 17-37
Set the TCP Connection Attempt Time 17-37
Enable Path MTU Discovery 17-38

Enable Fast Switching 17-38
Enable Fast Switching on the Same Interface 17-38
Enable SSE Fast Switching 17-39
Enable IP Autonomous Switching 17-39
Control Route Cache Invalidation 17-40

Configure IP over WANs 17-40

Monitor and Maintain the IP Network 17-40
Clear Caches, Tables, and Databases 17-41
Specify the Format of Network Masks 17-41
Display System and Network Statistics 17-42
Monitor and Maintain NHRP 17-43

IP Configuration Examples 17-43
Serial Interfaces Configuration Example 17-43
Creating a Network from Separated Subnets Example 17-44
Dynamic Lookup Example 17-44
Establishing IP Domains Example 17-45
Configuring HP Hosts on a Network Segment Example 17-45
Enabling NHRP Example 17-45
NHRP on a Multipoint Tunnel Example 17-47
Router A 17-48
Router B 17-48
Router C 17-48
Router D 17-49
NHRP Over ATM Example 17-49
Helper Addresses Example 17-50
Broadcasting Examples 17-51
Flooded Broadcast Example 17-51
Flooding of IP Broadcasts Example 17-51
Customizing ICMP Services Example 17-52
Simplex Ethernet Interfaces Example 17-52
Access List Examples 17-53
Examples of Implicit Masks in Access Lists 17-53
Examples of Configuring Extended Access Lists 17-54
IPSO Configuration Examples 17-54
Ping Command Example 17-56

Chapter 18

Configuring IP Routing Protocols 18-1
Cisco's Implementation of IP Routing Protocols 18-1
Interior Gateway Protocols 18-1
Exterior Gateway Protocols 18-2
Router Discovery Protocols 18-2
Multiple Routing Protocols 18-2

IP Routing Protocols Task List 18-3

Determine a Routing Process 18-3

Configure IGRP 18-4
Cisco's IGRP Implementation 18-4
IGRP Updates 18-5

IGRP Configuration Task List 18-5
Create the IGRP Routing Process 18-5
Allow Point-to-Point Updates for IGRP 18-6
Define Unequal-Cost Load Balancing 18-6
Control Traffic Distribution 18-7
Adjust the IGRP Metric Weights 18-7
Disable Holddown 18-7
Enforce a Maximum Network Diameter 18-8
Validate Source IP Addresses 18-8

Configure Enhanced IGRP 18-8
Cisco's Enhanced IGRP Implementation 18-8
Enhanced IGRP Configuration Task List 18-10
Enable IP Enhanced IGRP 18-10
Transition from IGRP to Enhanced IGRP 18-10
Configure IP Enhanced IGRP-Specific Parameters 18-10
Define Unequal-Cost Load Balancing 18-11
Adjust the IP Enhanced IGRP Metric Weights 18-11
Disable Route Summarization 18-12
Configure Summary Aggregate Addresses 18-12
Configure Protocol-Independent Parameters 18-12
Redistribute Routing Information 18-13
Set Metrics for Redistributed Routes 18-13
Filter Routing Information 18-14
Adjust the Interval between Hello Packets and the Hold Time 18-16
Disable Split Horizon 18-16

Configure OSPF 18-17
Cisco's OSPF Implementation 18-17
OSPF Configuration Task List 18-17
Enable OSPF 18-18
Configure OSPF Interface Parameters 18-18
Configure OSPF over Different Physical Networks 18-19
Configure Your OSPF Network Type 18-19
Configure OSPF for Nonbroadcast Networks 18-20
Configure OSPF Area Parameters 18-20
Configure Route Summarization between OSPF Areas 18-20
Configure Route Summarization when Redistributing Routes into OSPF 18-21
Create Virtual Links 18-21
Generate a Default Route 18-21
Configure Lookup of DNS Names 18-22
Force the Router ID Choice with a Loopback Interface 18-22
Disable Default OSPF Metric Calculation Based on Bandwidth 18-22
Configure OSPF on Simplex Ethernet Interfaces 18-23
Configure Route Calculation Timers 18-23

Configure RIP 18-23
Running IGRP and RIP Concurrently 18-24
Validate Source IP Addresses 18-24
Allow Point-to-Point Updates for RIP 18-24

Configure IS-IS 18-25
IS-IS Configuration Task List 18-25

Enable IS-IS 18-25
Configure IS-IS Interface Parameters 18-26
Configure IS-IS Link-State Metrics 18-26
Set the Advertised Hello Interval 18-26
Set the Advertised CSNP Interval 18-27
Set the Retransmission Interval 18-27
Specify Designated Router Election 18-27
Specify the Interface Circuit Type 18-27
Assign a Password for an Interface 18-28
Configure Miscellaneous IS-IS Parameters 18-28
Generate a Default Route 18-28
Specify Router-Level Support 18-28
Configure IS-IS Authentication Passwords 18-29
Summarize Address Ranges 18-29

Configure BGP 18-29
Cisco's BGP Implementation 18-29
How BGP Selects Paths 18-30
BGP Configuration Task List 18-30
Enable BGP Routing 18-31
Configure BGP Neighbors 18-31
Reset BGP Connections 18-32
Configure BGP Route Filtering by Neighbor 18-32
Configure BGP Path Filtering by Neighbor 18-32
Configure BGP Community Filtering 18-33
Disable Next-Hop Processing on BGP Updates 18-33
Configure BGP Administrative Weights 18-34
Configure BGP Interactions with IGPs 18-34
Configure Aggregate Addresses 18-35
Specify Automatic Summarization of Network Numbers 18-35
Configure a Common Autonomous System 18-36
Configure a Routing Domain Confederation 18-36
Configure Miscellaneous BGP Parameters 18-36
Configure Neighbor Options 18-36
Set the Network Weight 18-37
Indicate Backdoor Routes 18-38
Update IP Routing Table 18-38
Set Administrative Distance 18-38
Adjust BGP Timers 18-38
Configure the MULTI_EXIT_DISC METRIC 18-39
Change the Local Preference Value 18-39
Redistribute Network 0.0.0.0 18-39

Configure EGP 18-39
Cisco's EGP Implementation 18-39
EGP Configuration Task List 18-40
Enable EGP Routing 18-40
Configure EGP Neighbor Relationships 18-40
Adjust EGP Timers 18-41
Configure Third-Party EGP Support 18-41
Configure Backup Routers 18-41
Configure Default Routes 18-41

Define a Central Routing Information Manager (Core Gateway) 18-42

Configure GDP 18-42

Configure IRDP 18-44

Configure IP Multicast Routing 18-45
Cisco's Implementation of IP Multicast Routing 18-45
Internet Group Management Protocol (IGMP) 18-45
Protocol-Independent Multicast (PIM) Protocol 18-45
IP Multicast Routing Configuration Task List 18-46
Enable IP Multicast Routing on the Router 18-46
Enable PIM on an Interface 18-47
Configure a Router to Be a Member of a Group 18-48
Configure the Host-Query Message Interval 18-48
Control Access to IP Multicast Groups 18-48
Modify PIM Message Timers 18-49
Configure the TTL Threshold 18-49
Configure DVMRP Interoperability 18-49
Advertise Network 0.0.0.0 to DVMRP Neighbors 18-50
Configure a DVMRP Tunnel 18-50

Configure Routing Protocol-Independent Features 18-51
Use Variable-Length Subnet Masks 18-51
Configure Static Routes 18-51
Specify Default Routes 18-52
Specify a Default Network 18-53
Gateway of Last Resort 18-53
Redistribute Routing Information 18-53
Supported Metric Translations 18-55
Filter Routing Information 18-55
Suppress Routing Updates through an Interface 18-56
Suppress Routes from Being Advertised in Routing Updates 18-56
Suppress Routes Listed in Updates from Being Processed 18-57
Apply Offsets to Routing Metrics 18-57
Filter Sources of Routing Information 18-57
Adjust Timers 18-58
Enable or Disable Split Horizon 18-59

Monitor and Maintain the IP Network 18-60
Clear Caches, Tables, and Databases 18-60
Display System and Network Statistics 18-60

IP Routing Protocol Configuration Examples 18-62
Variable-Length Subnet Masks Example 18-63
Overriding Static Routes with Dynamic Protocols Example 18-64
Configuring IS-IS as an IP Routing Protocol Example 18-64
Static Routing Redistribution Example 18-65
IGRP Redistribution Example 18-65
RIP and IGRP Redistribution Example 18-66
IP Enhanced IGRP Redistribution Examples 18-66
RIP and IP Enhanced IGRP Redistribution Example 18-67
IP Multicast Routing Configuration Examples 18-68
Configure a Router to Operate in Dense Mode Example 18-68

Configure a Router to Operate in Sparse Mode Example 18-68
Configure DVMRP Interoperability Examples 18-68
OSPF Routing and Route Redistribution Examples 18-69
Example 1: Basic OSPF Configuration 18-69
Example 2: Another Basic OSPF Configuration 18-70
Example 3: Internal, Area Border, and Autonomous System Boundary Routers 18-71
Example 4: Complex OSPF Configuration 18-73
BGP Route Advertisement and Redistribution Examples 18-75
Example 1: Simple BGP Route Advertisement 18-75
Example 2: Mutual Route Redistribution 18-75
Default Metric Values Redistribution Example 18-76
Route-Map Examples 18-76
Using Route Maps with BGP 18-78
IGRP Feasible Successor Relationship Example 18-80
BGP Synchronization Example 18-81
BGP Basic Neighbor Specification Examples 18-81
Using Access Lists to Specify Neighbors 18-82
BGP Aggregate Route Examples 18-83
Third-Party EGP Support Example 18-83
Backup EGP Router Example 18-84
EGP Core Gateway Example 18-84
Autonomous System within EGP Example 18-85
Passive Interface Examples 18-86
Administrative Distance Examples 18-87
Split Horizon Examples 18-88

Chapter 19

Configuring ISO CLNS 19-1
Cisco's Implementation of ISO CLNS 19-1
ISO CLNS Configuration Task List 19-2
Assign Domain Boundaries, NSAP Addresses, and Area Addresses 19-2
ISO CLNS Addressing Background 19-2
Addressing Rules 19-4
Entering Routes 19-4
Configure NETs for Domains and Areas 19-5
Assign Multiple Area Addresses to IS-IS Areas 19-6
Configure a Static NET Address for the Router 19-6
Map NSAP Addresses to Media Addresses 19-7
Specify Shortcut NSAP Addresses 19-8
Use the IP Domain Name System to Discover ISO CLNS Addresses 19-8
Configure a Routing Process 19-9
Static Routing 19-9
Dynamic Routing 19-9
Intermediate Systems and End Systems 19-10
Configure CLNS Static Routing 19-10
Configure CLNS on the Router 19-10
Assign a Static NET Address for the Router 19-10
Enable ISO CLNS for Each Interface 19-11
Enter a Specific Static Route 19-11

Configure Variations of the Clns Route Command 19-11
Configure ISO-IGRP Dynamic Routing 19-12
Adjust ISO-IGRP Metrics 19-12
Adjust ISO-IGRP Timers 19-13
Enable or Disable Split Horizon 19-13
Redistribute Routes into an ISO-IGRP Domain 19-13
Specify Preferred Routes 19-14
Configure IS-IS Dynamic Routing 19-15
Configure IS-IS Interface Parameters 19-15
Configure IS-IS Link-State Metrics 19-15
Set the Advertised Hello Interval 19-16
Set the Advertised CSNP Interval 19-16
Set the Retransmission Interval 19-16
Specify Designated Router Election 19-17
Specify the Interface Circuit Type 19-17
Configure IS-IS Password Authentication 19-17
Configure IS-IS Parameters 19-17
Redistribute Routes into an IS-IS Domain 19-18
Specify Preferred Routes 19-18
Specify Router-Level Support 19-19
Configure IS-IS Authentication Passwords 19-19

Configure ES-IS Hello Packet Parameters 19-19

Create Packet-Forwarding Filters and Establish Adjacencies 19-20

Configure CLNS over WANs 19-21

Configure Miscellaneous Features 19-21
Assign Static NSAP Addresses for an Interface 19-22
Configure DECnet OSI or Phase V Cluster Aliases 19-22
Configure Digital-Compatible Mode 19-22
Allow Security-Option Packets to Pass 19-22
Header Options 19-23

Enhance ISO CLNS Performance 19-23
Specify the MTU Size 19-23
Disable Checksums 19-24
Disable Fast Switching Through the Cache 19-24
Set the Congestion Threshold 19-24
Transmit ERPDUs 19-24
Control RDPDUs 19-25
Configure Parameters for Locally Sourced Packets 19-25

Monitor and Maintain the ISO CLNS Network 19-25

ISO CLNS Configuration Examples 19-26
Configuring NETs Examples 19-27
Basic Static Routing Examples 19-28
Static Intradomain Routing Example 19-29
Static Interdomain Routing Example 19-30
Dynamic Routing within the Same Area Example 19-31
Dynamic Routing in More Than One Area Example 19-32
Dynamic Routing in Overlapping Areas Example 19-32

Dynamic Interdomain Routing Example 19-33
IS-IS Routing Configuration Examples 19-34
Configuring a Router in Two Areas Example 19-36
Configuring ISO CLNS over X.25 Example 19-37
Customizing Performance Parameters Example 19-38
Configuring DECnet Cluster Aliases Example 19-38
Route-Map Examples 19-38
CLNS Filter Examples 19-39

Chapter 20

Configuring Novell IPX 20-1
Cisco's Implementation of Novell IPX 20-1

IPX Addresses 20-2

IPX Configuration Task List 20-2

Enable IPX Routing 20-2
Enable IPX Routing on the Router 20-3
Assign Network Numbers to Individual Interfaces 20-3
Assign Network Numbers to Interfaces That Support a Single Network 20-3
Assign Network Numbers to Interfaces that Support Multiple Networks 20-4

Configure NLSP 20-5
Define an Internal Network 20-6
Enable NLSP Routing on the Router 20-7
Configure NLSP on an Interface 20-7
Configure NLSP on a LAN Interface 20-7
Configure NLSP on a WAN Interface 20-7
Configure RIP and SAP Compatibility 20-8
Configure Maximum Hop Count 20-8
Configure the Link Delay and Throughput 20-8
Configure the Metric Value 20-9
Configure the Priority of the System for Designated Router Election 20-9
Configure Default Routes 20-9
Configure Transmission and Retransmission Intervals 20-10
Modify Link-State Packet (LSP) Parameters 20-10

Configure IPX Enhanced IGRP 20-10
IPX Enhanced IGRP Configuration Task List 20-12
Enable IPX Enhanced IGRP 20-12
Configure Miscellaneous Enhanced IGRP Parameters 20-12
Redistribute Routing Information 20-13
Adjust the Interval between Hello Packets and the Hold Time 20-13
Disable Split Horizon 20-14
Control SAP Updates 20-14
Control the Advertising of Routes in Routing Updates 20-15
Control the Processing of Routing Updates 20-15
Query the Backup Server 20-15

Control Access to IPX Networks 20-15
Create Access Lists 20-17
Create Generic Filters 20-18
Create Filters for Updating the Routing Table 20-18

Create SAP Filters 20-19
Create GNS Response Filters 20-20
Create IPX NetBIOS Filters 20-20
Create Broadcast Message Filters 20-21

Tune IPX Network Performance 20-22
Control Novell IPX Compliance 20-22
Configure Static Routes 20-23
Adjust RIP Update Timers 20-24
Configure RIP Update Packet Size 20-25
Configure Static SAP Table Entries 20-25
Configure the Queue Length for SAP Requests 20-25
Adjust SAP Update Timers 20-25
Configure SAP Update Packet Size 20-26
Set Maximum Paths 20-26
Control Responses to GNS Requests 20-27
Use Helper Addresses to Forward Broadcast Messages 20-27
Control the Forwarding of Type 20 Packets 20-28
Enable the Forwarding of Type 20 Packets 20-28
Restrict the Acceptance of Incoming Type 20 Packets 20-28
Restrict the Forwarding of Outgoing Type 20 Packets 20-29
Disable IPX Fast Switching 20-29
Enable Autonomous Switching 20-29
Enable SSE Switching 20-30
Pad Odd-Length Packets 20-30
Repair Corrupted Network Numbers 20-30

