

BCRAN

Building Cisco Remote Access Networks

Version 2.1

Student Guide

Copyright © 2004, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe



Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)

Table of Contents

Volume 1

<i>Course Introduction</i>	1
Overview	1
Outline	1
Course Objectives	2
Course Activities	4
Cisco Certifications	5
Learner Skills and Knowledge	6
Learner Responsibilities	7
General Administration	8
Course Flow Diagram	9
Icons and Symbols	10
Learner Introductions	11
<i>WAN Technologies and Components</i>	1-1
Overview	1-1
Objectives	1-1
Outline	1-1
<i>Defining WAN Connection Types</i>	1-3
Overview	1-3
Relevance	1-3
Objectives	1-3
Learner Skills and Knowledge	1-3
Outline	1-4
WAN Connection Characteristics	1-5
Common WAN Connection Types	1-7
Dedicated Circuit-Switched Connections	1-8
On-Demand Circuit-Switched Connections	1-10
ISDN Connections	1-12
Packet-Switched Virtual Connections	1-13
Broadband Access	1-15
Summary	1-16
Quiz	1-17
Quiz Answer Key	1-19
<i>Defining WAN Encapsulation Protocols</i>	1-21
Overview	1-21
Relevance	1-21
Objectives	1-21
Learner Skills and Knowledge	1-21
Outline	1-22
WAN Encapsulation Protocols	1-23
PPP Encapsulation	1-25
Frame Relay Encapsulations	1-27
Summary	1-28
Quiz	1-29
Quiz Answer Key	1-30
<i>Determining the WAN Type to Use</i>	1-31
Overview	1-31
Relevance	1-31
Objectives	1-31
Learner Skills and Knowledge	1-32
Outline	1-32
WAN Connection Types	1-33

WAN Connection Speed Comparison	1-35
WAN Connection Summary	1-36
Site Requirements	1-37
Central Site Considerations	1-39
Central Site Router Equipment	1-41
Branch Office Considerations	1-42
Branch Office Router Equipment	1-44
SOHO Site Considerations	1-45
SOHO Site Router Equipment	1-46
Summary	1-47
Quiz	1-48
Quiz Answer Key	1-50
Selecting Cisco Products for Remote Connections	1-51
Overview	1-51
Relevance	1-51
Objectives	1-51
Learner Skills and Knowledge	1-51
Outline	1-52
Cisco Remote Access Solutions	1-53
Interfaces: Fixed Interface	1-55
Interfaces: Modular Interface	1-56
Network Cabling and Assembly	1-57
Verification of Network Installation	1-59
Verification of Branch Office Installation	1-61
Verification of SOHO Installation	1-63
Products with Cisco Product Selection Tools	1-65
Summary	1-66
Next Steps	1-66
Quiz	1-67
Quiz Answer Key	1-69
Supporting Asynchronous Modems	2-1
Overview	2-1
Objectives	2-1
Outline	2-1
Connecting and Operating Modems	2-3
Overview	2-3
Relevance	2-3
Objectives	2-3
Learner Skills and Knowledge	2-3
Outline	2-4
Modem Connections and Operation	2-5
The DTE-DCE Interface	2-6
Modem Signaling—Data	2-7
Modem Signaling—Control	2-8
Modem Control Example	2-9
Modem Operation	2-10
DTE-to-DTE Wiring	2-11
RJ-45 Wiring and Cables	2-12
Working Connections	2-13
Error Control and Data Compression Standards	2-15
Modem Modulation and Standards	2-16
Modem Speed and Compression	2-18
Theoretical Speeds	2-19

Summary	2-20
Quiz	2-21
Quiz Answer Key	2-24
Configuring Modems	2-25
Overview	2-25
Relevance	2-25
Objectives	2-25
Learner Skills and Knowledge	2-25
Outline	2-26
Modem Connections	2-27
EXEC Connection Commands	2-29
Sample Output for the show line Command	2-31
Line Types and Numbering	2-33
Interface Asynchronous and Line Configuration	2-34
Basic Modem Configuration	2-35
Standard Modem Commands	2-37
Nonstandard Modem Commands	2-38
Modem Initialization Strings	2-39
Summary	2-40
Quiz	2-41
Quiz Answer Key	2-43
Autoconfiguring Modems	2-45
Overview	2-45
Relevance	2-45
Objectives	2-45
Learner Skills and Knowledge	2-45
Outline	2-46
Modem Autoconfiguration	2-47
Automatic Modem Configuration	2-48
Modem Autodiscovery	2-49
Modem Autoconfiguration: Configuring	2-51
Modem Autodiscovery: Configuring	2-52
Known Modem Initialization String	2-53
Modemcap Database	2-54
Modemcap Database Management	2-55
Modemcap Entries: Viewing	2-56
Custom Modemcap Entry: Creating and Editing	2-57
Custom Modemcap Entry: Viewing	2-58
Summary	2-59
Quiz	2-60
Quiz Answer Key	2-62
Verifying and Debugging Modem Autoconfiguration	2-63
Overview	2-63
Relevance	2-63
Objectives	2-63
Learner Skills and Knowledge	2-63
Outline	2-64
Verification of Modem Autoconfiguration Operation	2-65
Modem Autoconfiguration Troubleshooting	2-66
Chat Scripts for Asynchronous Lines	2-67
Summary	2-69
Next Steps	2-69
Quiz	2-70
Quiz Answer Key	2-71