Configure IPX Accounting 20-30

Shut Down an IPX Network 20-31

Configure IPX over WANs 20-32
Configure IPX over DDR 20-32
Configure the IPXWAN Protocol 20-32

Monitor and Maintain the IPX Network 20-33

Configuration Examples 20-34
Enabling IPX Routing Example 20-34
Enabling and Disabling IPX Routing on Multiple Networks Example 20-35
Enabling and Disabling IPX Routing Protocols Examples 20-36
Enabling IPX over a WAN Interface Example 20-37
IPX over DDR Example 20-39
IPX Network Access Example 20-40
SAP Input Filter Example 20-41
SAP Output Filter Example 20-42
IPX NetBIOS Filter Examples 20-43
Helper Facilities to Control Broadcasts Examples 20-44
Forwarding to an Address Example 20-44
Forwarding to All Networks Example 20-46
All-Nets Flooded Broadcast Example 20-47
IPX Accounting Example 20-47
Enabling IPX Enhanced IGRP Example 20-48
Enhanced IGRP SAP Update Examples 20-48

Chapter 21

Configuring XNS 21-1
Cisco's Implementation of XNS 21-1
Ungermann-Bass Net/One Environments 21-1
XNS Addresses 21-2
Configuration Task List 21-3
Enable XNS Routing 21-3
Enable Standard XNS Routing 21-3
Enable Ungermann-Bass Net/One Routing 21-4
Control Access to the XNS Network 21-4
Create Access Lists 21-5
Create Generic Filters 21-6
Create Filters for Updating the Routing Table 21-6
Tune XNS Network Performance 21-7
Configure Static Routes 21-7
Set Routing Table Update Timers 21-8
Set Maximum Paths 21-8
Control Broadcast Messages 21-8
Forward Broadcast Messages to Specified Hosts 21-10
Specify XNS Protocol Types for Forwarding Broadcast Messages 21-10
Configure Flooding 21-10
Disable XNS Fast Switching 21-11
Configure XNS over WANs 21-11
Monitor the XNS Network 21-12
XNS Configuration Examples 21-12
Enabling XNS Routing Configuration Example 21-12
Enabling and Configuring Net/One Routing Configuration Example 21-13
Routing Update Timers Example 21-13
3Com Access List Example 21-14
Extended Access List with Network Mask Option Example 21-14
Helpering Example 21-14

Chapter 22

Configuring Transparent Bridging 22-1
Cisco's Implementation of Transparent and Source-Route Transparent Bridging 22-1
Transparent Bridging Features 22-1
Source-Route Transparent Bridging Features 22-2
Transparent and SRT Bridging Configuration Task List 22-3
Configure Transparent Bridging and SRT Bridging 22-3
Assign a Bridge Group Number and Define the Spanning-Tree Protocol 22-4
Assign Each Network Interface to a Bridge Group 22-4
Choose the OUI for Ethernet Type II Frames 22-5
Configure Transparently Bridged Virtual LANs 22-5

Configure Transparent Bridging over WANs 22-6
Configure X.25 Transparent Bridging 22-7
Configure Frame Relay Transparent Bridging 22-7
Bridging in a Frame Relay Network with No Multicasts 22-7
Bridging in a Frame Relay Network with Multicasts 22-8
Configure SMDS Transparent Bridging 22-8

Configure Transparent Bridging Options 22-8
Disable IP Routing 22-9
Enable Autonomous Bridging 22-9
Configure LAT Compression 22-10
Establish Multiple Spanning-Tree Domains 22-10
Prevent the Forwarding of Dynamically Determined Stations 22-11
Forward Multicast Addresses 22-11
Configure Bridge Table Aging Time 22-11

Filter Transparently Bridged Packets 22-12
Filter by MAC-Level Address 22-12
Filter by Specific MAC Address 22-13
Filter by Vendor Code 22-13
Filter by Protocol Type 22-14
Define and Apply Extended Access Lists 22-16
Filter LAT Service Announcements 22-16
Enable LAT Group Code Service Filtering 22-17
Specify Deny or Permit Conditions for LAT Group Codes on Input 22-17
Specify Deny or Permit Conditions for LAT Group Codes on Output 22-17

Adjust Spanning-Tree Parameters 22-18
Set the Bridge Priority 22-18
Set an Interface Priority 22-19
Assign Path Costs 22-19
Adjust BPDU Intervals 22-19
Adjust the Interval between Hello BPDUs 22-19
Define the Forward Delay Interval 22-20
Define the Maximum Idle Interval 22-20
Disable the Spanning Tree on an Interface 22-20

Tune the Transparently Bridged Network 22-20

Monitor and Maintain the Transparent Bridge Network 22-21

Transparent and SRT Bridging Configuration Examples 22-22
Basic Bridging Example 22-22
Transparently Bridged Virtual LANs Configuration Example 22-23
Transparent Bridging Example 22-25
Ethernet Bridging Example 22-25
SRT Bridging Example 22-27
Configuration for the New York City Router 22-27
Configuration for the Thule, Greenland Router 22-27
Multicast or Broadcast Packets Bridging Example 22-28
X.25 Transparent Bridging Example 22-28
Frame Relay Transparent Bridging Examples 22-29
Bridging in a Frame Relay Network with No Multicasts 22-30
Bridging in a Frame Relay Network with Multicasts 22-31

Complex Transparent Bridging Network Topology Example 22-31

Chapter 23

Configuring Source-Route Bridging 23-1
Source-Route Bridging Overview 23-1
Cisco's Implementation of Source-Route Bridging 23-2
SRB Configuration Task List 23-3
Configure Source-Route Bridging 23-3
Configure a Dual-Port Bridge 23-5
Configure a Multiport Bridge Using a Virtual Ring 23-6
Define a Ring Group in SRB Context 23-6
Enable SRB and Assign a Ring Group to an Interface 23-6
Configure Autonomous FDDI SRB 23-7
Enable the Forwarding and Blocking of Spanning-Tree Explorers 23-7
Enable the Automatic Spanning-Tree Function 23-8
Configure Remote Source-Route Bridging 23-9
Configure RSRB Using Direct Encapsulation 23-10
Define a Ring Group in RSRB Context 23-10
Identify the Remote Peers (Direct Encapsulation) 23-10
Enable SRB on the Appropriate Interfaces 23-11
Configure RSRB Using IP Encapsulation over an FST Connection 23-11
Set Up an FST Peer Name and Assign an IP Address 23-11
Identify the Remote Peers (FST Connection) 23-12
Enable SRB on the Appropriate Interfaces 23-12
Performance Considerations When Using FST in a Redundant Network Topology 23-12
Configure RSRB Using IP Encapsulation over a TCP Connection 23-13
Identify the Remote Peer (TCP Connection) 23-13
Enable SRB on the Appropriate Interfaces 23-14
Configure RSRB Using IP Encapsulation over a Fast-Switched TCP Connection 23-14
Identify the Remote Peer (TCP Connection) 23-14
Enable SRB on the Appropriate Interfaces 23-15
Configure RSRB Using TCP and LLC2 Local Acknowledgment 23-15
Enable LLC2 Local Acknowledgment between Two Remote Peer Bridges 23-17
Enable SRB on the Appropriate Interfaces 23-17
Enable Local Acknowledgment and Passthrough 23-18
Notes on Using LLC2 Local Acknowledgment 23-18
Configure Direct Frame Relay Encapsulation between RSRB Peers 23-19
Establish SAP Prioritization 23-19
Define a SAP Priority List 23-19
Define SAP Filters 23-20
Configure Bridging of Routed Protocols 23-20
Enable Use of the RIF 23-21
Configure a Static RIF Entry 23-21
Configure the RIF Timeout Interval 23-22
Configure Translation between SRB and Transparent Bridging Environments 23-22
Overview of SR/TLB 23-22
Enable Bridging between Transparent Bridging and SRB 23-24
Enable Translation Compatibility with IBM 8209 Bridges 23-24

Enable Token Ring LLC2-to-Ethernet Conversion 23-24
Enable 0x80d5 Processing 23-25
Enable Standard Token Ring LLC2-to-Ethernet LLC2 Conversion 23-25

Configure NetBIOS Support 23-25
Enable the Proxy Explorers Feature on the Appropriate Interface 23-26
Specify Timeout and Enable NetBIOS Name Caching 23-27
Configure the NetBIOS Cache Name Length 23-27
Enable NetBIOS Proxying 23-28
Create Static Entries in the NetBIOS Name Cache 23-28
Specify Dead-Time Intervals for NetBIOS Packets 23-28

Configure LAN Network Manager Support 23-29
How the Router Works with LNM 23-31
Configure LNM Software on the Management Stations to Communicate with the Router 23-32
Prevent LNM Stations from Modifying Router Parameters 23-32
Enable Other LRMs to Change Router/Bridge Parameters 23-33
Apply a Password to an LNM Reporting Link 23-33
Enable LNM Servers 23-33
Change Reporting Thresholds 23-34
Change an LNM Reporting Interval 23-34
Monitor LNM Operation 23-34

Secure the SRB Network 23-35
Configure NetBIOS Access Filters 23-35
Configure NetBIOS Access Filters Using Station Names 23-35
Configure Access Filters Using a Byte Offset 23-36
Configure Administrative Filters for Token Ring Traffic 23-37
Filter Frames by Protocol Type 23-37
Filter Frames by Vendor Code 23-38
Filter Input by Source Addresses 23-38
Filter Output by Source Addresses 23-38
Configure Access Expressions that Combine Administrative Filters 23-39
Configure Access Expressions 23-40
Optimize Access Expressions 23-40
Alter Access Lists Used in Access Expressions 23-41

Tune the SRB Network 23-41
Prioritize Traffic Based on SNA Local LU Addresses 23-42
Enable Class of Service 23-43
Assign a Priority Group to an Input Interface 23-43
Enable or Disable the Source-Route Fast-Switching Cache 23-43
Enable or Disable the Source-Route Autonomous-Switching Cache 23-43
Enable or Disable the SSE 23-44
Optimize Explorer Processing 23-44
Configure Proxy Explorers 23-45
Configure the Largest Frame Size 23-45

Establish SRB Interoperability with Specific Token Ring Implementations 23-45
Establish SRB Interoperability with IBM PC/3270 Emulation Software 23-46
Establish SRB Interoperability with TI MAC Firmware 23-46
Reporting Spurious Frame-Copied Errors 23-46

Monitor and Maintain the SRB Network 23-47

SRB Configuration Examples 23-48
Basic SRB with Spanning-Tree Explorers Example 23-49
SRB with Automatic Spanning-Tree Function Configuration Example 23-49
Optimized Explorer Processing Configuration Example 23-50
SRB Only Example 23-50
SRB and Routing Certain Protocols Example 23-50
Multiport SRB Example 23-52
SRB with Multiple Virtual Ring Groups Example 23-53
Autonomous FDDI SRB Configuration Example 23-53
RSRB Direct Frame Relay Encapsulation Example 23-54
RSRB Using IP Encapsulation over a TCP Connection Example 23-54
RSRB/TCP Fast Switching Configuration Example 23-55
RSRB Using IP Encapsulation over an FST Connection Example 23-55
RSRB Using All Types of Transport Methods Example 23-56
RSRB with Local Acknowledgment Example 23-57
RSRB with Local Acknowledgment and Passthrough Example 23-60
Local Acknowledgment for LLC2 Example 23-63
IP for Load Sharing over RSRB Example 23-65
Adding a Static RIF Cache Entry Example 23-66
Adding a Static RIF Cache Entry for a Two-Hop Path Example 23-66
SR/TLB for a Simple Network Example 23-67
SR/TLB with Access Filtering Example 23-68
NetBIOS Support with a Static NetBIOS Cache Entry Example 23-69
LNM for a Simple Network Example 23-69
LNM for a More Complex Network Example 23-71
NetBIOS Access Filters Example 23-72
Filtering Bridged Token Ring Packets to IBM Machines Example 23-72
Administrative Access Filters—Filtering SNAP Frames on Output Example 23-73
Creating Access Expressions Example 23-74
Access Expressions Example 23-75
Configuring Priority for Locally Terminated Token Ring Interfaces in RSRB Example 23-76
Fast Switching Example 23-77
Autonomous Switching Example 23-77
SNA Traffic Prioritization by LU Address Example 23-78

Chapter 24

Configuring STUN 24-1
Cisco’s Implementation of Serial Tunneling 24-2
The STUN Network 24-4
STUN Configuration Task List 24-5
Enable STUN 24-5
Configure SDLC Broadcast 24-5
Specify a STUN Protocol Group 24-6
Specify a Basic STUN Group 24-6
Specify an SDLC Group 24-7
Specify an SDLC Transmission Group 24-7
Create and Specify a Custom STUN Protocol 24-7
Enable STUN Interfaces and Place in STUN Group 24-8

Establish the Frame Encapsulation Method 24-8
Configure HDLC Encapsulation without Local Acknowledgment 24-8
Configure TCP Encapsulation without Local Acknowledgment 24-9
Configure TCP Encapsulation with SDLC Local Acknowledgment and Priority Queuing 24-9
Assign the Router an SDLC Primary or Secondary Role 24-10
Enable the SDLC Local Acknowledgment Feature 24-11
Establish Priority Queuing Levels 24-11

Configure STUN with Multilink Transmission Groups 24-11
Design Recommendations 24-12

Set up Traffic Priorities 24-13
Assign Queuing Priorities 24-13
Prioritize by Serial Interface Address or TCP Port 24-13
Prioritize by Logical Unit Address 24-14
Prioritize STUN Traffic over All Other Traffic 24-15

Monitor STUN Network Activity 24-15

STUN Configuration Examples 24-15
Configuring STUN Priorities Using HDLC Encapsulation Example 24-15
Configuring SDLC Broadcast Example 24-17
Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example 24-17
Configuring STUN Multipoint Implementation Using a Line-Sharing Device Example 24-19
Configuring STUN Local Acknowledgment Example 24-21
Configuring LOCADDR Priority Groups—Simple Example 24-21
Configuring LOCADDR Priority Groups for STUN Example 24-22

Chapter 25

Configuring LLC2 and SDLC Parameters 25-1
LLC2 25-1
LLC2 Configuration Task List 25-2
Control Transmission of I-Frames 25-2
Set the Maximum Number of I-Frames Received before Sending an Acknowledgment 25-3
Set the Maximum Delay for Acknowledgments 25-3
Set the Maximum Number of I-Frames Sent before Requiring Acknowledgment 25-3
Set the Number of Retries Allowed 25-3
Set the Time for Resending I-Frames 25-4
Set the Time for Resending Rejected Frames 25-4
Establish Polling Level 25-4
Set the Polling Frequency 25-4
Set the Polling Interval 25-5
Set the Transmit-Poll-Frame Timer 25-5
Set Up XID Transmissions 25-5
Set the Frequency of XID Transmissions 25-6
Set the Time for XID Retries 25-6
Monitor LLC2 Stations 25-6

SDLC 25-7
SDLC Configuration Task List 25-7
Enable the Router as a Primary or Secondary SDLC Station 25-8
Establish an SDLC Station for Frame Relay Access Support 25-8
Establish an SDLC Station for DLSw+ Support 25-8

Establish an SDLC Station for SDLLC Media Translation 25-9
Enable SDLC Two-Way Simultaneous Mode 25-9
Determine Use of Frame Rejects 25-10
Set SDLC Timer and Retry Counts 25-10
Set SDLC Frame and Window Sizes 25-10
Control the Buffer Size 25-11
Control Polling of Secondary Stations 25-11
Configure an SDLC Interface for Half-Duplex Mode 25-12
Specify the XID Value 25-12
Set the Largest SDLC I-Frame Size 25-12
Monitor SDLC Stations 25-13

Configuration Examples 25-13
LLC2 Configuration Example 25-13
SDLC Two-Way Simultaneous Mode Configuration Example 25-13
SDLC Encapsulation for Frame Relay Access Support Configuration Examples 25-14
SDLC Configuration for DLSw+ Example 25-15
Half-Duplex Configuration Example 25-15

Chapter 26

Configuring IBM Network Media Translation 26-1
SDLLC Media Translation 26-1
Virtual Token Ring Concept Implementation 26-2
Resolving Differences in LLC2 and SDLC Frame Size 26-2
Maintaining a Dynamic RIF Cache 26-3
Other Implementation Considerations 26-3
SDLLC Configuration Task List 26-3
Configure SDLLC with Direct Connection 26-3
Enable SDLLC Media Translation 26-4
Associate a SAP Value 26-4
Specify the XID Value 26-4
Initiate Connection to Token Ring Host 26-4
Configure SDLLC with RSRB 26-5
Configure RSRB Using Direct Encapsulation 26-5
Configure RSRB over FST Connection 26-6
Configure RSRB over TCP Connection 26-6
Configure SDLLC with RSRB and Local Acknowledgment 26-6
Configure SDLLC with Ethernet and Translational Bridging 26-7
Customize SDLLC Media Translation 26-7
Set the Largest LLC2 I-Frame Size 26-7
Set the Largest SDLC I-Frame Size 26-8
Increase the SDLC Line Speed 26-8
Other Customizing Considerations 26-8
Monitor SDLLC Media Translation 26-9

QLLC Conversion 26-9
Cisco's Implementation of QLLC Conversion 26-10
Comparing QLLC Conversion to SDLLC 26-12
Other Implementation Considerations 26-13
QLLC Conversion Configuration Task List 26-13
Enable QLLC Conversion on a Serial Interface 26-13
Enable QLLC Conversion on the Appropriate Serial Interfaces 26-14

Define the XID Value Associated with an X.25 Device 26-14
Enable the Router to Open a Connection to the Local Token Ring Device 26-15
Customize QLLC Conversion 26-15
Enable QLLC Local Acknowledgment for Remote Source-Route-Bridged Connections 26-15
Specify SAP Values Other Than the Default IBM SAP Values 26-16
Specify the Largest Packet That Can Be Sent or Received on the X.25 Interface 26-16
Monitor QLLC Conversion 26-17

SDLLC Configuration Examples 26-17
Example of SDLLC with Direct Connection 26-17
Example of SDLLC with Single Router Using RSRB 26-18
Example of SDLLC with RSRB (Single 3x74) 26-19
Example of SDLLC with RSRB (Multiple 3x74s) 26-21
Example of SDLLC with RSRB and Local Acknowledgment 26-23

QLLC Conversion Configuration Examples 26-24
QLLC Conversion between a Single 37x5 and a Single 3x74 Example 26-25
QLLC Conversion between a Single 37x5 and Multiple 3x74s Example 26-25
QLLC Conversion between Multiple 37x5s and Multiple 3x74s Example 26-27
QLLC Conversion between a Single 37x5 and Multiple 3x74s across an Arbitrary WAN Example 26-27
NCP and VTAM Sysgen Parameters 26-28

Chapter 27

Configuring DSPU 27-1
Cisco's Implementation of DSPU 27-1

DSPU Configuration Task List 27-3

Define DSPU Upstream Hosts 27-3

Define Downstream PUs 27-3
Explicitly Define a Downstream PU 27-3
Enable the Default PU Option 27-4

Define DSPU LUs 27-4
Dedicated LU Routing 27-4
Pooled LU Routing 27-5

Configure DSPU to Use a Data Link Control 27-5
Configure DSPU to Use Token Ring 27-5
Configure DSPU to Use RSRB 27-6
Configure DSPU to Use RSRB with Local Acknowledgment 27-7

Define the Number of Outstanding, Unacknowledged Activation RUs 27-8

Monitor DSPU Feature Status 27-8

DSPU Configuration Examples 27-8
Dedicated LU Routing Example 27-9
Pooled LU Routing Example 27-9
DSPU Configuration Example 27-10

Chapter 28

Configuring SNA Frame Relay Access Support 28-1
Cisco's Implementation of SNA Frame Relay Access 28-1

RFC 1490 Multiprotocol Encapsulation for SNA Data 28-1
Frame Relay Access Support 28-1

SNA Frame Relay Access Support Configuration Task List 28-2

Configure Frame Relay Access Support 28-2

Configure Frame Relay Access Support Congestion Management 28-3

Monitor and Maintain Frame Relay Access Support 28-3

Frame Relay Access Support Configuration Examples 28-3
LAN-Attached SNA Devices Example 28-3
SDLC-Attached SNA Devices Example 28-4

Chapter 29

Configuring IBM Channel Attach 29-1
Cisco's Implementation of IBM Channel Attach 29-1
IBM Channel Attach Hardware Requirements 29-1
IBM Channel Attach Host Software Requirements 29-2

Interface Configuration Task List 29-2

Understand the IBM Channel Attach Interface 29-2

Select the Interface 29-3

Configure IBM Channel Attach 29-3
Define the Routing Process 29-3
Assign an IP Address 29-4
Configure the IBM Channel Attach Interface 29-4
Select a Data Rate for the Parallel Channel Adapter (PCA) 29-4
Configure Other Interface Support 29-4

Select Host System Parameters 29-5
Values from the Host IOCP File 29-5
Values from the Host TCPIP File 29-7
Example of a Derived Value 29-7

Monitor and Maintain the Interface 29-8
Monitor Interface Status 29-8
Clear and Reset the Interface 29-9
Shut Down and Restart an Interface 29-9
Run CIP Interface Loopback Diagnostics 29-10

IBM Channel Attach Interface Configuration Examples 29-10
Routing Process Configuration Example 29-10
IP Address and Network Mask Configuration Example 29-10
CLAW Configuration Example 29-10
Interface Shutdown and Startup Example 29-11

Chapter 30

Configuring DLSw+ 30-1
Cisco's Implementation of DLSw: DLSw+ 30-1
DLSw Standard 30-1
DLSw+ Features and Enhancements 30-2
Modes of Operation 30-2

Improved Scalability 30-3
Performance 30-4
Enhanced Availability 30-4
DLSw+ Configuration Task List 30-5
Define a Source-Bridge Ring Group for DLSw+ 30-6
Define a DLSw+ Local Peer for the Router 30-6
Define a DLSw+ Ring List or Port List 30-7
Define a DLSw+ Bridge Group List 30-8
Define DLSw+ Remote Peers 30-8
Configure Peer-on-Demand Defaults 30-8
Configure Static Resources Exchanged in Capabilities Exchange 30-9
Configure Static Paths 30-9
Configure Duplicate Path Handling 30-9
Enable DLSw+ on the Appropriate Token Ring Interface 30-9
Enable DLSw+ on the Appropriate Ethernet Interface 30-10
Enable DLSw+ on the Appropriate SDLC Interface 30-10
Tune the DLSw+ Configuration 30-10
Monitor and Maintain the DLSw+ Network 30-10
DLSw+ Configuration Examples 30-11
DLSw+ Using TCP Encapsulation and LLC2 Local Acknowledgment—Basic Configuration Example 30-11
Notes on Using LLC2 Local Acknowledgment 30-13
DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 1 30-14
DLSw+ Using TCP Encapsulation with Local Acknowledgment—Peer Group Configuration Example 2 30-16
DLSw+ Translation between Ethernet and Token Ring Configuration Example 30-20
DLSw+ Translation between SDLC and Token Ring Media Example 30-22

LIST OF FIGURES

Figure 3-1 Using SLARP to Acquire the New Router's IP Address 3-6

Figure 3-2 Using BOOTP or RARP to Acquire the New Router's IP Address 3-7

Figure 3-3 Dynamically Resolving the New Router's IP Address-to-Host Name Mapping 3-8

Figure 3-4 Configuring a Router as a RARP Server 3-34

Figure 4-1 EXEC and Daemon Creation on a Line with No Modem Control 4-7

Figure 4-2 EXEC and Daemon Creation on a Line Configured for Continuous CTS 4-9

Figure 4-3 EXEC Creation on a Line Configured for a High-Speed Dial-up Modem 4-10

Figure 4-4 EXEC Creation on a Line Configured for Modem Callin 4-11

Figure 4-5 Daemon Creation on a Line Configured for Modem Callout 4-13

Figure 4-6 EXEC and Daemon Creation on a Line Configured for Incoming and Outgoing Calls 4-14

Figure 5-1 Communication between an SNMP Agent and Manager 5-14

Figure 5-2 Flow of Management Operations Requests, Responses, and Traps between the Manager and the Agent 5-17

Figure 6-1 Cisco 1000 Series LAN Extender Connection to a Core Router 6-25

Figure 6-2 Expanded View of Cisco 1000 Series LAN Extender Connection 6-25

Figure 6-3 LAN Extender Interface Connected to an Ethernet Network 6-26

Figure 6-4 Binding a Serial Line to a LAN Extender Interface 6-27

Figure 6-5 Packet Filtering on the LAN Extender 6-29

Figure 6-6 Packet Filtering on the Core Router 6-29

Figure 6-7 LAN Extender LEDs 6-34

Figure 6-8 IP Tunneling Terminology and Concepts 6-49

Figure 6-9 Providing Workarounds for Networks with Limited Hop Counts 6-50

Figure 6-10 Tunnel Precautions: Hop Counts 6-51

Figure 6-11 HSSI Loopback Testing 6-64

Figure 6-12 HSSI External Loopback Request 6-66

Figure 6-13 Connecting Multiprotocol Subnetworks across a Single-Protocol Backbone 6-73

Figure 6-14 Creating Virtual Private Networks across WANs 6-74

Figure 7-1 Basic ATM Environment 7-15

Figure 7-2 One or More SVCs Require a Signaling PVC 7-16

Figure 7-3 Source and Destination Routers Have Corresponding QOS Settings 7-18

Figure 7-4 Basic ATM Environment 7-26

Figure 7-5 One or More SVCs Require a Signaling PVC 7-27

Figure 7-6 Source and Destination Routers Have Corresponding QOS Settings 7-29

Figure 7-7 Fully Meshed ATM Configuration Example 7-36

Figure 7-8 Fully Meshed ATM Configuration Example 7-41
Figure 8-1 DDR Interconnection 8-2
Figure 8-2 Sample Dialer Interface Configuration 8-12
Figure 8-3 Hub-and-Spoke Configuration Using Dial-on-Demand Routing 8-18
Figure 8-4 Active and Quiet Periods in Snapshot Routing 8-19
Figure 8-5 Retry Period in Snapshot Routing 8-19
Figure 8-6 Sample Dialer String or Dialer Map Configuration 8-38
Figure 8-7 Chat Script Configuration and Function 8-39
Figure 8-8 Dial-on-Demand Routing Configuration 8-42
Figure 8-9 DTR Dialing through a PSTN 8-42
Figure 9-1 Typical Frame Relay Configuration 9-3
Figure 9-2 Using Subinterfaces to Provide Full Connectivity on a Partially Meshed Frame Relay Network 9-8
Figure 9-3 Frame Relay Switched Network 9-12
Figure 9-4 PVC Switching Configuration 9-23
Figure 9-5 Frame Relay DCE Configuration 9-24
Figure 9-6 Hybrid DTE/DCE PVC Switching 9-26
Figure 9-7 Frame Relay Switch over IP Tunnel 9-27
Figure 10-1 Configuring ISDN Access 10-2
Figure 10-2 Customer Premises and ISDN Network Boundary 10-4
Figure 11-1 Typical SMDS Configuration 11-3
Figure 11-2 Multiple Logical IP Subnet Configuration 11-13
Figure 12-1 Transporting LAN Protocols across an X.25 Public Data Network 12-15
Figure 12-2 DDN IP Address Conventions 12-32
Figure 12-3 BFE IP Address Conventions 12-32
Figure 12-4 Establishing an IP Encapsulation PVC through an X.25 Network 12-42
Figure 12-5 X.25 Tunneling Connection 12-43
Figure 12-6 Local Switching and Remote Tunneling PVCs 12-43
Figure 12-7 Example Network Topology for Switching CMNS over a PDN 12-45
Figure 12-8 Example Network Topology for Switching CMNS over a Leased Line 12-47
Figure 12-9 Parallel Serial Lines to X.25 Network 12-49
Figure 13-1 Apollo Domain Addresses 13-2
Figure 14-1 IPTalk Configuration Example 14-23
Figure 14-2 Allowed Configuration of Domain Router Connecting Two Domains 14-34
Figure 14-3 Improper Configuration of Domain Routers Connecting Two Domains 14-34

Figure 14-4 Inter•Poll Output 14-38
Figure 14-5 Nonextended AppleTalk Routing between Two Ethernet Networks 14-39
Figure 14-6 Routing in Discovery Mode 14-40
Figure 14-7 Transition Mode Topology and Configuration 14-41
Figure 14-8 Example Topology of Partially Obscured Zone 14-44
Figure 14-9 GZL and ZIP Reply Filters Sample Topology 14-45
Figure 14-10 Controlling Access to Common AppleTalk Network 14-47
Figure 14-11 Controlling Resource Access among Multiple AppleTalk Zones 14-48
Figure 14-12 Example Network Topology 14-51
Figure 14-13 AppleTalk over DDR Configuration 14-53
Figure 15-1 VINES Logical Network 15-2
Figure 15-2 VINES Simple Configuration 15-11
Figure 15-3 VINES Serverless Configuration 15-12
Figure 15-4 VINES Serverless X.25 Configuration 15-12
Figure 15-5 VINES Complex Serverless Configuration 15-13
Figure 15-6 VINES Access-List Configuration 15-14
Figure 16-1 DECnet Nodes and Areas 16-4
Figure 16-2 DECnet Cost Values 16-6
Figure 16-3 Sample Phase IV/V Network 16-18
Figure 16-4 Sample Phase IV/Phase V Network 16-19
Figure 16-5 ATG Configuration Example 16-20
Figure 17-1 No IP Classless Routing 17-5
Figure 17-2 IP Classless Routing 17-5
Figure 17-3 Next Hop Resolution Protocol (NHRP) 17-13
Figure 17-4 IP Path MTU Discovery 17-26
Figure 17-5 IP Fast Switching on the Same Interface 17-39
Figure 17-6 Creating a Network from Separated Subnets 17-44
Figure 17-7 Two Logical NBMA Networks over One Physical NBMA Network 17-46
Figure 17-8 Physical Configuration of a Sample NBMA 17-47
Figure 17-9 IP Helper Addresses 17-50
Figure 17-10 IP Flooded Broadcast 17-51
Figure 17-11 Simplex Ethernet Connections 17-52
Figure 17-12 IPSO Security Levels 17-55
Figure 18-1 Interior, System, and Exterior Routes 18-4