Configuring PPP Features	3-1
Overview	3-1
Objectives	3-1
Outline	3-1
Describing PPP Features	3-3
Overview	3-3
Relevance	3-3
Objectives	3-3
Learner Skills and Knowledge	3-3
Outline	3-4
Remote Node Connections	3-5
PPP Architecture	3-7
HDLC and PPP Frames	3-9
Summary	3-10
Quiz	3-11
Quiz Answer Key	3-12
Configuring Basic PPP	3-13
Overview	3-13
Relevance	3-13
Objectives	3-13
Learner Skills and Knowledge	3-13
Outline	3-14
PPP: Enabling	3-15
PPP Session and EXEC Session	3-16
PPP and Asynchronous Interface: Enabling Commands	3-17
Autoselect	3-18
Asynchronous Interface Commands for Addressing	3-20
Summary	3-23
Quiz	3-24
Quiz Answer Key	3-25
Configuring LCP Options: Authentication with PAP and CHAP	3-27
Overview	3-27
Relevance	3-27
Objectives	3-27
Learner Skills and Knowledge	3-27
Outline	3-28
PPP Authentication	3-29
PPP Using PAP Authentication	3-30
PAP Configuration Example	3-31
PPP Using CHAP Authentication	3-32
CHAP Configuration Example	3-37
CHAP and PAP Configuration Authentication	3-38
Summary	3-39
Quiz	3-40
Quiz Answer Key	3-42
Configuring LCP Options: Callback and Compression	3-43
Overview	3-43
Relevance	3-43
Objectives	3-43
Learner Skills and Knowledge	3-43
Outline	3-44
PPP Callback Overview	3-45
Asynchronous Callback Operation Flowchart	3-47

PPP Callback Operation	3-48
Asynchronous Callback Line and Interface Commands	3-50
PPP Callback Client Configuration	3-51
PPP Callback Server Configuration	3-52
Compression and PPP	3-53
Compression Configuration	3-55
Compression Verification	3-56
Uncompressed Bytes	3-56
Throughput Ratio	3-56
Buffer Allocation	3-56
Bytes Transmitted	3-57
Bytes Received	3-57
Interpreting the <i>show compress</i> Command Output	3-57
Summary	3-58
Quiz	3-59
Quiz Answer Key	3-61
Configuring LCP Options: Multilink PPP	3-63
Overview	3-63
Relevance	3-63
Objectives	3-63
Learner Skills and Knowledge	3-63
Outline	3-64
Multilink PPP Overview	3-65
Multilink PPP Operation and Configuration	3-66
Multilink PPP Example	3-67
Summary	3-68
Quiz	3-69
Quiz Answer Key	3-70
Verifying and Debugging PPP	3-71
Overview	3-71
Relevance	3-71
Objectives	3-71
Learner Skills and Knowledge	3-71
Outline	3-72
PPP Verification	3-73
<i>show dialer</i> Command Example	3-74
PPP Debugging	3-75
Multilink Verification	3-76
Summary	3-78
Next Steps	3-78
Quiz	3-79
Quiz Answer Key	3-80
Accessing Broadband	4-1
Overview	4-1
Objectives	4-1
Outline	4-1
Identifying Broadband Features	4-3
Overview	4-3
Relevance	4-3
Objectives	4-3
Learner Skills and Knowledge	4-3
Outline	4-4
Broadband Uses	4-5
Cable Options	4-6

DSL Options	4-7
Satellite Options	4-8
Wireless Options	4-9
Summary	4-11
Quiz	4-12
Quiz Answer Key	4-14
Addressing Broadband with NAT	4-15
Overview	4-15
Relevance	4-15
Objectives	4-15
Learner Skills and Knowledge	4-15
Outline	4-16
NAT Overview	4-17
NAT Concepts and Terminology	4-18
NAT Operation	4-20
Inside Source Address Translation	4-21
Inside Global Address Overload	4-23
Dynamic NAT Configuration	4-24
Inside Global Address Overload Configuration	4-26
NAT Verification and Troubleshooting	4-27
NAT Troubleshooting	4-29
NAT Entry Clearing	4-31
Summary	4-32
Quiz	4-33
Quiz Answer Key	4-35
Describing Cable Technology	4-37
Overview	4-37
Relevance	4-37
Objectives	4-37
Learner Skills and Knowledge	4-37
Outline	4-38
Cable Features	4-39
Data over Cable	4-40
Cable System Functionality	4-41
Cable System Components	4-43
Hybrid Fiber-Coaxial Architecture	4-44
Digital Signals over RF Channels	4-45
Cable Technology Terms	4-48
Cable Technology: Putting It All Together	4-52
Process for Provisioning a Cable Modem	4-53
Configuration of a Router with a Cable Modem	4-54
Summary	4-56
Quiz	4-57
Quiz Answer Key	4-59
Defining DSL Technology	4-61
Overview	4-61
Relevance	4-61
Objectives	4-61
Learner Skills and Knowledge	4-61
Outline	4-62
DSL Features	4-63
DSL Types	4-64
DSL Limitations	4-66
ADSL	4-67

ADSL and POTS Coexistence	4-68
ADSL Channels and Encoding	4-69
Data over ADSL: Bridging	4-71
Data over ADSL: PPPoE	4-73
Data over ADSL: PPPoA	4-77
Summary	4-78
Quiz	4-79
Quiz Answer Key	4-82
Configuring the CPE as the PPPoE Client	4-83
Overview	4-83
Relevance	4-83
Objectives	4-83
Learner Skills and Knowledge	4-84
Outline	4-84
Configuration of a Cisco 827 Router as the PPPoE Client	4-85
Configuration of PPPoE in a VPDN Group	4-86
Configuration of a PPPoE Client	4-87
Configuration of the PPPoE DSL Dialer Interface	4-88
Configuration of PAT	4-89
PAT Configuration Example	4-90
DHCP to Scale DSL	4-91
Configuration of a DHCP Server	4-92
Configuration of a Static Default Route	4-93
PPPoE Sample Configuration	4-94
Summary	4-95
Quiz	4-96
Quiz Answer Key	4-97
Configuring DSL with PPPoA	4-99
Overview	4-99
Relevance	4-99
Objectives	4-99
Learner Skills and Knowledge	4-99
Outline	4-100
Configuration of a PPPoA DSL Connection	4-101
DSL Modulation Configuration	4-102
Configuration of the DSL ATM Interface	4-103
Configuration of the DSL Dialer Interface	4-104
Configuration of PAT	4-105
PAT Configuration Example	4-106
DHCP to Scale DSL	4-107
Configuration of a Static Default Route	4-108
PPPoA Sample Configuration	4-109
Summary	4-110
Quiz	4-111
Quiz Answer Key	4-112
Troubleshooting DSL	4-113
Overview	4-113
Relevance	4-113
Objectives	4-113
Learner Skills and Knowledge	4-113
Outline	4-114
Layer Troubleshooting	4-115
Layer 1 Issues	4-116
Administratively Down State for an ATM Interface	4-118
Correct Power Supply	4-119