Figure 18-2 GDP Report Message Packet Format 18-43
Figure 18-3 Overriding Static Routes 18-64
Figure 18-4 Illustration of IS-IS Routing 18-64
Figure 18-5 Sample OSPF Autonomous System Network Map 18-71
Figure 18-6 Interface and Area Specifications for OSPF Example Configuration 18-73
Figure 18-7 Assigning Metrics for IGRP Path Feasibility 18-80
Figure 18-8 BGP Synchronization Configuration 18-81
Figure 18-9 Assigning Internal and External BGP Neighbors 18-82
Figure 18-10 Core EGP Third-Party Update Configuration Example 18-85
Figure 18-11 Router in AS 164 Peers with Router in AS 109 18-86
Figure 18-12 Filtering IGRP Updates 18-86
Figure 18-13 Disabled Split Horizon Example for Frame Relay Network 18-89
Figure 19-1 ISO-IGRP NSAP Addressing Structure 19-3
Figure 19-2 IS-IS NSAP Addressing Structure 19-3
Figure 19-3 Static Routing Illustration 19-29
Figure 19-4 CLNS X.25 Intradomain Routing 19-29
Figure 19-5 CLNS Interdomain Static Routing 19-30
Figure 19-6 CLNS Dynamic Routing within a Single Area 19-31
Figure 19-7 CLNS Dynamic Routing within Two Areas 19-32
Figure 19-8 CLNS Dynamic Interdomain Routing 19-33
Figure 19-9 ISO-IGRP Configuration 19-36
Figure 19-10 Routers Acting as DTEs and DCEs 19-37
Figure 20-1 IPX over a WAN Interface 20-37
Figure 20-2 IPX over DDR Configuration 20-39
Figure 20-3 Novell IPX Servers Requiring Access Control 20-40
Figure 20-4 SAP Input Filter 20-41
Figure 20-5 SAP Output Filter 20-42
Figure 20-6 IPX Clients Requiring Server Access through a Router 20-45
Figure 20-7 Type 2 Broadcast Flooding 20-46
Figure 20-8 IPX Accounting Example 20-47
Figure 21-1 Helper Addresses 21-15
Figure 22-1 Transparently Bridged Virtual LANs on an FDDI Backbone 22-6
Figure 22-2 Example of Basic Bridging 22-23
Figure 22-3 Ethernet Bridging Configuration Example 22-26

Figure 22-4 Example Network Configuration 22-27
Figure 22-5 Network Demonstrating Output Address List Filtering 22-28
Figure 22-6 X.25 Bridging Examples 22-28
Figure 22-7 Frame Relay Bridging Example 22-29
Figure 22-8 Bridged Subnetworks with Domains 22-32
Figure 23-1 IEEE 802.5 Token Ring Frame Format 23-1
Figure 23-2 Dual-Port Bridge 23-3
Figure 23-3 Multiple Dual-Port Bridges 23-4
Figure 23-4 Multiport Bridge Using a Virtual Ring 23-4
Figure 23-5 Autonomous FDDI SRB 23-5
Figure 23-6 Remote Source-Route Bridged Topology 23-9
Figure 23-7 LLC2 Session without Local Acknowledgment 23-16
Figure 23-8 LLC2 Session with Local Acknowledgment 23-16
Figure 23-9 RSRB Direct Frame Relay Encapsulation 23-19
Figure 23-10 Topology for Bridging Routed Protocols across a Source-Route Bridged Network 23-21
Figure 23-11 Example of a Simple SR/TLB Topology 23-22
Figure 23-12 LNM Linking to a Source-Route Bridge on Each Local Ring 23-30
Figure 23-13 LAN Network Manager Monitoring and Translating 23-31
Figure 23-14 Access Expression Example 23-39
Figure 23-15 SNA Local Address Prioritization 23-42
Figure 23-16 Dual Port Source-Route Bridge Configuration 23-49
Figure 23-17 Four-Port Source-Route Bridge 23-52
Figure 23-18 Two Virtual Rings Connected by an Actual Token Ring 23-53
Figure 23-19 RSRB Using TCP as a Transport 23-54
Figure 23-20 RSRB Using FST as a Transport 23-55
Figure 23-21 RSRB Using All Types of Transport Methods 23-57
Figure 23-22 RSRB with Local Acknowledgment—Simple Configuration 23-58
Figure 23-23 Network Topology for RSRB with Local Acknowledgment and Passthrough 23-60
Figure 23-24 RSRB with Local Acknowledgment— Complex Configuration 23-63
Figure 23-25 RSRB—Simple Reliability 23-65
Figure 23-26 Assigning a RIF to a Source-Route Bridge 23-66
Figure 23-27 Assigning a RIF to a Two-Hop Path 23-66
Figure 23-28 Example of a Simple SR/TLB Configuration 23-67
Figure 23-29 Example of a Bit-Swapped Address 23-68

Figure 23-30 Specifying a Static Entry 23-69
Figure 23-31 Router with Two Token Rings Configured as a Local Source-Route Bridge 23-70
Figure 23-32 Router with Three Token Rings Configured as a Multiport Bridge 23-71
Figure 23-33 Router Filtering Bridged Token Ring Packets to IBM Machines 23-73
Figure 23-34 Router Filtering SNAP Frames on Output 23-73
Figure 23-35 Network Configuration Using NetBIOS Access Filters 23-75
Figure 23-36 RSRB Configuration Example 23-76
Figure 24-1 IBM Network Configuration with and without STUN 24-3
Figure 24-2 Comparison of STUN in Passthrough Mode and Local Acknowledgment Mode 24-4
Figure 24-3 SDLC Broadcast across Virtual Multidrop Lines 24-5
Figure 24-4 SDLC Session without Local Acknowledgment 24-9
Figure 24-5 SDLC Session with Local Acknowledgment 24-10
Figure 24-6 Serial Link Address Prioritization 24-14
Figure 24-7 SNA LU Address Prioritization 24-14
Figure 24-8 STUN Simple Serial Transport 24-16
Figure 24-9 STUN TCP/IP Encapsulation 24-17
Figure 24-10 STUN Communication Involving a Line-Sharing Device 24-19
Figure 25-1 Two SDLC Secondary Stations Attached to a Single Serial Interface through an MSD 25-14
Figure 26-1 SNA Data Link Layer Support 26-1
Figure 26-2 SDLLC with Ethernet and Translational Bridging 26-7
Figure 26-3 SNA Data Link Layer Support. 26-9
Figure 26-4 SNA Devices Running QLLC 26-10
Figure 26-5 Router Running QLLC Conversion Feature 26-10
Figure 26-6 QLLC Conversion Running on Router with Intermediate IP Network 26-10
Figure 26-7 QLLC Conversion between a Single 37x5 and a Single 3x74 26-11
Figure 26-8 QLLC Conversion between a Single 37x5 and Multiple 3x74s across an Arbitrary WAN 26-12
Figure 26-9 SDLLC Communication between a 37x5 and a 3x74 Connected to the Same Router (Direct Connection) 26-18
Figure 26-10 SDLLC with Single Router with RSRB 26-19
Figure 26-11 SDLLC with RSRB with Single 3x74 26-20
Figure 26-12 SDLLC with RSRB (Multiple 3x74s) 26-21
Figure 26-13 SDLLC with RSRB and Local Acknowledgment 26-23
Figure 26-14 QLLC Conversion between a Single 37x5 and Multiple 3x74s 26-26
Figure 27-1 Router Acting as a DSPU Concentrator 27-2

Figure 27-2 SNA Perspective of DSPU 27-2
Figure 27-3 Dedicated LU Routing 27-9
Figure 27-4 Pooled LU Routing 27-10
Figure 28-1 Frame Relay Encapsulation Based on RFC 1490 28-1
Figure 28-2 SNA BNN Support for Frame Relay 28-2
Figure 28-3 LAN-Attached SNA Devices 28-4
Figure 28-4 SDLC-Attached SNA Devices 28-4
Figure 29-1 System with an ESCON Director Switch and a Directly Attached Channel 29-6
Figure 30-1 Scalability with DLSw+ 30-4
Figure 30-2 Enhanced Availability and Performance 30-5
Figure 30-3 DLSw+ Port List Implementation 30-7
Figure 30-4 LLC2 Session without Local Acknowledgment 30-12
Figure 30-5 LLC2 Session with Local Acknowledgment 30-12
Figure 30-6 DLSw+ with Local Acknowledgment—Simple Configuration 30-14
Figure 30-7 DLSw with Local Acknowledgment—Peer Group Configuration 1 30-15
Figure 30-8 DLSw+ with Local Acknowledgment—Peer Group Configuration 2 30-17
Figure 30-9 DLSw+ Translation between Ethernet and Token Ring Media 30-20
Figure 30-10 DLSw+ Translation between SDLC and Token Ring Media 30-22

LIST OF TABLES

Table 2-1 Summary of Command Modes 2-2

Table 2-2 Editing Keys and Functions for Software Release 9.1 and Earlier 2-26

Table 3-1 Downloading an Image and Booting from Flash 3-52

Table 5-1 Factory Diagnostic Mode Settings for the Configuration Register 5-28

Table 5-2 Protocols with Access Lists Specified by Names 5-28

Table 5-3 Protocols with Access Lists Specified by Numbers 5-28

Table 5-4 TACACS Command Comparison 5-29

Table 5-5 Error Message Logging Keywords 5-44

Table 5-6 Logging Facility Types 5-45

Table 6-1 LED Trouble Indicators 6-34

Table 8-1 ITU-T V.25bis Options 8-3

Table 8-2 Modem Script Execution 8-40

Table 8-3 System Script Execution 8-40

Table 10-1 ISDN Service Provider Switch Types 10-6

Table 11-1 Protocol Families and Types of Multicasts Needed 11-7

Table 12-1 LAPB Parameters 12-4

Table 12-2 LAPB Parameters 12-14

Table 12-3 Protocol Identification in the Call User Data Field 12-18

Table 12-4 Treatment of Standard X.25 Facilities 12-36

Table 12-5 Default Treatment of ITU-T-Specified Marker Facilities 12-37

Table 12-6 Default Treatment of Local Marker Facilities Specified for DDN or BFE X.25 12-37

Table 14-1 AppleTalk Phase 1 and Phase 2 14-3

Table 14-2 Zone and Interface Associations for Partial Zone Advertisement Example 14-45

Table 14-3 Partial Zone Advertisement Control on Network 30 14-45

Table 16-1 A Packet Exchange between Nodes A and D 16-21

Table 17-1 Reserved and Available IP Addresses 17-2

Table 17-2 Configuration Register Settings for Broadcast Address Destination 17-23

Table 17-3 Default Security Keyword Values 17-33

Table 18-1 Default Administrative Distances 18-15

Table 18-2 Default Administrative Distances 18-52

Table 18-3 Default Administrative Distances 18-58

Table 19-1 Sample Routing Table Entries 19-4

Table 19-2 Hierarchical Routing Examples 19-5

Table 20-1 Novell IPX Encapsulation Types on IEEE Interfaces 20-4

Table 20-2 IPX Filters 20-16

Table 21-1 XNS Filters 21-5

Table 26-1 QLLC and SDLLC Command Comparison 26-13

About This Manual

This section discusses the objectives, audience, organization, and conventions of the *Router Products Configuration Guide*.

Document Objectives

This publication describes the tasks necessary to configure and maintain your router. It includes task overviews, expanded descriptions of tasks, and comprehensive configuration examples. It does not provide complete command syntax descriptions, and therefore must be used in conjunction with the *Router Products Command Reference* publication.

Audience

This publication is intended primarily for network administrators who will be configuring and maintaining routers but are not necessarily familiar with the tasks involved, the relationship between them, or the commands necessary to perform particular tasks.

Document Organization

This publication is divided into six main parts. Each part comprises chapters describing related tasks or functions. The organization of parts and chapters in this publication matches the organization of parts and chapters in the *Router Products Command Reference*, except that this document does not contain appendixes. The parts in this publication are as follows:

- Part 1, “Product Introduction,” contains an overview of the router and task descriptions for the system user interface and command parser. Begin your system configuration process with this part of the manual.
- Part 2, “System and Interface Configuration and Management,” describes the tasks pertaining to booting, terminal sessions and modem lines, system management, and system interfaces. It also describes the command interpreter, or EXEC.
- Part 3, “Wide-Area Networking,” describes the tasks pertaining to ATM, DDR, Frame Relay, ISDN, SMDS, and X.25. The chapters are arranged in alphabetical order for ease of use.

- Part 4, “Routing Protocols,” contains chapters that describe how to configure each supported network protocol. These protocols include Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, ISO CLNS, Novell IPX, and XNS (including Ungermann-Bass and 3Com variations). This part also contains a chapter that discusses IP routing protocols, which include IGRP, BGP, RIP, OSPF, IS-IS, and ISO-IGRP. The chapters are arranged in alphabetical order for ease of use.
- Part 5, “Bridging,” contains chapters that describe how to configure transparent bridging, source-route bridging, source-route transparent (SRT) bridging, and source-route translational bridging (SR/TLB) on our routers.
- Part 6, “IBM Networking,” contains chapters that describe how to configure the SDLC transport and serial tunneling mechanisms in an IBM local-area network. Also included are the tasks for configuring the local acknowledgment feature, managing your source-route bridges with LAN Network Manager, and configuring SDLLC and QLLC conversion, our IBM network protocol translation features. Part 6 also contains chapters that describe how to configure SNA Downstream Physical Unit (DSPU) support and SNA Frame Relay Access Support. The IBM Channel Attach chapter describes how to configure a Channel Interface Processor (CIP).

Document Conventions

Software and hardware documentation uses the following conventions:

- The symbol ^ represents the Control key.

  For example, the key combinations ^D and Ctrl-D mean hold down the Control key while you press the D key. Keys are indicated in capitals, but are not case sensitive.

- A string is defined as a nonquoted set of characters.

  For example, when setting up a community string for SNMP to “public,” do not use quotes around the string, or the string will include the quotation marks.

Command descriptions use these conventions:

- Vertical bars (|) separate alternative, mutually exclusive, elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice.
- Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).

Examples use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating that the user enters commands at the prompt. The system prompt indicates the current command mode. For example, the prompt `router(config)#` indicates global configuration mode.
- Terminal sessions and information the system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([ ]).

- Exclamation points (!) at the beginning of a line indicate a comment line. They are also displayed by the router for certain processes.

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

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

CHAPTER 1

Router Product Overview

Computer networks that run different protocols on a variety of local-area network (LAN) media over a variety of wide-area network (WAN) technologies must be able to communicate. The Cisco Systems Internetwork Operating System (IOS) software provides this capability. The IOS software runs on internetworking platforms purchased directly from Cisco Systems and from many Cisco partners.

This chapter describes the capabilities of the IOS as implemented on router platforms. It contains the following sections:

- IOS Software Benefits
- Supported Network Protocols
- Supported IP Routing Protocols
- Supported Media
- Supported Platforms
- Configuring the Router

We provide various documents about your router. Refer to the *Documentation Roadmap* for information about the interrelationship among the various documents. For the latest information about the software, including new features added since the documentation was printed and additional caveats about using the software, refer to the release note that accompanies the software.

IOS Software Benefits

The IOS software supports users and applications throughout the enterprise and provides security and data integrity for the internetwork. The IOS software cost-effectively manages resources by controlling and unifying complex, distributed network intelligence. It also functions as a flexible vehicle for adding new services, features, and applications to the internetwork.

The IOS software provides four types of internetwork benefits, which are described in the following sections:

- Reliable, Adaptive Routing
- WAN Optimization
- Management and Security
- Scalability

Reliable, Adaptive Routing

The IOS software is reliable and adaptive because it identifies the best paths and routes traffic around network failures. It also reduces costs by efficiently using network bandwidth and resources while eliminating needless management of static routes.

Policy-based IOS features such as route filtering and routing information translatability save network resources by preventing data from being unnecessarily broadcast to nodes that do not require it. Priority output queuing and custom queuing grant priority to important sessions when network bandwidth is saturated. Load balancing makes use of all available paths across the internetwork, preserving valuable bandwidth and improving performance. The IOS software also provides the most effective and efficient scaling available for network applications that require transparent or source-route bridging algorithms.

Increasingly, internetworks are incorporating new technologies such as Asynchronous Transfer Mode (ATM) and LAN switching. Through CiscoFusion, Cisco's scalable architecture for switched internetworks, the IOS software provides the framework for a new technology called multilayer switching, which fuses the ease of switching solutions with the power of routed solutions.

By distributing routing intelligence and switching functions to create "virtual LANs," CiscoFusion's multilayer switching increases bandwidth while simplifying moves, additions, and changes across the enterprise. This extends the power and flexibility of the IOS beyond internetwork routers to include the ATM and LAN switches that are increasingly being deployed throughout today's internetworks.

WAN Optimization

Because most network costs are expended on WAN switching and usage functions, an effective internetwork must optimize all WAN-related operations. Optimization increases network throughput while reducing delay time. It also minimizes costs by eliminating unnecessary traffic and intelligently selecting the most economical WAN links available.

The IOS software seamlessly accommodates circuit-switched services such as Integrated Services Digital Network (ISDN), switched T1, and dial-up telephone lines. IOS software innovations such as dial-on-demand access and dial backup capabilities provide cost-effective alternatives to point-to-point switched leased lines. Support for advanced, packet-switched services such as X.25, Frame Relay, Switched Multimegabit Data Service (SMDS), and ATM extends the internetwork across the broad range of WAN interface alternatives now available.

Management and Security

The IOS software provides an array of network management and security capabilities designed to meet the needs of today's large, complex internetworks. Integrated management simplifies administrative procedures and shortens the time required to diagnose and fix problems. Automated operations reduce hands-on tasks and make it possible to manage large, geographically dispersed internetworks with a small staff of experts located at a central site.

The IOS software provides several important management features that are built into every Cisco router. These include configuration services that lower the cost of installing, upgrading, and reconfiguring routers, as well as comprehensive monitoring and diagnostic services. In addition, the IOS software provides valuable information and services to router management applications developed by Cisco and its partners. The Cisco applications, known collectively as CiscoWorks, offer administrators a wide-ranging suite of operational, design, and management capabilities that increase productivity and reduce costs.

The IOS management services are matched by their security capabilities. The IOS software includes a diverse tool kit for partitioning resources and prohibiting access to sensitive or confidential information or processes. Multidimensional filters prevent users from knowing that other users or resources are even on the network. Encrypted passwords, dial-in authentication, multilevel configuration permissions, and accounting and logging features provide protection from—and information about—unauthorized access attempts.

Scalability

Scalability provides the flexibility required to address all of the key issues facing internetworks as organizations evolve. The IOS software's scalable routing protocols help avoid needless congestion, overcome inherent protocol limitations, and bypass many of the obstacles that can arise because of the scope and geographical dispersion of an internetwork.

The IOS software also helps to cut costs by reducing network bandwidth and processing overhead, off-loading servers and conserving resources, and easing system configuration tasks. Advanced IOS features such as filtering, protocol termination and translation, smart broadcasts, and helper address services combine to create a flexible, scalable infrastructure that can keep pace with evolving network requirements.

Supported Network Protocols

IOS software supports many networking protocols, as well as their associated routing protocols. These protocols are based on both open standards and proprietary protocols from a variety of vendors. The IOS software also supports a wide set of bridging and IBM connectivity solutions.

The IOS software can receive and forward packets concurrently from any combination of the following:

- WAN protocols
  - Asynchronous Transfer Mode (ATM)
  - Frame Relay
  - High-Level Data Link Control (HDLC)
  - Integrated Services Digital Networks (ISDN)
  - Point-to-Point Protocol (PPP)
  - Serial Line Internet Protocol (SLIP)—for asynchronous lines
  - Switched Multimegabit Data Service (SMDS)
  - X.25 and its derivatives, including Link Access Procedure, Balanced (LAPB) and Defense Data Network (DDN) X.25
- Network protocols
  - Apollo Domain
  - AppleTalk (Phase 1 and Phase 2)
  - Banyan VINES
  - DECnet Phase IV, Phase IV Prime, and Phase V
  - Internet Protocol (IP)
  - ISO Connectionless Network Services (CLNS) and Connection Mode Network Services (CMNS)

  - Novell IPX
  - Xerox Network Systems (XNS) and two variations developed by Ungermann-Bass and 3Com
- Bridging types
  - Transparent bridging and source-route transparent (SRT) bridging
  - Source-route bridging (SRB) and remote source-route bridging (RSRB)
  - Source-route translational bridging (SR/TLB)
- Support for IBM networking
  - Serial tunnel (STUN)
  - Logical Link Control, type 2 (LLC2) and Synchronous Data Link Control (SDLC)
  - SDLLC media translation—A software feature that translates between LLC2 and Synchronous Data Link Control (SDLC)
  - Qualified Logical Link Control (QLLC) conversion
  - IBM Channel Attach

These protocols, bridging, and IBM networking topics are described in separate chapters of this manual. For background information, refer to the *Internetworking Technology Overview* publication.

Supported IP Routing Protocols

The IOS software supports the following IP routing protocols:

- Interior Gateway Protocols
  - Internet Gateway Routing Protocol (IGRP)
  - Enhanced IGRP
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
  - Intermediate System-to-Intermediate System (IS-IS)
- Exterior Gateway Protocols
  - Border Gateway Protocol (BGP)
  - Exterior Gateway Protocol (EGP)
- Router Discovery Protocols
  - ICMP Router Discovery Protocol (IRDP)
  - Hot Standby Router Protocol (HSRP)

The “Configuring IP Routing Protocols” chapter in this manual describes these protocols in detail.

Supported Media

Our routers support the following industry-standard networking media:

- Asynchronous serial
- Channelized T1
- Ethernet—IEEE 802.3 and Type II
- Fiber Distributed Data Interface (FDDI)—single and dual mode
- High-Speed Serial Interface (HSSI)—Supports T1, T3, E3, and SONET rates
- ISDN Basic Rate Interface (BRI) and Multiport BRI (MBRI)
- ISDN Primary Rate Interface (PRI)
- Synchronous serial—V.35, RS-232, RS-449, RS-530, X.21, and G.703
- Token Ring—IEEE 802.5

These media are described briefly in the "Configuring Interfaces" chapter of this manual. For additional information, refer to the *Internetworking Technology Overview* publication.

Supported Platforms

The IOS software runs on a variety of Cisco internetworking devices and partners' platforms. For details on the supported platforms, refer to the *Cisco Systems Products Catalogue*.

Configuring the Router

The following sections describe alternative mechanisms for configuring a router:

- Using Cisco Configuration Builder
- Using the Command Interpreter

Using Cisco Configuration Builder

Cisco's Configuration Builder lets you create configuration files for multiple routers without knowing the router command-line language or syntax. It is a Microsoft Windows-based application that runs on an IBM PC or compatible computer.

To use Configuration Builder, refer to the *Cisco Configuration Builder Getting Started Guide*.

If you do not have the platform to run Configuration Builder, configure your router using the command interpreter, as described in the next section.

Using the Command Interpreter

This manual set describes how to use the command interpreter. You can build most straightforward router configurations and create a configuration file using the **setup** facility. This facility is described in the *Router Products Getting Started Guide*.

In order to configure your router, you must decide the following:

- What network protocols you are supporting (for example, AppleTalk, IP, Novell IPX, and so on)
- Your addressing plan for each network protocol

- What WAN protocols you will run on each interface (for example, Frame Relay, HDLC, SMDS, X.25, and so on)
- What routing protocol you will use for each network protocol

The *Router Products Getting Started Guide* contains worksheets to help you plan your router configuration.

To enhance the configuration, perform the protocol-specific tasks described in the appropriate chapters of this manual.

The router software provides a user interface called a command interpreter, or EXEC, that lets you configure and manage the router. This user interface also provides context-sensitive help. The command interpreter has several command modes, each of which provides a group of related commands that you can use to configure the router and display its status. Some commands are available to all users; others can be executed only after the user enters an enabling password. Context-sensitive help gives information about command syntax. The command interpreter and its help feature are described in the "Understanding the User Interface" chapter of this manual.

You use the command interpreter (also known as the command-line parser) to configure interfaces, terminal sessions, and asynchronous communications lines. Interfaces are connections to network media, such as Ethernet, Token Ring, and serial media. You configure them to run different routing protocols and other networking protocols. You configure terminal sessions and modems connected to the router so that other network users can log in to the router. Configuring terminal sessions and asynchronous communications lines is discussed in the "Configuring Terminal Lines and Modem Support" chapter. Configuring interfaces is described in the "Configuring Interfaces" chapter; the routing, bridging, and IBM protocols you can configure on these interfaces are described in the protocol-specific chapters.

You also can configure and manage the router itself, performing such tasks as naming the router, setting the router's time, configuring SNMP, and setting security. These tasks are described in the "Managing the System" chapter.

CHAPTER 2

Understanding the User Interface

The Internetwork Operating System (IOS) user interface provides access to several different command modes. Each command mode provides a group of related commands. This chapter describes how to access and list the commands available in each command mode, and explains the primary uses for each command mode.

For security purposes, the IOS provides two levels of access to commands: *user* and *privileged*. The unprivileged, user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode, and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.

From the privileged level, you can access global configuration mode and ten specific configuration modes: interface, subinterface, controller, hub, map-list, map-class, line, router, ipx-router, and route-map configuration. In addition, if your router does not find a valid system image, or if its configuration file is corrupted at startup, the system might enter read-only memory (ROM) monitor mode. Entering a question mark **(?**) at the system prompt allows you to obtain a list of commands available for each command mode.

Almost every system configuration command also has a **no** form. In general, use the **no** form to disable a feature or function. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. Specify the command **no ip routing** to disable IP routing and specify **ip routing** to reenable it. The *Router Products Command Reference* publication provides the complete syntax for every router configuration command and describes what the **no** form of a command does.

The user interface also provides context-sensitive help on command syntax. This chapter describes how to use the help system. It also describes the command editing and command history features that enable you to recall previous command entries and easily edit command entries.

For a complete description of the commands mentioned in this chapter, refer to the "User Interface Commands" chapter in the *Router Products Command Reference* publication.

User Interface Task List

You can perform the tasks in the following sections to become familiar with the IOS user interface:

- Access Each Command Mode
- Get Context-Sensitive Help
- Check Command Syntax
- Use the Command History Features
- Use the Editing Features

- Check Command Syntax

Access Each Command Mode

This section describes how to access each of the IOS command modes:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Subinterface Configuration Mode
- Controller Configuration Mode
- Hub Configuration Mode
- Map-List Configuration Mode
- Map-Class Configuration Mode
- Line Configuration Mode
- Router Configuration Mode
- IPX-Router Configuration Mode
- Route-Map Configuration Mode
- ROM Monitor Mode

Table 2-1 lists the command modes, how to access each mode, the prompt you will see while you are in that mode, the main uses for each configuration mode, and the method to exit that mode. The prompts listed assume the default router name "Router." Table 2-1 might not include all of the possible ways to access or exit each command mode.

Table 2-1 Summary of Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in to router.	`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 exit into global configuration mode, use the **configure** privileged EXEC command.
Global configuration	From privileged EXEC mode, use the **configure** privileged EXEC command.	`Router(config)#`	To exit to privileged EXEC mode, use the **exit** or **end** command or press Ctrl-Z. To exit to 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, press Ctrl-Z. To exit to subinterface configuration mode, specify a subinterface with the **interface** command.

Command Mode	Access Method	Prompt	Exit Method
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 exit to privileged EXEC mode, press Ctrl-Z.
Controller configuration	From global configuration mode, use the **controller** command to configure a channelized T1 interface.	`Router(config-controller)#`	To exit to global configuration mode, use the **exit** command.
Hub configuration	From global configuration mode, enter by specifying a hub with the **hub** command.	`Router(config-hub)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, press Ctrl-Z.
Map-list configuration	From global configuration mode, define a map list with the **map-list** command.	`Router(config-map-list)#`	To exit to map-class configuration mode, use the **map-class** command. To exit to privileged EXEC mode, press Ctrl-Z.
Map-class configuration	From global configuration mode, configure a map class with the **map-class** command.	`Router(config-map-class)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, press Ctrl-Z.
Line configuration	From global configuration mode, enter by specifying a line with a **line** command.	`Router(config-line)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, press Ctrl-Z.
Router configuration	From global configuration mode, enter by entering a command that begins with **router** (such as **router igrp)**.	`Router(config-router)#`	To exit to global configuration mode, use **exit** command. To exit to privileged EXEC mode, press Ctrl-Z.
IPX-router configuration	From global configuration mode, enter by issuing the **ipx routing** command, then a command that begins with **ipx router** (such as **ipx router eigrp**).	`Router(config-ipx-router)#`	To exit to global configuration mode, use the **exit** command.
Route-map configuration	From global configuration mode, enter by specifying the **route-map** command.	`Router(config-route-map)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, press Ctrl-Z.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press Break during the first 60 seconds while the system is booting.	`>`	To exit to user EXEC mode, press **c** to continue.

User EXEC Mode

After you log in to the router, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote routers, change terminal settings on a temporary basis, perform basic tests, and list system information.

To list the user EXEC commands, complete the following task:

Task	Command
List the user EXEC commands.	**?**

The user-level prompt consists of the router's host name followed by the angle bracket (>):

```
Router>
```

The default host name is `Router` unless it has been changed during initial configuration using the **setup** command. (Refer to the *Router Products Getting Started Guide* for information on the **setup** facility.) You can also change the router name using the **hostname global configuration** command described in the "System Management Commands" chapter in the *Router Products Command Reference* publication.

To list the commands available in user EXEC mode, enter a question mark (?) as shown in the following example:

```
Router> ?
Exec commands:
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from the EXEC
 help             Description of the interactive help system
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from the EXEC
 name-connection  Name an existing telnet connection
 ping             Send echo messages
 resume           Resume an active telnet connection
 show             Show running system information
 systat           Display information about terminal lines
 telnet           Open a telnet connection
 terminal         Set terminal line parameters
 where            List active telnet connections
Router>
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which you can access the remaining command modes. Privileged EXEC mode also includes high-level testing commands, such as **debug**. For details on the **debug** command, see the *Debug Command Reference* publication.

To access and list the privileged EXEC commands, complete the following tasks:

Task		Command
Step 1	Enter the privileged EXEC mode.	**enable** [*password*]
Step 2	List privileged EXEC commands.	**?**

If the system administrator has set a password, you are prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. The system administrator uses the **enable password global config**uration command to set the password that restricts access to privileged mode. This command is described in the "System Management Commands" chapter in the *Router Products Command Reference* publication.

The privileged-level prompt consists of the router's host name followed by the pound sign (#). (If the router was named with the **hostname** command, that name would appear as the prompt instead of "Router.")

```
Router#
```

The following example shows how to access privileged EXEC mode and list privileged EXEC commands:

```
Router> enable
Password:
Router# ?
Exec commands:
 bfe              For manual emergency modes setting
 clear            Reset functions
 clock            Manage the system clock
 configure        Enter configuration mode
 connect          Open a terminal connection
 copy             Copy a config file to or from a tftp server
 debug            Debugging functions
 disable          Turn off privileged commands
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from the EXEC
 help             Description of the interactive help system
 llc2             Execute llc2 tests
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from the EXEC
 name-connection  Name an existing telnet connection
 ping             Send echo messages
 reload           Halt and perform a cold restart
 resume           Resume an active telnet connection
 send             Send a message to other tty lines
 setup            Run the SETUP command facility
 show             Show running system information
 systat           Display information about terminal lines
 telnet           Open a telnet connection
 terminal         Set terminal line parameters
 test             Test subsystems, memory, and interfaces
 trace            Trace route to destination
 where            List active telnet connections
 which-route      Do route table lookup and display results
 write            Write running configuration to memory, network, or terminal
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

From the privileged level, you can access global configuration mode. For instructions, see the "Global Configuration Mode" section, which follows this section.

To return from privileged EXEC mode to user EXEC mode, perform the following task:

Task	Command
Move from privileged EXEC mode to user EXEC mode.	**disable**

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. When you enter this command, the EXEC prompts you for the source of the configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

You can then specify either the terminal, nonvolatile memory (NVRAM), or a file stored on a network server as the source of configuration commands (see the "System Image, Microcode Image, and Configuration File Load Commands" chapter in the *Router Products Command Reference* publication). The default is to enter commands from the terminal console. Pressing the Return key begins this configuration method.