Correct DSL Operating Mode	4-120
Layer 2 Issues	4-121
Data Received from the ISP	4-122
Proper PPP Negotiation	4-123
Summary	4-124
Next Steps	4-124
Quiz	4-125
Quiz Answer Key	4-126

Table of Contents

Volume 2

<i>Virtual Private Networks</i>	5-1
Overview	5-1
Objectives	5-1
Outline	5-1
Identifying VPN Features	5-3
Overview	5-3
Relevance	5-3
Objectives	5-3
Learner Skills and Knowledge	5-3
Outline	5-4
VPN Features and Advantages	5-5
Tunneling and Encryption	5-8
VPN Usage Scenarios	5-9
VPN Technologies	5-14
VPN Protocols	5-16
L2TP	5-16
GRE	5-17
IPSec	5-17
Selecting a VPN Technology	5-18
VPN and IPSec Terms	5-19
Summary	5-22
References	5-23
Quiz	5-24
Quiz Answer Key	5-26
Identifying Cisco IOS Cryptosystem Features	5-27
Overview	5-27
Relevance	5-27
Objectives	5-27
Learner Skills and Knowledge	5-27
Outline	5-28
Cryptosystem Overview	5-29
Symmetric Encryption	5-30
Asymmetric Encryption	5-32
Key Exchange—Diffie-Hellman	5-33
Hashing	5-34
Summary	5-35
Quiz	5-36
Quiz Answer Key	5-37
Identifying IPSec Technologies	5-39
Overview	5-39
Relevance	5-39
Objectives	5-39
Learner Skills and Knowledge	5-40
Outline	5-40
IPSec	5-41
Tunnel vs. Transport Mode	5-43
Security Associations	5-44
Five Steps to IPSec	5-46
IPSec and IKE Relationship	5-47
IKE and IPSec Flowchart	5-49
Tasks to Configure IPSec	5-50
Summary	5-52

Quiz	5-53
Quiz Answer Key	5-55
Task 1: Preparing for IKE and IPSec	5-57
Overview	5-57
Relevance	5-57
Objectives	5-57
Learner Skills and Knowledge	5-58
Outline	5-58
IKE Creation and IPSec Security Policy	5-59
Step 1: Determine IKE (IKE Phase 1) Policy	5-60
IKE Phase 1 Policy Parameters	5-62
Step 2: Determine IPSec (IKE Phase 2) Policy	5-64
IPSec Transforms Supported in Cisco IOS Software	5-65
IPSec Policy Example	5-67
IPSec Peers	5-68
Step 3: Check Current Configuration	5-69
Step 4: Ensure That the Network Works	5-71
Step 5: Ensure That Access Lists Are Compatible with IPSec	5-72
Summary	5-74
Quiz	5-75
Quiz Answer Key	5-77
Task 2: Configuring IKE	5-79
Overview	5-79
Relevance	5-79
Objectives	5-79
Learner Skills and Knowledge	5-79
Outline	5-80
IKE Configuration	5-81
Step 1: Enable or Disable IKE	5-82
Step 2: Create IKE Policies	5-83
IKE Policy Creation with the <i>crypto isakmp</i> Command	5-84
IKE Policy Negotiation	5-86
Step 3: Configure ISAKMP Identity	5-87
Step 4: Configure Preshared Keys	5-89
Step 5: Verify IKE Configuration	5-91
Summary	5-92
Quiz	5-93
Quiz Answer Key	5-95
Task 3: Configuring IPSec	5-97
Overview	5-97
Relevance	5-97
Objectives	5-97
Learner Skills and Knowledge	5-98
Outline	5-98
IPSec Configuration	5-99
Step 1: Configure Transform Set Suites	5-100
Edit Transform Sets	5-101
Set Negotiation Transformation	5-102
Step 2: Configure Global IPSec Security Association Lifetimes	5-103
Crypto Access Lists Functionality	5-104
Step 3: Create Crypto ACLs Using Extended Access Lists	5-105
Symmetric Peer Crypto Access Lists Configuration	5-107
Crypto Maps Functionality	5-108
Crypto Map Parameters	5-109

Step 4: Configure IPsec Crypto Maps	5-110
Crypto Map Commands Example	5-112
Step 5: Apply Crypto Maps to Interfaces	5-114
IPsec Configuration Examples	5-115
Summary	5-117
Quiz	5-118
Quiz Answer Key	5-120
Task 4: Testing and Verifying IPsec	5-121
Overview	5-121
Relevance	5-121
Objectives	5-121
Learner Skills and Knowledge	5-121
Outline	5-122
Task 4: Test and Verify IPsec	5-123
The <i>show crypto isakmp policy</i> Command	5-124
The <i>show crypto ipsec transform-set</i> Command	5-125
The <i>show crypto ipsec sa</i> Command	5-126
The <i>show crypto map</i> Command	5-127
The <i>clear</i> Commands	5-128
The <i>debug crypto</i> Commands	5-129
Crypto System Error Messages for ISAKMP	5-133
Summary	5-134
Next Steps	5-134
Quiz	5-135
Quiz Answer Key	5-137
Using ISDN and DDR to Enhance Remote Connectivity	6-1
Overview	6-1
Objectives	6-1
Outline	6-1
Configuring ISDN BRI	6-3
Overview	6-3
Relevance	6-3
Objectives	6-3
Learner Skills and Knowledge	6-3
Outline	6-4
ISDN Services	6-5
ISDN Protocols	6-6
ISDN Protocol Layers	6-8
ISDN Configuration Tasks	6-9
ISDN Configuration Commands	6-10
ISDN Switch Types	6-11
Interface Protocol Settings	6-13
SPID Setting If Necessary	6-14
Caller Identification Screening	6-16
Configuration of Caller ID Screening	6-17
Called-Party Number Verification	6-18
Rate Adaption	6-20
Summary	6-21
Quiz	6-22
Quiz Answer Key	6-24

Configuring ISDN PRI	6-25
Overview	6-25
Relevance	6-25
Objectives	6-25
Learner Skills and Knowledge	6-25
Outline	6-26
ISDN Services	6-27
PRI Reference Points	6-29
Configuration Tasks for PRI	6-30
ISDN PRI Configuration	6-31
T1 and E1 Controller Parameters	6-33
Additional ISDN PRI Configuration Parameters	6-35
PRI Configuration Example	6-37
Summary	6-38
Quiz	6-39
Quiz Answer Key	6-40
Configuring DDR	6-41
Overview	6-41
Relevance	6-41
Objectives	6-41
Learner Skills and Knowledge	6-41
Outline	6-42
DDR Operation	6-43
DDR and ISDN Usage	6-44
DDR Configuration Tasks	6-46
Interesting Traffic for DDR	6-48
Access Lists for DDR	6-50
Destination Parameters for DDR	6-51
Configuration of a Simple ISDN Call	6-53
Configuration Example: RouterA	6-54
Configuration Example: RouterB	6-56
Access List for DDR Example	6-58
Summary	6-61
Quiz	6-62
Quiz Answer Key	6-64
Verifying ISDN and DDR Configurations	6-65
Overview	6-65
Relevance	6-65
Objectives	6-65
Learner Skills and Knowledge	6-65
Outline	6-66
ISDN BRI Monitoring	6-67
ISDN Layer 2 <i>debug</i> Commands	6-69
ISDN Layer 3 <i>debug</i> Commands	6-70
ISDN BRI D Channel Monitoring	6-71
ISDN BRI B Channel Monitoring	6-73
PPP on BRI Monitoring	6-74
DDR Configuration Test	6-75
Summary	6-77
Next Steps	6-77
Quiz	6-78
Quiz Answer Key	6-80

<i>Using DDR Enhancements</i>	7-1
Overview	7-1
Objectives	7-1
Outline	7-1
Describing the Dialer Profile	7-3
Overview	7-3
Relevance	7-3
Objectives	7-3
Learner Skills and Knowledge	7-3
Outline	7-4
Dialer Profile	7-5
Dialer Profile Features	7-7
Dialer Profile Elements	7-9
Dialer Map Classes	7-10
Summary	7-11
Quiz	7-12
Quiz Answer Key	7-13
Configuring Dialer Profiles	7-15
Overview	7-15
Relevance	7-15
Objectives	7-15
Learner Skills and Knowledge	7-15
Outline	7-16
Dialer Profile Configuration Concepts and Commands	7-17
Typical Dialer Profile Application	7-18
Configuration of Dialer Interfaces	7-19
Configuration of Physical Interfaces	7-22
Dialer Profiles Configuration Example	7-24
Summary	7-25
Quiz	7-26
Quiz Answer Key	7-27
Verifying and Troubleshooting a Dialer Profile Configuration	7-29
Overview	7-29
Relevance	7-29
Objectives	7-29
Learner Skills and Knowledge	7-29
Outline	7-30
Verification of Dialer Profiles	7-31
Outbound Dialing Issues	7-33
Outbound Binding Issues	7-34
Examples	7-36
Inbound Call Issues	7-38
Disconnect Issues	7-40
Summary	7-42
Next Steps	7-42
Quiz	7-43
Quiz Answer Key	7-45

Table of Contents

Volume 3

<u>Configuring Frame Relay with Traffic Shaping</u>	8-1
Overview	8-1
Objectives	8-1
Outline	8-1
<u>Reviewing Frame Relay</u>	8-3
Overview	8-3
Relevance	8-3
Objectives	8-3
Learner Skills and Knowledge	8-3
Outline	8-4
Frame Relay Overview	8-5
Frame Relay Operation	8-6
Data-Link Connection Identifier	8-7
DLCI-to-Address Mappings	8-7
Frame Relay Signaling	8-8
Local Management Interface	8-8
Summary	8-10
Quiz	8-11
Quiz Answer Key	8-12
<u>Configuring Frame Relay</u>	8-13
Overview	8-13
Relevance	8-13
Objectives	8-13
Learner Skills and Knowledge	8-13
Outline	8-14
Configuration of Basic Frame Relay	8-15
Dynamic Address Mapping	8-16
Configuration of Static Address Mapping	8-17
Different DLCIs at the Remote Routers	8-19
Hub-and-Spoke Topology	8-20
Spoke Router	8-22
Summary	8-23
Quiz	8-24
Quiz Answer Key	8-25
<u>Verifying Frame Relay Configuration</u>	8-27
Overview	8-27
Relevance	8-27
Objectives	8-27
Learner Skills and Knowledge	8-27
Outline	8-27
Verification of Frame Relay Operation	8-28
Summary	8-34
Quiz	8-35
Quiz Answer Key	8-36
<u>Configuring Frame Relay Subinterfaces</u>	8-37
Overview	8-37
Relevance	8-37
Objectives	8-37
Learner Skills and Knowledge	8-38
Outline	8-38
Reachability Issues with Routing Updates	8-39
Resolution of Reachability Issues	8-40

Subinterface Usages	8-41
Point-to-Point Subinterfaces	8-42
Multipoint Subinterfaces	8-43
Configuration of Subinterfaces	8-44
Subinterface Configuration Example	8-46
Summary	8-48
Quiz	8-49
Quiz Answer Key	8-50
Identifying Frame Relay Traffic Shaping Features	8-51
Overview	8-51
Relevance	8-51
Objectives	8-51
Learner Skills and Knowledge	8-51
Outline	8-52
Frame Relay Traffic Flow Terminology	8-53
Traffic Shaping Over Frame Relay	8-55
Summary	8-57
Quiz	8-58
Quiz Answer Key	8-59
Configuring Frame Relay Traffic Shaping	8-61
Overview	8-61
Relevance	8-61
Objectives	8-61
Learner Skills and Knowledge	8-61
Outline	8-62
Step 1: Configuration of FRTS	8-63
Step 2: Configuration of FRTS	8-64
Steps 3-5: Configuration of FRTS	8-67
Traffic-Shaping Rate Enforcement	8-68
Traffic-Shaping Rate Enforcement Configuration Example	8-69
Traffic-Shaping BECN Support Example	8-71
Traffic-Shaping BECN Support Configuration Example	8-72
Traffic-Shaping Example	8-74
Verification of FRTS	8-75
<i>show traffic-shape</i> Command	8-76
<i>show traffic-shape statistics</i> Command	8-77
Summary	8-78
Next Steps	8-78
Quiz	8-79
Quiz Answer Key	8-81
Implementing DDR Backup	9-1
Overview	9-1
Objectives	9-1
Outline	9-1
Configuring Dial Backup	9-3
Overview	9-3
Relevance	9-3
Objectives	9-3
Learner Skills and Knowledge	9-4
Outline	9-4
Dial Backup Overview	9-5
Dial Backup for High Primary Line Usage	9-6
Activation of Backup Interfaces for Primary Line Failures	9-7