Commands to enable a particular routing or bridging function are also global configuration commands. For information on protocol-specific global configuration commands, see the appropriate chapter in this guide.

To access and list the global configuration commands, complete the following tasks:

Task		Command
Step 1	At the terminal, from the privileged EXEC mode, enter global configuration mode.	**configure**[1] <CR>
Step 2	List the global configuration commands.	**?**

1. This command is documented in the "System Image, Microcode Image, and Configuration File Load Commands" chapter in the *Router Products Command Reference* publication.

The following example shows how to access global configuration mode and list global configuration commands:

```
Router# configure
Configuring from terminal, memory, or network [terminal]? <CR>
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ?
Configure commands:
 access-list            Add an access list entry
 apollo                 Apollo global configuration commands
 appletalk              Appletalk global configuration commands
 arp                    Set a static ARP entry
 async-bootp            Modify system bootp parameters
 autonomous-system      Specify local AS number to which we belong
 banner                 Define a login banner
 boot                   Modify system boot parameters
 bridge                 Transparent bridging
 buffers                Adjust system buffer pool parameters
 busy-message           Display message when connection to host fails
 chat-script            Define a modem chat script
 clns                   Global CLNS configuration subcommands
 clock                  Configure time-of-day clock
 decnet                 Global DECnet configuration subcommands
 default-value          Default character-bits values
 dialer-list            Create a dialer list entry
 enable                 Modify enable password parameters
 end                    Exit from configure mode
 exit                   Exit from configure mode
 frame-relay            Global frame relay configuration commands
 help                   Description of the interactive help system
 hostname               Set system's network name
 interface              Select an interface to configure
 ip                     Global IP configuration subcommands
 ipx                    Novell/IPX global configuration commands
```

```
line                    Configure a terminal line
lnm                     IBM Lan Manager
locaddr-priority-list   Establish queueing priorities based on LU address
logging                 Modify message logging facilities
login-string            Define a host-specific login string
mop                     The DEC MOP Server
netbios                 NETBIOS access control filtering
no                      Negate a command or set its defaults
ntp                     Configure NTP
priority-list           Build a priority list
queue-list              Build a custom queue list
rif                     Source-route RIF cache
route-map               Create route-map or enter route-map command mode
router                  Enable a routing process
scheduler-interval      Maximum interval before running lowest priority process
service                 Modify use of network based services
smt-queue-threshold     Set the max number of unprocessed SMT frames
snmp-server             Modify SNMP parameters
source-bridge           Source-route bridging ring groups
stun                    STUN global configuration commands
tacacs-server           Modify TACACS query parameters
tftp-server             Provide TFTP service for netload requests
tn3270                  tn3270 configuration command
username                Establish User Name Authentication
vines                   Vines global configuration commands
x25                     X.25 Level 3
xns                     XNS global configuration commands
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands:

Task	Command
Exit global configuration mode.	**exit** **end** **Ctrl-Z**

From global configuration mode, you can access ten configuration modes: interface, subinterface, hub, controller, map-list, map-class, line, router, ipx-router, and route-map configuration commands. These command modes are described in the following sections.

Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as **bandwidth**, clock rate, and so on, see the "Configuring Interfaces" chapter. For protocol-specific commands, see the appropriate chapter in this guide.

To access and list the interface configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, enter interface configuration mode.	**interface** *interface-type interface-number*[1]

Task	Command
Step 2 List the interface configuration commands.	**?**

1. This command is documented in the "Interface Commands" chapter in the *Router Products Command Reference* publication.

In the following example, serial interface 0 is about to be configured. The new prompt `Router(config-if)#` indicates interface configuration mode. In this example, the user asks for help by requesting a list of commands.

```
Router(config)# interface serial 0 <CR>
Router(config-if)# ?
Interface configuration commands:
 access-expression     Build a bridge boolean access expression
 apollo                Apollo interface subcommands
 appletalk             Appletalk interface subcommands
 arp                   Set arp type (arpa, probe, snap) or timeout
 backup                Modify dial-backup parameters
 bandwidth             Set bandwidth informational parameter
 bridge-group          Transparent bridging interface parameters
 clns                  CLNS interface subcommands
 clockrate             Configure serial interface clock speed
 custom-queue-list     Assign a custom queue list to an interface
 decnet                Interface DECnet config commands
 delay                 Specify interface throughput delay
 description           Interface specific description
 dialer                Dial-on-demand routing (DDR) commands
 dialer-group          Assign interface to dialer-list
 down-when-looped      Force looped serial interface down
 encapsulation         Set encapsulation type for an interface
 ethernet-transit-oui  Token-ring to Ethernet OUI handling
 exit                  Exit from interface configuration mode
 frame-relay           Set frame relay parameters
 hdh                   Set HDH mode
 help                  Description of the interactive help system
 hold-queue            Set hold queue depth
 ip                    Interface Internet Protocol config commands
 ipx                   Novell interface subcommands
 isis                  IS-IS commands
 iso-igrp              ISO-IGRP interface subcommands
 keepalive             Enable keepalive
 lapb                  X.25 Level 2 parameters (Link Access Procedure, Balanced)
 llc2                  LLC2 Interface Subcommands
 lnm                   IBM Lan Manager
 locaddr-priority      Assign a priority group
 loopback              Configure internal loopback on an interface
 mac-address           Manually set interface MAC address
 mop                   DEC MOP server commands
 mtu                   Set the interface Maximum Transmission Unit (MTU)
 netbios               Use a defined NETBIOS access list or enable name-caching
 no                    Negate a command or set its defaults
 ntp                   Configure NTP
 ppp                   Point-to-point protocol
 priority-group        Assign a priority group to an interface
 pulse-time            Enables pulsing of DTR during resets
 pup                   PUP interface subcommands
 sdlc                  SDLC commands
 sdllc                 Configure SDLC to LLC2 translation
 shutdown              Shutdown the selected interface
 smds                  Modify SMDS parameters
 source-bridge         Configure interface for source-route bridging
 stun                  STUN interface subcommands
 transmit-interface    Assign a transmit interface to a receive-only interface
```

```
transmitter-delay     Set dead-time after transmitting a datagram
tunnel                protocol-over-protocol tunneling
tx-queue-limit        Configure card level transmit queue limit
vines                 Vines interface subcommands
xns                   XNS interface subcommands
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

To exit interface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

Subinterface Configuration Mode

You can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. This feature is supported on serial interfaces with Frame Relay encapsulation.

Subinterfaces appear to be distinct physical interfaces to the various protocols. For example, Frame Relay networks provide multiple point-to-point links called permanent virtual circuits (PVCs). PVCs can be grouped under separate subinterfaces that in turn are configured on a single physical interface. From a bridging spanning-tree viewpoint, each subinterface is a separate bridge port, and a frame arriving on one subinterface can be sent out on a another subinterface.

Subinterfaces also allow multiple encapsulations for a protocol on a single interface. For example, a router can receive an ARPA-framed IPX packet and forward the packet back out the same physical interface as a SNAP-framed IPX packet.

For detailed information on how to configure subinterfaces, see the “Configuring Interfaces” chapter, later in this publication.

To access and list the subinterface configuration commands, complete the following tasks:

Task		Command
Step 1	From interface configuration mode, configure a virtual interface.	See the example that follows. For a list of all interface commands that allow subinterface implementation, see the “Configuring Interfaces” chapter.
Step 2	List the subinterface configuration commands.	**?**

In the following example, a subinterface is configured for serial line 2, which is configured for Frame Relay encapsulation. The subinterface is called 2.1 to indicate that it is subinterface 1 of serial interface 2. The new prompt `Router(config-subif)#` indicates subinterface configuration mode. The subinterface can be configured to support one or more Frame Relay PVCs. To list the commands available in subinterface configuration mode, enter a question mark (**?**).

```
Router(config)# interface serial 2
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 2.1
Router(config-subif)# ?
Interface configuration commands:
 apollo        Apollo interface subcommands
 appletalk     Appletalk interface subcommands
 bandwidth     Set bandwidth informational parameter
 bridge-group  Transparent bridging interface parameters
 clns          CLNS interface subcommands
 decnet        Interface DECnet config commands
 delay         Specify interface throughput delay
 description   Interface specific description
 exit          Exit from interface configuration mode
```

```
frame-relay   Set frame relay parameters
ip            Interface Internet Protocol config commands
ipx           Novell interface subcommands
isis          IS-IS commands
iso-igrp      ISO-IGRP interface subcommands
no            Negate a command or set its defaults
ntp           Configure NTP
shutdown      Shutdown the selected interface
```

The list of commands might vary slightly from this example depending upon how your router has been configured.

To exit subinterface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

Controller Configuration Mode

You can configure channelized T1 interfaces in the controller configuration mode.

To access and list the controller configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, configure a channelized T1 interface.	**controller t1** *slot*/*port* [1]
Step 2	List the controller configuration commands.	**?**

1. This command is documented in the "Interface Commands" chapter in the *Router Products Command Reference* publication.

In the following example, a channelized T1 interface is being configured on interface 0/0. The new prompt `Router(config-controller)#` indicates controller configuration mode.

```
Router(config)# controller t1 0/0
Router(config-controller)# ?
Controller configuration commands:
  channel-group  Specify the timeslots to channel-group mapping for an
                 interface
  clocksource    Specify the clock source for a DS1 link
  exit           Exit from controller configuration mode
  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
  shutdown       Shut down a DS1 link (send Blue Alarm)
```

Note The controller configuration mode applies only to the Cisco 7000 series MultiChannel Interface Processor (MIP) that has one or two CxBus Channelized T1 (CxCT1) port adaptor modules attached.

Hub Configuration Mode

Hub configuration commands configure hub functionality for an Ethernet interface on the Cisco 2500. They always follow a **hub** global configuration command. To access and list the **hub** configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, use the **hub** command.	**hub** *number port* [*port*] [1]
Step 2	List the hub configuration commands.	**?**

1. This command is documented in the "Interface Configuration Commands" chapter in the *Router Products Command Reference* publication.

The following example shows how to enter **hub** configuration mode and list the hub configuration commands. In this example, the new prompt `Router(config-hub)#` indicates hub configuration mode.

```
Router (config)# hub ethernet 0 1 3
Router(config-hub)# ?
Hub configuration commands:
  auto-polarity   Enable automatic receiver polarity reversal
  exit            Exit from hub configuration mode
  help            Description of the interactive help system
  link-test       Enable Link Test Function of Hub port
  no              Negate or set default values of a command
  shutdown        Shutdown the selected port
  source-address  Enable Source Address control for Hub port
```

To exit hub configuration mode and return to global configuration mode, enter the **exit** command. To exit configuraton mode an return to privileged EXEC mode, pres Ctrl-Z.

Map-List Configuration Mode

The Asynchronous Transfer Mode (ATM) interface in the Cisco 7000 series router supports a static mapping scheme that identifies the ATM address of remote hosts or routers.

Map-list configuration commands configure a map list. They always follow a **map-list** global configuration command. To access and list the map list configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, use the **map-list** command.	**map-list** *name* [1]
Step 2	List the map-list configuration commands.	**?**

1. This command is documented in the "ATM Configuration Commands" chapter in the *Router Products Command Reference* publication.

The following example shows how to enter map-list configuration mode and list the map list configuration commands. In this example, the static map-list configuration commands are listed. The new prompt `Router(config-map-list)#` indicates map-list configuration mode.

```
Router(config)# map-list atm
Router(config-map-list)# ?
Static maps list configuration commands:
  A.B.C.D             Protocol specific address
  aarp                AppleTalk ARP
  apollo              Apollo Domain
```

```
appletalk           AppleTalk
arp                 IP ARP
bridge              Bridging
clns                ISO CLNS
clns_es             ISO CLNS End System
clns_is             ISO CLNS Intermediate System
cmns                ISO CMNS
compressedtcp       Compressed TCP
decnet              DECnet
decnet_node         DECnet Node
decnet_prime_router DECnet Prime Router
decnet_router       DECnet Router
exit-class          Exit from static map class configuration mode
help                Description of the interactive help system
ip                  IP
ipx                 Novell IPX
no                  Negate or set default values of a command
pad                 PAD links
rsrb                Remote Source-Route Bridging
stun                Serial Tunnel
vines               Banyan VINES
xns                 Xerox Network Services
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

To exit map-list configuration mode and return to global configuration mode, enter the **exit** command. To exit configuraton mode an return to privileged EXEC mode, pres Ctrl-Z.

Map-Class Configuration Mode

The ATM interface allows you to specify Quality of Service (QOS) parameters that control how much traffic the source router will be sending over a switched virtual circuit (SVC).

To define QOS parameters that are associated with a static map for an SVC, use the **map-class** global configuration command.

Task		Command
Step 1	From global configuration mode, configure a map class.	**map-class encapsulation class-name**[1]
Step 2	List the map-class configuration commands.	**?**

1. This command is documented in the "ATM Configuration Commands" chapter in the *Router Products Command Reference* publication.

In the following example, the static map-class configuration commands are listed. The new prompt `Router(config-map-class)#` indicates map-class configuration mode.

```
Router(config)# map-class atm aaa
Router(config-map-class)# ?
Static maps class configuration commands:
atm         Configure atm static map class
exit-class  Exit from static map class configuration mode
help        Description of the interactive help system
no          Negate or set default values of a command
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

To exit map-class configuration mode and return to global configuration mode, enter the **exit** command. To exit configuraton mode an return to privileged EXEC mode, press Ctrl-Z.

Note The static mapping configuration mode applies only to the Cisco 7000 series router.

Line Configuration Mode

Line configuration commands modify the operation of a serial terminal line. Line configuration commands always follow a **line** command, which defines a line number. These commands are generally used to connect to remote routers, change terminal parameter settings on a line-by-line basis, and set up the auxiliary port modem configuration to support dial-on-demand routing (DDR) (see the "DDR Commands" chapter in the *Router Products Command Reference publicatio*n).

To access and list the auxiliary port, console port, and virtual terminal line configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, configure an auxiliary, console, or virtual terminal line.	**line** {**aux** | **con** | **vty**} *line-number* [*ending-line-number*][1]
Step 2	List the line configuration commands.	**?**

1. This command is documented in the "Terminal Lines and Modem Support Commands" chapter in the *Router Products Command Reference* publication.

The following example shows how to enter line configuration mode for virtual terminal line 3 and list the line configuration commands. The new prompt `Router(config-line)#` indicates line configuration mode.

```
Router(config)# line vty 3 <CR>
Router(config-line)# ?
Line configuration commands:
 access-class            Filter connections based on an IP access list
 activation-character    Define the activation character
 autobaud                Set line to autobaud
 autocommand             Automatically execute an EXEC command
 autohangup              Automatically hangup when last connection closes
 autohost                Automatically connect to a host
 cts-required            Require CTS on line
 data-character-bits     Size of characters being handled
 databits                Set number of data bits per character
 disconnect-character    Define the disconnect character
 dispatch-character      Define the dispatch character
 dispatch-timeout        Set the dispatch timer
 editing                 Enable command line editing
 escape-character        Change the current line's escape character
 exec                    Start an EXEC process
 exec-banner             Enable the display of the EXEC banner
 exec-character-bits     Size of characters to the command exec
 exec-timeout            Set the EXEC timeout
 exit                    Exit from line configuration mode
 flowcontrol             Set the flow control
 help                    Description of the interactive help system
 history                 Enable the command history function
 hold-character          Define the hold character
 length                  Set number of lines on a screen
 location                Enter terminal location description
 lockable                Allow users to lock a line
 login                   Enable password checking
 modem                   Configure the Modem Control Lines
 monitor                 Copy debug output to the current terminal line
 no                      Negate a command or set its defaults
 notify                  Inform users of output from concurrent sessions
```

```
 padding                 Set padding for a specified output character
 parity                  Set terminal parity
 password                Set a password
 private             Configuration options that user can set will remain in effect
between terminal sessions
 refuse-message          Define a refuse banner
 rotary                  Add line to a rotary group
 rxspeed                 Set the receive speed
 session-limit           Set maximum number of sessions
 session-timeout            Set interval for closing connection when there is no input
traffic
 special-character-bits  Size of the escape (and other special) characters
 speed                   Set the transmit and receive speeds
 start-character         Define the start character
 stop-character          Define the stop character
 stopbits                Set async line stop bits
 telnet                  Telnet protocol-specific configuration
 telnet-transparent      Send a CR as a CR followed by a NULL instead of a CR followed
by a LF
 terminal-type           Set the terminal type
 transport               Define transport protocols for line
 txspeed                 Set the transmit speeds
 vacant-message          Define a vacant banner
 width                   Set width of the display terminal
```

The list of commands might vary from this example, depending upon how your router has been configured.