Activation of Dial Backup	9-9
Dial Backup Activation Example	9-10
Configuration of Dial Backup for Excessive Traffic Load	9-11
Configuration Example of Dial Backup for Excessive Traffic Load	9-13
Backup Limitations with Physical Interfaces	9-14
Dial Backup with Dialer Profile	9-15
Configuration of a Backup Dialer Profile	9-16
Dialer Profile Backup Example	9-19
Summary	9-20
Quiz	9-21
Quiz Answer Key	9-24
Routing with the Load Backup Feature	9-25
Overview	9-25
Relevance	9-25
Objectives	9-25
Learner Skills and Knowledge	9-26
Outline	9-26
Load Sharing with OSPF and EIGRP	9-27
Verification of Dial Backup Configuration	9-30
Configuration of Floating Static Routes as Backup	9-31
Dialer Watch as Backup	9-33
Configuration of Dialer Watch	9-35
Summary	9-37
Next Steps	9-37
Quiz	9-38
Quiz Answer Key	9-40
Using QoS in Wide-Area Networks	10-1
Overview	10-1
Objectives	10-1
Outline	10-2
Identifying Quality of Service Models and Tools	10-3
Overview	10-3
Relevance	10-3
Objectives	10-3
Learner Skills and Knowledge	10-3
Outline	10-4
Quality of Service Defined	10-5
Converged Networks: Quality Issues	10-6
QoS Considerations	10-8
QoS Application Requirements	10-9
QoS Models	10-10
QoS Mechanisms	10-11
QoS Mechanisms and Remote Access	10-12
Congestion Avoidance: Random Early Detection	10-13
Congestion Avoidance: Weighted Random Early Detection	10-14
Effective Use of Traffic Prioritization	10-16
Queuing Overview	10-17
Establishing a Queuing Policy	10-18
Cisco IOS Queuing Options	10-20
Link Efficiency Usage	10-22
Summary	10-23
Quiz	10-24
Quiz Answer Key	10-26

Configuring Congestion Management	10-27
Overview	10-27
Relevance	10-27
Objectives	10-27
Learner Skills and Knowledge	10-28
Outline	10-28
WFQ Operation	10-29
Configuring WFQ	10-33
WFQ Example	10-34
CBWFQ Operation	10-35
CBWFQ vs. Flow-Based WFQ	10-36
Step 1: Configuring CBWFQ	10-37
Step 2a: Configuring CBWFQ with Tail Drop	10-39
Step 2b: Configuring CBWFQ with WRED	10-40
Step 2c: Configuring CBWFQ Default Class (Optional)	10-42
Step 3: Configuring CBWFQ	10-43
CBWFQ Example	10-44
LLQ Operation	10-46
Configuring LLQ	10-47
Summary	10-49
Quiz	10-50
Quiz Answer Key	10-52
Verifying Congestion Management	10-53
Overview	10-53
Relevance	10-53
Objectives	10-53
Learner Skills and Knowledge	10-53
Outline	10-54
Verification of Queuing Operation	10-55
Queuing Comparison Summary	10-58
Summary	10-59
Quiz	10-60
Quiz Answer Key	10-61
Implementing Link Efficiency	10-63
Overview	10-63
Relevance	10-63
Objectives	10-63
Learner Skills and Knowledge	10-63
Outline	10-64
Compression Overview	10-65
Link Compression over a Point-to-Point Connection	10-66
Payload Compression Implementation	10-67
TCP/IP Header Compression	10-68
Microsoft Point-to-Point Compression	10-69
Other Compression Considerations	10-70
Data Compression	10-71
Summary	10-72
Next Steps	10-72
Quiz	10-73
Quiz Answer Key	10-75

<i>Using AAA to Scale Access Control</i>	<i>11-1</i>
Overview	11-1
Objectives	11-1
Outline	11-1
<i>Identifying Cisco Access Control Solutions</i>	<i>11-3</i>
Overview	11-3
Relevance	11-3
Objectives	11-3
Learner Skills and Knowledge	11-3
Outline	11-4
Cisco Access Control Solutions Overview	11-5
Basic Security Devices and Router Security	11-6
Cisco Security Options Overview	11-8
Cisco Secure ACS Overview	11-9
Cisco Secure ACS Components	11-10
Cisco Secure ACS Administrator GUI Client	11-11
Summary	11-12
Quiz	11-13
Quiz Answer Key	11-14
<i>Defining and Configuring AAA</i>	<i>11-15</i>
Overview	11-15
Relevance	11-15
Objectives	11-15
Learner Skills and Knowledge	11-15
Outline	11-16
AAA Definitions	11-17
AAA Overview and Configuration	11-18
Router Access Modes	11-19
AAA Protocols	11-20
AAA and the Cisco Secure ACS	11-21
AAA Authentication Commands	11-23
Character Mode Login Example	11-24
AAA Authorization Commands	11-25
Character Mode with Authorization	11-26
Packet Mode Example	11-27
AAA Accounting Commands	11-28
AAA Accounting Example	11-29
Summary	11-30
Next Steps	11-30
Quiz	11-31
Quiz Answer Key	11-33
<i>Course Glossary</i>	<i>1</i>

Course Introduction

Overview

Building Cisco Remote Access Networks (BCRAN) v2.1 is an instructor-led course presented by Cisco Systems training partners to end-user customers. This five-day course focuses on how to use one or more of the available permanent or dialup WAN technologies to connect company sites. In addition, network security and general security components are presented.

Outline

The Course Introduction includes these topics:

- Course Objectives
- Course Activities
- Cisco Certifications
- Learner Skills and Knowledge
- Learner Responsibilities
- General Administration
- Course Flow Diagram
- Icons and Symbols
- Learner Introductions

Course Objectives

This topic lists the course objectives.

Course Objectives

Cisco.com

Upon completing this course, you will be able to:

- **Interconnect network devices used for WANs**
- **Build a functional configuration to support network requirements**
- **Verify the functionality of the network**
- **Determine network device operational status and performance**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3

Course Objectives (Cont.)

Cisco.com

Upon completing this course, you will be able to:

- **Manage device configuration files**
- **Configure access lists to meet requirements**
- **Use show commands to display network operational performance**
- **Use debug commands to detect processes and anomalies**

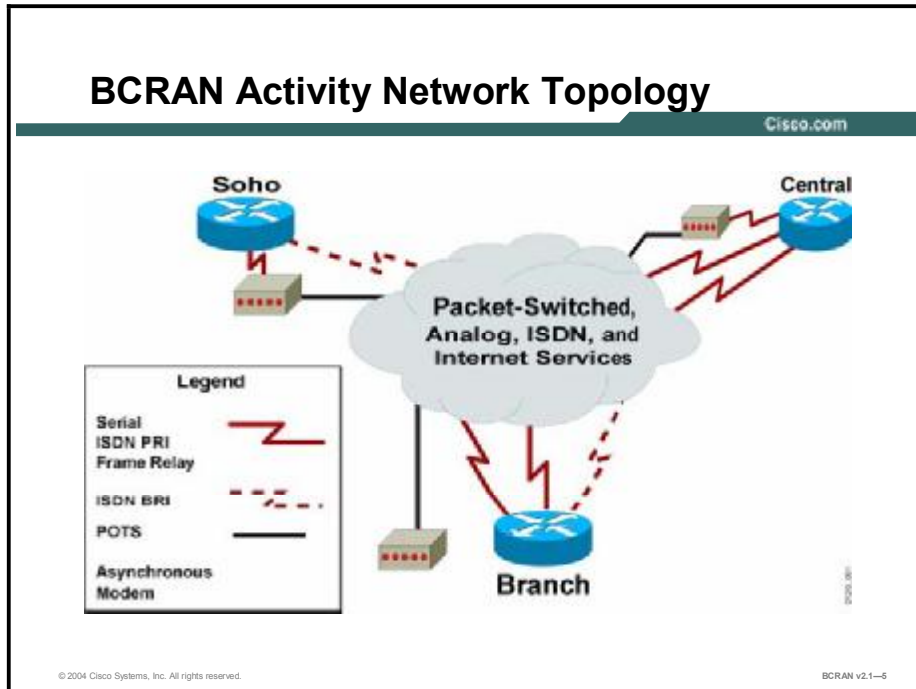
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4

Upon completing this course, you will be able to meet these objectives:

- Interconnect network devices as specified by a design and installation plan
- Build a functional configuration to support specified network operational requirements
- Verify the functionality of a network to ensure that it operates as specified
- Verify network connectivity to non-Cisco devices
- Accurately determine network device operational status and network performance using the command-line interface
- Manage device configuration files to reduce device downtime according to best practices using Cisco IOS commands
- Configure access lists to meet specified operational requirements using the command-line interface
- Display network operational parameters using the appropriate **show** commands so that you can detect anomalies
- Monitor network operational parameters using the appropriate **debug** commands so that you can detect anomalies

Course Activities

This topic discusses the enterprise WAN network that you will build in this course.



During the lab exercises in this course, you will build the network depicted in the figure. To accomplish this task, you will practice the following:

- Assembling and cabling WAN components
- Supporting asynchronous modems
- Configuring PPP features
- Accessing broadband
- Using Virtual Private Networks (VPNs) with IP Security (IPSec)
- Using ISDN and dial-on-demand routing (DDR) to enhance remote connectivity
- Using DDR enhancements
- Configuring a Frame Relay connection with traffic shaping
- Implementing DDR backup
- Using quality of service (QoS) in WANs
- Using authentication, authorization, and accounting (AAA) to scale access control

Cisco Certifications

This topic discusses Cisco career certifications and paths.

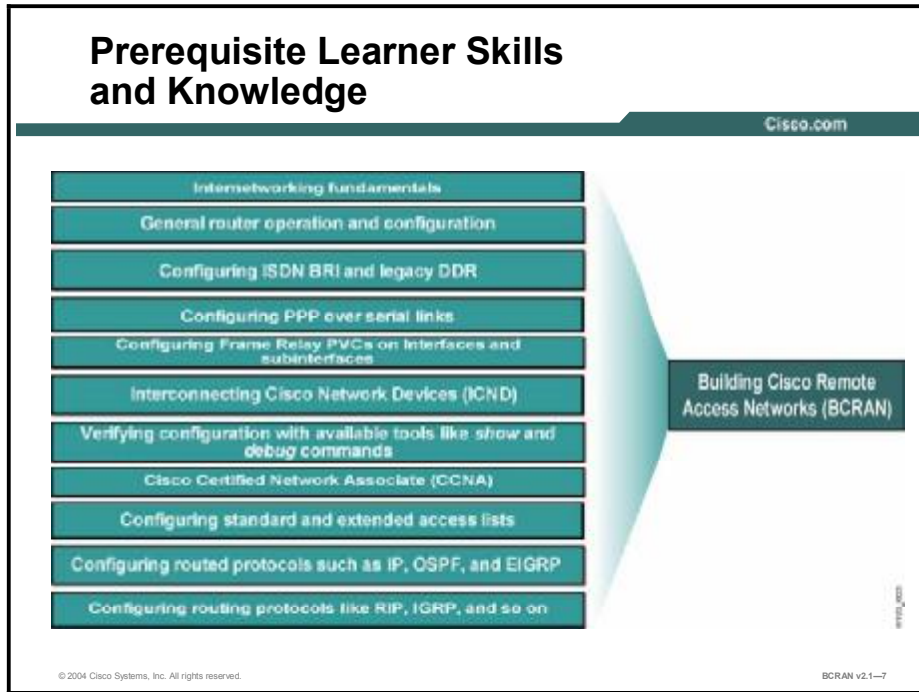


Cisco provides three levels of general career certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused Cisco Qualified Specialist (CQS) certifications for designated areas such as cable communications, voice, and security.

There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to <http://www.cisco.com/go/certifications>.