To exit line configuration mode and return to global configuration mode, use the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

Router Configuration Mode

Router configuration commands configure a routing protocol and always follow a **router** command. To access and list the router configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, enter router configuration mode.	**router** [*keyword*][1] See the list in the example for keywords.
Step 2	List the router configuration commands.	**?**

1. This command is documented in the "IP Routing Protocols Commands" chapter in the *Router Products Command Reference* publication.

To list the available router configuration keywords, enter the **router** command followed by a space and a question mark (?) at the global configuration prompt:

```
Router(config)# router ?
 bgp       Border Gateway Protocol (BGP)
 egp       Exterior Gateway Protocol (EGP)
 igrp      Interior Gateway Routing Protocol (IGRP)
 isis      ISO IS-IS
 iso-igrp  IGRP for OSI networks
 ospf      Open Shortest Path First (OSPF)
 rip       Routing Information Protocol (RIP)
 static    Static CLNS Routing
```

In the following example, the router is configured to support the Routing Information Protocol (RIP). The new prompt is `Router(config-router)#`.

```
Router(config)# router rip
```

```
Router(config-router)# ?
router configuration commands:
  default-information  Control distribution of default information
  default-metric       Set metric of redistributed routes
  distance             Define an administrative distance
  distribute-list      Filter networks in routing updates
  exit                 Exit from routing protocol configuration mode
  help                 Description of the interactive help system
  neighbor             Specify a neighbor router
  network              Enable routing on an IP network
  no                   Negate or set default values of a command
  offset-list          Add or subtract offset from IGRP, RIP, or HELLO metrics
  passive-interface    Suppress routing updates on an interface
  redistribute         Redistribute information from another routing protocol
  timers               Adjust routing timers
```

The list of commands might vary slightly from this example, depending upon how your router has been configured.

To exit router configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

IPX-Router Configuration Mode

Internet Packet Exchange (IPX) is a Novell network-layer protocol. To access and list the IPX routing configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, enter IPX-router configuration mode.	**ipx router** [*keyword*][1] See the Novell IPX chapter for keywords.
Step 2	List the IPX-router configuration commands.	**?**

1. This command is documented in the "Novell IPX Commands" chapter in the *Router Products Command Reference* publication.

In the following example, IPX RIP routing is configured. The new prompt is `Router(config-ipx-router)#`.

```
Router(config)# ipx router rip<CR>
Router(config-ipx-router)# ?
Novell router configuration commands:
  distribute-list  Filter networks in routing updates
  exit             Exit from IPX routing protocol configuration mode
  help             Description of the interactive help system
  network          Enable routing on an IPX network
  no               Negate or set default values of a command
  redistribute     Enable routing protocol redistribution
```

To exit IPX-router configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

Route-Map Configuration Mode

Use the route-map configuration mode to configure routing table and source and destination information. To access and list the **route-map** configuration commands, complete the following tasks:

Task		Command
Step 1	From global configuration mode, enter route-map configuration mode.	**route-map** [*route map tag*][1]
Step 2	List the route-map configuration commands.	**?**

1. This command is documented in the "IP Routing Protocols Commands" chapter in the *Router Products Command Reference* publication.

In the following example, a route map named arizona1 is configured. The new prompt is `Router(config-route-map)#`. Enter a question mark (**?**) to list **route-map** configuration commands.

```
Router(config)# route-map arizona1 <CR>
Router(config-route-map)# ?
Route Map configuration commands:
 exit   Exit from route-map configuration mode
 help   Description of the interactive help system
 match  Match values from routing table
 no     Negate or set default values of a command
 set    Set values in destination routing protocol
```

To exit route-map configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press Ctrl-Z.

ROM Monitor Mode

If your router does not find a valid system image, or if its configuration file is corrupted at startup, the system might enter read-only memory (ROM) monitor mode. From ROM monitor mode, you can boot the router or perform diagnostic tests.

From the Cisco 2000, Cisco 3000, and Cisco 4000, you can also enter ROM monitor mode by entering the **reload** EXEC command and then pressing the Break key during the first 60 seconds of startup. To save changes to the configuration file, use the **write memory** command before issuing the **reload** command.

To access and list the ROM monitor configuration commands, complete the following tasks:

Task	Command
Enter ROM monitor mode from privileged EXEC mode.	**reload**[1] Press Break during the first 60 seconds while the system is booting.
List the ROM monitor commands.	**?**

1. This command is documented in the "System Image, Microcode Image, and Configuration File Load Commands" chapter of the *Router Products Command Reference* publication.

The ROM monitor prompt is the angle bracket (>):

```
> ?
$ state      Toggle cache state (? for help)
B [filename] [TFTP Server IP address | TFTP Server Name]
             Load and execute system image from ROM or from TFTP server
```

```
C [address]  Continue execution [optional address]
D /S M L V   Deposit value V of size S into location L with modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin execution
H            Help for commands
I            Initialize
K            Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
             Load system image from ROM or from TFTP server, but do not
             begin execution
O            Show configuration register option settings
P            Set the break point
S            Single step next instruction
T function   Test device (? for help)
Deposit and Examine sizes may be B (byte), L (long) or S (short).
Modifiers may be R (register) or S (byte swap).
Register names are: D0-D7, A0-A6, SS, US, SR, and PC
```

To return to user EXEC mode, enter **c** to continue. To boot the system image file, use the **b** command (described in the "System Image, Microcode Image, and Configuration File Load Commands" chapter in the *Router Products Command Reference* publication). For details on other ROM monitor mode commands, refer to the appropriate hardware installation guide.

Get Context-Sensitive Help

The previous sections described the first level of help available with the user interface. 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 arguments, perform one of the following tasks:

Task	Command
Obtain a brief description of the help system in any command mode.	**help**
Obtain help for the full set of user-level commands.	**full-help**
Obtain help for the full set of user-level commands in user EXEC command mode.	**terminal full-help**[1]
Obtain a list of commands that begin with a particular character string.	*abbreviated-command-entry***?**
Complete a partial command name.	*abbreviated-command-entry*<**Tab**>
List all commands available for a particular command mode.	**?**
List a command's associated keywords.	*command* **?**
List a keyword's associated arguments.	*command keyword* **?**

1. This command is documented in the *Cisco Access Connection Guide*.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called *word help*, because it completes a word for you.

To list keywords or arguments, enter a question mark **(?)** in place of a keyword or argument. Include a space before the **?**. This form of help is called *command syntax help*, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **show** command to **sh**.

Enter the **help** command (which is available in any command mode) for a brief description of the help system:

```
Router# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

As described in the **help** command output, you can enter a partial command name and a **question mark** (?) to obtain a list of commands beginning with a particular character set. See "Complete a Partial Command Name" later in this chapter for more detail.

The following example illustrates how the context-sensitive help feature enables you to create an access list from configuration mode. First enter the letters **co** at the system prompt followed by a question mark (?). Do not leave a space between the last letter and the question mark (?). The system provides the commands that begin with **co**.

```
Router# co?
configure  connect  copy
```

Enter the **configure** command followed by a space and a **question mark (?**) to list the command's keywords and a brief explanation:

```
Router# configure ?
  memory    Configure from NV memory
  network   Configure from a TFTP network host
  terminal  Configure from the terminal
  <cr>
```

Enter the **terminal** keyword to enter configuration mode from the terminal:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Enter the **access-list** command followed by a space and a question mark (?) to list the command's keywords:

```
Router(config)# access-list ?
  <1-99>       IP standard access list
  <100-199>    IP extended access list
  <1000-1099>  IPX SAP access list
  <1100-1199>  Extended 48-bit MAC address access list
  <200-299>    Protocol type-code access list
  <300-399>    DECnet access list
  <400-499>    XNS standard access list
  <500-599>    XNS extended access list
  <600-699>    Appletalk access list
  <700-799>    48-bit MAC address access list
  <800-899>    IPX standard access list
  <900-999>    IPX extended access list
```

Enter the access list number **99** and then enter another question mark (?) to see the arguments that apply to the keyword and brief explanations:

```
Router(config)# access-list 99 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
```

Enter the **deny** argument followed by a question mark (?) to list additional options:

```
Router(config)# access-list 99 deny ?
  A.B.C.D  Address to match
```

Enter the IP address followed by a question mark (?) to list additional options:

```
Router(config)# access-list 99 deny 131.108.134.0 ?
  A.B.C.D  Mask of bits to ignore
  <cr>
```

The <cr> symbol appears in the list, indicating that one of your options is to press Return to execute the command. The other option is to add a wildcard mask. Enter the wildcard mask followed by a question mark (?) to list further options.

```
Router(config)# access-list 99 deny 131.108.134.0 0.0.0.255 ?
<cr>

Router(config)# access-list 99 deny 131.108.134.0 0.0.0.255
```

The <cr> symbol by itself indicates there are no more keywords or arguments. Press Return to execute the command. The system adds an entry to access list 99 that denies access to all hosts on subnet 131.108.134.0.

Check Command Syntax

The user interface provides syntax checking in the form of an error location indicator (^). The ^ symbol appears at the point in the command string where you have entered an incorrect command, keyword, or argument. The error location indicator and interactive help system allow you to easily find and correct syntax errors.

In the following example, suppose you want to set the router clock. First, use context-sensitive help to check the syntax for setting the clock.

```
Router# clock ?
  set  Set the time and date
Router# clock
```

The help output shows that the **set** keyword is required. Next, check the syntax for entering the time:

```
Router# clock set ?
hh:mm:ss   Current time
Router# clock set
```

Enter the current time:

```
Router# clock set 13:32:00
% Incomplete command.
```

The system indicates that you need to provide additional arguments to complete the command. Press Ctrl-P (see the next section, “Use the Command History Features”) to automatically repeat the previous command entry. Then add a space and question mark (**?**) to reveal the additional arguments:

```
Router# clock set 13:32:00 ?
```

```
  <1-31>     Day of the month
  January    Month of the year
  February
  March
  April
  May
  June
  July
  August
  September
  October
  November
  December
```

Now you can complete the command entry:

```
Router# clock set 13:32:00 23 February 93
                                        ^
% Invalid input detected at '^' marker.
```

The caret symbol (^) and help response indicate an error at 93. To list the correct syntax, enter the command up to the point where the error occurred and then enter a question mark (?):

```
Router# clock set 13:32:00 23 February ?
  <1993-2035> Year
Router# clock set 13:32:00 23 February
```

Enter the year using the correct syntax and press Return to execute the command.

```
Router# clock set 13:32:00 23 February 1993
```

Use the Command History Features

With the current software release, the user interface provides a history or record of commands you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. With the command history feature, you can complete the tasks in the following sections:

- Set the Command History Buffer Size
- Recall Commands
- Disable the Command History Feature

Set the Command History Buffer Size

By default, the system records ten command lines in its history buffer. To set the number of command lines the system will record during the current terminal session, complete the following task in EXEC mode:

Task	Command
Enable the command history feature for the current terminal session.	**terminal history** [**size** *number-of-lines*][1]

1. This command is documented in the *Cisco Access Connnection Guide*.

The **terminal history no size** command resets to default.

To configure the number of command lines the system will record, complete the following task in line configuration mode:

Task	Command
Enable the command history feature.	**history** [**size** *number-of-lines*][1]

1. The **no history** command resets to default.

Recall Commands

To recall commands from the history buffer, perform one of the following tasks:

Task	Key Sequence/Command
Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.	Press Ctrl-P or the up arrow key.[1]
Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.	Press Ctrl-N or the down arrow key.[1]
While in EXEC mode, list the commands you have just entered.	**show history**

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disable the Command History Feature

The command history feature is automatically enabled. To disable it during the current terminal session, complete the following task in EXEC mode:

Task	Command
Disable the command history feature for the current session.	**terminal no history**[1]

1. This command is documented in the *Cisco Access Connnection Guide*.

To configure a specific line so that the command history feature is disabled, complete the following task in line configuration mode:

Task	Command
Configure the line so that the command history feature is disabled.	**no history**

Use the Editing Features

The current software release includes an enhanced editing mode that provides a set of editing key functions similar to those of the Emacs editor.

You can enter commands in uppercase, lowercase, or a mix of both. Only passwords are casesensitive. You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **show** command to **sh**. After entering the command line at the system prompt, press the Return key to execute the command.

The following subsections are included in this section:

- Enable Enhanced Editing Mode

- Move Around on the Command Line
- Complete a Partial Command Name
- Paste in Buffer Entries
- Edit Command Lines that Wrap
- Delete Entries
- Scroll Down a Line or a Screen
- Redisplay the Current Command Line
- Transpose Mistyped Characters
- Control Capitalization
- Designate a Keystroke as a Command Entry
- Disable Enhanced Editing Mode

Enable Enhanced Editing Mode

Although enhanced editing mode is automatically enabled with the current software release, you can disable it and revert to the editing mode of previous software releases. See the section "Disable Enhanced Editing Mode" later in this chapter.

To reenable the enhanced editing mode for the current terminal session, complete the following task in EXEC mode:

Task	Command
Enable the enhanced editing features for the current terminal session.	**terminal editing**[1]

1. This command is documented in the *Cisco Access Connection Guide*.

To reconfigure a specific line to have enhanced editing mode, complete the following task in line configuration mode:

Task	Command
Enable the enhanced editing features.	**editing**

Move Around on the Command Line

Perform the following tasks to move the cursor around on the command line for corrections or changes:

Task	Keystrokes
Move the cursor back one character.	Press Ctrl-B or press the left arrow key.[1]
Move the cursor forward one character.	Press Ctrl-F or press the right arrow key.[1]
Move the cursor to the beginning of the command line.	Press Ctrl-A.
Move the cursor to the end of the command line.	Press Ctrl-E.
Move the cursor back one word.	Press Esc-B.
Move the cursor forward one word.	Press Esc-F.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Complete a Partial Command Name

If you cannot remember a complete command name, you can use the Tab key to allow the system to complete a partial entry. To do so, perform the following task:

Task	Keystrokes
Recall a complete command name.	Enter the first few letters and press the Tab key.

If your keyboard does not have a Tab key, press Ctrl-I instead.

In the following example, when you enter the letters **conf** and press the Tab key, the system provides the complete command:

```
Router# conf<Tab>
Router# configure
```

If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. Enter a question mark (**?**) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter and the question mark (**?**).

For example, there are three commands in privileged mode that start with co. To see what they are, type **co?** at the privileged EXEC prompt:

```
Router# co?
configure  connect  copy
Router# co
```

Paste in Buffer Entries

The system provides a buffer that contains the last ten items you deleted. You can recall these items and paste them in the command line by performing the following task:

Task		Keystrokes
Step 1	Recall the most recent entry in the buffer.	Press Ctrl-Y.
Step 2	Recall the next buffer entry.	Press Esc-Y.

The buffer contains only the last ten items you have deleted or cut. If you press **Esc-Y** more than ten times, you will cycle back to the first buffer entry.

Edit Command Lines that Wrap

The new editing command set provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, perform the following task:

Task	Keystrokes
Return to the beginning of a command line to verify that you have entered a lengthy command correctly.	Press Ctrl-B or the left arrow key repeatedly until you scroll back to the beginning of the command entry, or press Ctrl-A to return directly to the beginning of the line.[1]

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

In the following example, the **access-list** command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) indicates that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Router(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Router(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Router(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

When you have completed the entry, press Ctrl-A to check the complete syntax before pressing the Return key to execute the command. The dollar sign ($) appears at the end of the line to indicate that the line has been scrolled to the right:

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The router assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** command to tell the router the correct width of your terminal.

Use line wrapping in conjunction with the command history feature to recall and modify previous complex command entries. See the section “Recall Commands” earlier in this chapter for information about recalling previous command entries.

Delete Entries

Perform any of the following tasks to delete command entries if you make a mistake or change your mind:

Task	Keystrokes
Erase the character to the left of the cursor.	Press the Delete or Backspace key.
Delete the character at the cursor.	Press Ctrl-D.
Delete all characters from the cursor to the end of the command line.	Press Ctrl-K.
Delete all characters from the cursor to the beginning of the command line.	Press Ctrl-U or Ctrl-X.
Delete the word to the left of the cursor.	Press Ctrl-W.
Delete from the cursor to the end of the word.	Press Esc-D.

Scroll Down a Line or a Screen

When you use the help facility to list the commands available in a particular mode, the list is often longer than the terminal screen can display. In such cases, a `---More---` prompt is displayed at the bottom of the screen. To view the next line or screen, complete the following tasks:

Task	Keystrokes
Scroll down one line.	Press the Return key.
Scroll down one screen.	Press the Space bar.

Note The `---More---` prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the keystrokes listed above whenever you see the `---More---` prompt.

Redisplay the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To do so, perform the following task:

Task	Keystrokes
Redisplay the current command line.	Press Ctrl-L or Ctrl-R.

Transpose Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters by performing the following task:

Task	Keystrokes
Transpose the character to the left of the cursor with the character located at the cursor.	Press Ctrl-T.

Control Capitalization

You can capitalize or lowercase words or capitalize a set of letters with simple keystroke sequences. To do so, perform the following task:

Task	Keystrokes
Capitalize the word at the cursor.	Press Esc-C.
Change the word at the cursor to lowercase.	Press Esc-L.
Capitalize letters from the cursor to the end of the word.	Press Esc-U.

Designate a Keystroke as a Command Entry

Sometimes you might want to use a particular keystroke as an executable command, perhaps as a shortcut. Complete the following task to insert a system code for this purpose:

Task	Keystrokes
Insert a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* an editing key.	Press Ctrl-V or Esc-Q.

Disable Enhanced Editing Mode

To disable enhanced editing mode and revert to the editing mode of software releases before 9.21, perform the following task in EXEC mode:

Task	Command
Disable the enhanced editing features for the local line.	**terminal no editing**[1]

1. This command is documented in the *Cisco Access Connection Guide*.

You might want to disable enhanced editing if you have prebuilt scripts; for example, scripts that do not interact well when enhanced editing is enabled. You can reenable enhanced editing mode with the **terminal editing** command.

The editing keys and functions of software releases before 9.21 are listed in Table 2-2.

Table 2-2 Editing Keys and Functions for Software Release 9.1 and Earlier

Key	Function
Delete or Backspace	Erases the character to the left of the cursor.
Ctrl-W	Erases a word.
Ctrl-U	Erases a line.
Ctrl-R	Redisplays a line.
Ctrl-Z	Ends configuration mode and returns to the EXEC prompt.
Return	Executes single-line commands.

End a Session

After using the **setup** command or other configuration commands, exit the router and close the console port connection to return to the Telnet prompt, from which you can quit the session.

To end a session, perform the following steps:

Task		Command
Step 1	Exit the router and close the console port connection.	Press Ctrl-]
Step 2	Quit the Telnet session.	**quit**

Refer to the *Cisco Access Connection Guide* for more information on exiting sessions and closing connections.

CHAPTER 3

Loading System Images, Microcode Images, and Configuration Files

This chapter describes how to load system images, microcode images, and configuration files. The system images contain the system software, and the configuration files contain commands entered to customize the function of the router. Microcode images contain microcode to be downloaded to various hardware devices. The instructions in this chapter describe how to copy system images from routers to network servers (and vice versa), display and compare different configuration files, and list the system software version running on the router.

This chapter also describes the AutoInstall procedure, which you can use to automatically configure and enable a new router upon startup.

For a complete description of the commands mentioned in this chapter, refer to the "System Image, Microcode Image, and Configuration File Load Commands" chapter in the *Router Products Command Reference* publication.

Note You also can use the **setup** command and its interactive prompts to create a basic configuration file. See the *Router Products Getting Started Guide* for more information.

Cisco's rsh and rcp Implementation

One of the first attempts to use the network as a resource in the UNIX community resulted in the design and implementation of the remote shell protocol, which included the remote shell (rsh) and remote copy (rcp). Rsh and rcp give users the ability to execute commands remotely and copy files to and from a file system residing on a remote host or server on the network. Cisco's implementation of rsh and rcp will interoperate with standard implementations of rsh and rcp.

From the router, you can use rsh to execute commands on remote systems to which you have access. When you issue the rsh command, a shell is started on the remote system. The shell allows you to execute commands on the remote system without having to log into the target host.

In other words, you do not need to connect to the system or router and then disconnect after you execute a command if you use rsh. For example, you can use rsh to remotely look at the status of other routers without connecting to the target router, executing the command, and then disconnecting from the router. This is useful for looking at statistics on many different routers.

To gain access to a remote system running rsh, such as a UNIX host, there must be an entry in the system's *.rhosts* file or its equivalent identifying you as a trusted user who is authorized to execute commands remotely on the system. On UNIX systems, the *.rhosts* file identifies trusted users who can remotely execute commands on the system.

You can enable rsh support on a Cisco router to allow users on remote systems to execute commands on the router. However, our implementation of rsh does not support an *.rhosts* file. Instead, you configure a local authentication database to control access to the router by users attempting to execute commands remotely using rsh. A local authentication database is similar in concept and use to a UNIX *.rhosts* file. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user.

The rcp copy commands rely on the rsh server (or daemon) on the remote system. To copy files using rcp, you do not need to create a server for file distribution, as you do with TFTP.You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, rcp creates it for you.

Although our rcp implementation emulates the behavior of the UNIX rcp implementation—copying files among systems on the network—our command syntax differs from the UNIX rcp command syntax. Our rcp support offers a set of copy commands that use rcp as the transport mechanism. These rcp copy commands are similar in style to our TFTP copy commands, but they offer an alternative that provides faster performance and reliable delivery of data. This is because the rcp transport mechanism is built on and uses the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented. You can use rcp commands to copy system images and configuration files from the router to a network server and vice versa.

You can also enable rcp support on the router to allow users on remote systems to copy files to and from the router.

System Image, Microcode Image, and Configuration File Load Task List

You can perform the tasks in the following sections to load system images, microcode images, and configuration files.

- Use the AutoInstall Procedure
- Enter Configuration Mode
- Modify the Configuration Register Boot Field
- Specify the System Image the Router Loads upon Restart
- Specify the Configuration File the Router Loads upon Restart
- Additional Cisco 3000 and Cisco 4000 Copying and Automatic Booting Features
- Change the Buffer Size for Loading Configuration Files
- Compress Configuration Files
- Manually Load a System Image
- Boot Systems That Have Dual-Bank Flash Memory
- Configure a Router as a TFTP Server
- Configure a Router to Support Incoming rcp Requests and rsh Commands
- Configure a Router as a RARP Server
- Configure the Remote Username for rcp Requests
- Specify SLIP Extended BOOTP Requests

- Specify MOP Server Boot Requests
- Copy System Images from a Network Server to Flash Memory Using TFTP
- Copy System Images from a Network Server to Flash Memory Using rcp
- Additional Cisco 3000 and Cisco 4000 Flash Upgrade Features
- Copy Bootstrap Images from a Network Server to Flash Memory Using rcp or TFTP
- Use Flash Load Helper to Upgrade Software on Run-from-Flash Systems
- Verify the Image in Flash Memory
- Partition Flash Memory Using Dual Flash Bank
- Copy System Images from Flash Memory to a Network Server Using TFTP
- Copy System Images from Flash Memory to a Network Server Using rcp
- Copy a Configuration File from a Network Server to the Router Using rcp
- Copy a Configuration File from the Router to a Network Server Using TFTP
- Copy a Configuration File from the Router to a Network Server Using rcp
- Display System Image and Configuration Information
- Clear the Contents of NVRAM
- Re-execute the Configuration Commands in NVRAM
- Remotely Execute Commands Using rsh
- Use Flash Memory as a TFTP Server
- Load Microcode Images over the Network
- Display Microcode Information

Use the AutoInstall Procedure

This section provides information about AutoInstall, a procedure that allows you to configure a new router automatically and dynamically. The AutoInstall procedure involves connecting a new router to a network on which there is an existing preconfigured router, turning on the new router, and enabling it with a configuration file that is automatically downloaded from a Trivial File Transfer Protocol (TFTP) server.

The following sections provide the requirements for AutoInstall and an overview of how the procedure works. To start the procedure, go to “Perform the AutoInstall Procedure” later in this section.

AutoInstall Requirements

For the AutoInstall procedure to work, your system must meet the following requirements:

- Both routers must be physically attached to the network using one or more of the following interface types: Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), serial with High-Level Data Link Control (HDLC) encapsulation, or serial with Frame Relay encapsulation. HDLC is the default serial encapsulation. Frame Relay will be automatically configured by the AutoInstall process. If the AutoInstall process fails over HDLC, the router will automatically configure Frame Relay encapsulation.
- The existing preconfigured router must be running Software Release 9.1 or later. For AutoInstall over Frame Relay, routers on both sides must be running Cisco Internetwork Operating System (IOS) Release 10.3 or later.
- The new router must be running Software Release 9.1 or later. For AutoInstall over Frame Relay, the new router must be running Cisco IOS Release 10.3 or later.

Note Only Token Ring interfaces that set ring speed with physical jumpers will support AutoInstall. AutoInstall does not work with Token Ring interfaces for which the ring speed must be set using software configuration commands. If the ring speed is not set, the interface is set to shutdown mode.

- You must complete procedures 1 and either 2 or 3:
  - Procedure 1: A configuration file for the new router must reside on a TFTP server. This file can contain the new router's full configuration or the minimum needed for the administrator to Telnet into the new router for configuration.
  - Procedure 2: A file named network-confg also must reside on the server. The file must have an Internet Protocol (IP) host name entry for the new router. The server must be reachable from the existing router.
  - Procedure 3: An IP address-to-host name mapping for the new router must be added to a Domain Name System (DNS) database file.
- If the existing router is to help automatically install the new router via a HDLC-encapsulated serial interface using Serial Line Address Resolution Protocol (SLARP), that interface must be configured with an IP address whose host portion has the value 1 or 2. (AutoInstall over Frame Relay does not have this address constraint.) Subnet masks of any size are supported.
- If the existing router is to help automatically install the new router using Frame Relay encapsulated serial interface, that interface must be configured with the following:
  - An IP helper address pointing to the TFTP server. In the following example, 171.69.2.75 is the address of the TFTP server:

    ```
    ip helper 171.69.2.75
    ```

  - A Frame Relay map pointing back to the newrouter. In the following example, 172.21.177.100 is the IP address of *newrouter*'s serial interface. 100 is the PVC identifier:

    ```
    frame-relay map ip 172.21.177.100 100 dlci
    ```

- If the existing router is to help automatically install the new router via an Ethernet, Token Ring, or FDDI interface using BOOTP or Reverse Address Resolution Protocol (RARP), a BOOTP or RARP server also must be set up to map the new router's Media Access Control (MAC) address to its IP address.
- IP helper addresses might need to be configured in order to forward the TFTP and DNS broadcast requests from the new router to the host that is providing those services.

Using a DOS-based TFTP Server

AutoInstall over Frame Relay and over other WAN encapsulations support downloading configuration files from UNIX-based and DOS-based TFTP servers. Other booting mechanisms such as RARP and SLARP also support UNIX-based and DOS-based TFTP servers.

The DOS format of the UNIX network-confg file that must reside on the server must be eight characters or less, with a three-letter extension. Therefore, when an attempt to load network-confg fails, AutoInstall automatically attempts to download cisconet.cfg from the TFTP server.

If cisconet.cfg exists and a download succeeds, then the server is assumed to be a DOS machine. The AutoInstall program will then attempt to resolve the host name for the router through host commands in cisconet.cfg.

If cisconet.cfg does not exist or cannot be downloaded, or the program is unable to resolve a host name, DNS will attempt to resolve the host name of the router. If it is unable to resolve the host name through DNS, the router will attempt to download ciscortr.cfg. If the host name is longer than eight characters, it will get truncated to eight characters. For example, a router with a host name "australia" will be treated as "australi" and an attempt will be made to download australi.cfg.

The format of cisconet.cfg and ciscortr.cfg are to be the same as those described for network-confg and hostname-confg.

If neither network-confg nor cisconet.cfg exist and DNS is unable to resolve the host name, the program will attempt to load router-confg, and then ciscortr.cfg if router-confg does not exist or cannot be downloaded. The cycle is repeated three times.

How AutoInstall Works

Once the requirements for using AutoInstall are met, the dynamic configuration of the new router occurs in the following order:

1. The new router acquires its IP address. Depending upon the interface connection between the two routers, the new router's IP address is dynamically resolved by either SLARP requests or BOOTP or RARP requests.
2. The new router resolves its name either through network-confg or cisconet.cfg or through DNS.
3. The new router automatically requests and downloads its configuration file from a TFTP server.
4. If a host name is not resolved, the *newrouter* will attempt to load router-confg or ciscortr.cfg.

Acquiring the New Router's IP Address

The new router (*newrouter*) resolves its interface's IP addresses by one of the following means:

- If *newrouter* is connected by an HDLC-encapsulated serial line to the existing router (*existing*), *newrouter* sends a SLARP request to *existing.*
- If *newrouter* is connected by an Ethernet, Token Ring, or FDDI interface, it broadcasts BOOTP and RARP requests.
- If *newrouter* is connected by a Frame Relay-encapsulated serial interface, it first attempts the HDLC automatic installation process and then attempts the BOOTP/RARP process over Ethernet, Token Ring or FDDI. If both of these attempts fail, it attempts to automatically install over Frame Relay. In this case, a BOOTP request is sent over the lowest numbered serial or HSSI interface.

The existing router (*existing*) responds in one of the following ways depending upon the request type:

- In response to a SLARP request, *existing* sends a SLARP reply packet to *newrouter*. The reply packet contains the IP address and netmask of *existing*. If the host portion of the IP address in the SLARP response is 1, *newrouter* will configure its interface using the value 2 as the host portion of its IP address and vice versa. (See Figure 3-1.)

Figure 3-1 Using SLARP to Acquire the New Router's IP Address

- In response to BOOTP or RARP requests, an IP address is sent from the BOOTP or RARP server to *newrouter*.

  A BOOTP or RARP server must have already been set up to map *newrouter*'s MAC address to its IP address. If the BOOTP server does not reside on the directly attached network segment, routers between *newrouter* and the BOOTP server can be configured using the **ip helper-address** command to allow the request and response to be forwarded between segments, as shown in Figure 3-2.

  AutoInstall over Frame Relay is a special case in which BOOTP is used but the existing router acts as a BOOTP server and responds to the incoming BOOTP request. Only a helper address and a Frame Relay map need to be set up. There is no need for a MAC-to-IP address map on the existing router.