Learner Skills and Knowledge

This topic lists the course prerequisites.




Before attending the BCRAN course, you must have basic knowledge of data networking equivalent to the information in the *Introduction to Cisco Networking Technologies* (INTRO) course and the *Interconnecting Cisco Network Devices* (ICND) course. Experience working in a network environment is recommended.

Learner Responsibilities

This topic discusses the responsibilities of the learners.

Learner Responsibilities

Cisco.com



- **Complete prerequisites**
- **Introduce yourself**
- **Ask questions**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8

To take full advantage of the information presented in this course, you must have completed the prerequisite requirements.

In class, you are expected to participate in all lesson exercises and assessments.

In addition, you are encouraged to ask any questions relevant to the course materials.

If you have pertinent information or questions concerning future Cisco product releases and product features, please discuss these topics during breaks or after class. The instructor will answer your questions or direct you to an appropriate information source.

General Administration

This topic lists the administrative issues for the course.

General Administration

Cisco.com

Class-Related	Facilities-Related
<ul style="list-style-type: none">• Sign-in sheet• Length and times• Course materials• Attire	<ul style="list-style-type: none">• Break and lunch room locations• Site emergency procedures• Rest rooms• Telephones/faxes

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-9

The instructor will discuss these administrative issues:

- Sign-in process
- Starting and anticipated ending times of each class day
- Class breaks and lunch facilities
- Appropriate attire during class
- Materials that you can expect to receive during class
- What to do in the event of an emergency
- Location of the rest rooms
- How to send and receive telephone and fax messages

Course Flow Diagram

This topic covers the suggested flow of the course materials.

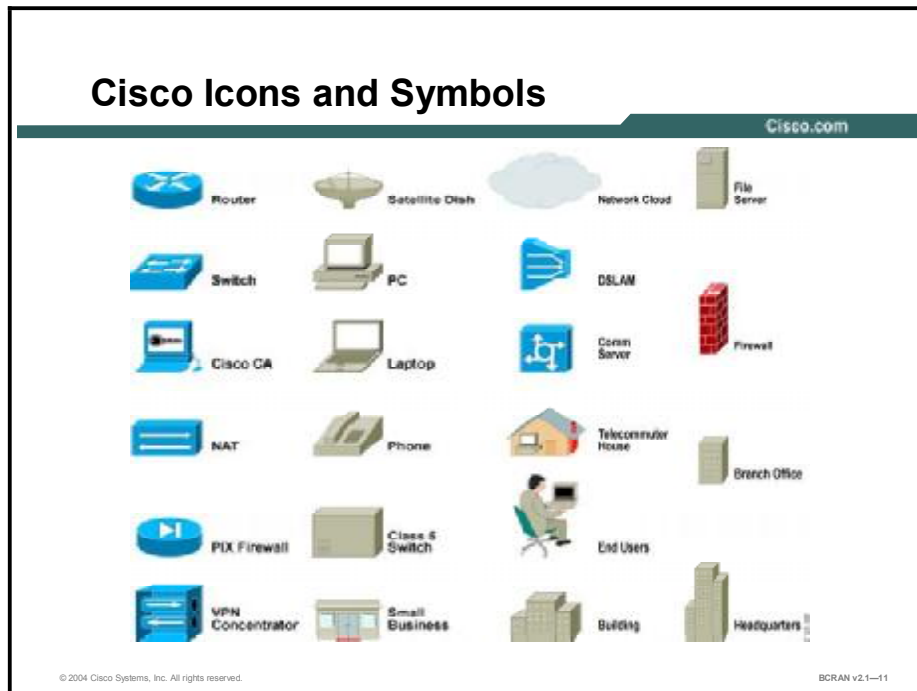
		Day 1	Day 2	Day 3	Day 4	Day 5
A M	Course Introduction		Module 3: Configuring PPP Features (cont.)	Module 5: Virtual Private Networks (cont.)	Module 7: Using DDR Enhancements (cont.)	Module 10: Using QoS in Wide-Area Networks
	Module 1: WAN Technologies and Components				Module 8: Configuring Frame Relay with Traffic Shaping	
	Module 2: Supporting Asynchronous Modems		Module 4: Accessing Broadband	Module 6: Using ISDN and DDR to Enhance Remote Connectivity		
Lunch						
P M	Module 2: Supporting Asynchronous Modems (cont.)		Module 4: Accessing Broadband	Module 6: Using ISDN and DDR to Enhance Remote Connectivity (cont.)	Module 8: Configuring Frame Relay with Traffic Shaping (cont.)	Module 11: Using AAA to Scale Access Control
	Module 3: Configuring PPP Features		Module 5: Virtual Private Networks	Module 7: Using DDR Enhancements	Module 9: Implementing DDR Backup	Super Lab

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-10

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab exercises. The exact timing of the subject materials and labs depends on the pace of your specific class.

Icons and Symbols

This topic shows the Cisco icons and symbols used in this course.




Learner Introductions

This is the point in the course where you introduce yourself.

Learner Introductions

Cisco.com

- **Your name**
- **Your company**
- **Skills and knowledge**
- **Brief history**
- **Objective**



© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-12

Prepare to share the following information:

- Your name
- Your company
- If you have most or all of the prerequisite skills
- A profile of your experience
- What you would like to learn from this course

Module 1

WAN Technologies and Components

Overview

This module discusses various remote access technologies and considerations for an enterprise that is building its corporate network. This module also addresses Cisco Systems product selection information.

Objectives

Upon completing this module, you will be able to:

- Explain the advantages and disadvantages of a variety of WAN connection types
- Select the appropriate WAN connection types
- Select Cisco equipment that will suit the specific needs of each site
- Use Cisco tools to select the proper equipment

Outline

The module contains these lessons:

- Defining WAN Connection Types
- Defining WAN Encapsulation Protocols
- Determining the WAN Type to Use
- Selecting Cisco Products for Remote Connections

Defining WAN Connection Types

Overview

This lesson provides an overview of WAN connection types and explains some advantages and disadvantages of each.

Relevance

It is important to understand how to select the appropriate WAN connection type that best meets the needs and budget of the customer.

Objectives

Upon completing this lesson, you will be able to:

- Describe the characteristics of WAN connections
- Identify the types of WAN connections
- Describe dedicated circuit-switched WAN connections
- Describe on-demand circuit-switched WAN connections
- Identify packet-switched WAN connections
- Describe selected broadband access connections
- Describe various DSL connections
- Describe cable connections

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- WAN Connection Characteristics
- Common WAN Connection Types
- Dedicated Circuit-Switched Connections
- On-Demand Circuit-Switched Connections
- ISDN Connections
- Packet-Switched Virtual Connections
- Broadband Access
- Summary
- Quiz

WAN Connection Characteristics

This topic describes various WAN connection types.

WAN Connection Characteristics		
Cisco.com		
Connection Duration	Dedicated	On Demand
Switching	Circuit	Packet
Synchronization	External	Embedded
Data Rate	Narrowband	Broadband
Termination	End-to-End	Transport network
Media	Copper	Fiber
	- Twisted Pair	- Multimode
	- Coaxial	- Single-Mode

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1-2

Many significant WAN connection characteristics can be grouped into these categories:

- Connection duration
 - Dedicated
 - Always *on*
 - Cost typically related to bandwidth and distance
 - On demand
 - Connected on demand
 - Cost related to time of usage, bandwidth, and distance
- Switching
 - Circuit-switched
 - End-to-end bandwidth allocation and control
 - Provisioned permanently or on demand
 - Packet-switched
 - Asynchronous transport network
 - Statistical bandwidth allocation in transport network
 - Cost typically related to bandwidth guarantee and other quality of service (QoS) parameters

- Synchronization mechanism
 - External
 - Clocking determined by separate conductor in the media
 - Thicker cable with more conductors per connection
 - Embedded
 - Clocking determined by bit times within the data stream
 - Fewer conductors per connection
- Data rate
 - Narrowband
 - Rates up to and including 128 kbps.
 - Broadband
 - Data rates greater than narrowband rate. Exact dividing line is more marketing than technology. Greater than ISDN BRI and equal to or less than T1.
- Termination
 - End-to-end circuits
 - Bit synchronization and data-link termination managed at ends of circuit. Appearance of increased control. Service provider transparent.
 - Transport network
 - Intermediate network terminates bit synchronization, content carried asynchronously across transport network. Includes packet switching (Frame Relay and ATM) and broadband access technologies.
- Transmission media
 - Copper: Cheaper for lower data rates and shorter distances
 - Twisted pair
 - Coaxial cable
 - Fiber: More expensive for high data rates and longer distances
 - Multimode
 - Single-mode

Common WAN Connection Types

This topic describes the more common types of WAN connections.

Common WAN Connection Types

Cisco.com

- **Dedicated Circuit-Switched**
- **On-Demand Circuit-Switched**
- **Packet-Switched Virtual Circuit**
- **Broadband Access**

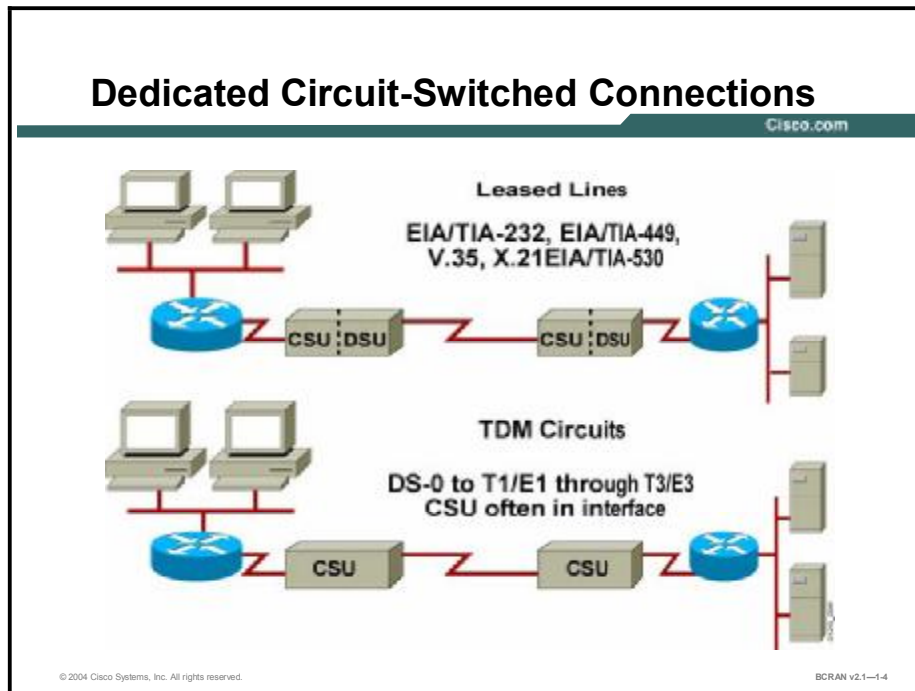
© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-1-3

For the purposes of this discussion, WAN connections have been grouped into four general categories that reflect generally available WAN services:

- Dedicated circuit-switched
- On-demand circuit-switched
- Packet-switched virtual circuit
- Broadband access

Dedicated Circuit-Switched Connections

This topic describes dedicated circuit-switched WAN connections.



Leased-line serial connections typically connect to a transport service provider through a DCE device, which provides clocking and transforms the signal to the channelized format that is used in the service provider network. These point-to-point dedicated links provide a single, preestablished WAN communications path from the customer circuit-switched premises, through a carrier network, to a remote network. Dedicated lines through T3/E3 rates are frequently described as leased lines. The established path is permanent and fixed for each remote network that is reached through the carrier facilities. The service provider reserves the full-time private use of the customer circuits through the transport network.

Synchronization of timing and data-link control is preserved end to end. These dedicated connections are made using the synchronous serial ports on the router with bandwidth of up to 34 Mbps over a service provider E3 transport link and 45 Mbps over T3. Different encapsulation methods at the data-link layer provide flexibility and reliability for user traffic. Typical connections on a dedicated network WAN connection employ 56-kbps, 64-kbps, T1, E1, T3, and E3 data rates.

These synchronous serial standards are supported on Cisco routers through serial interfaces:

- EIA/TIA-232
- EIA/TIA-449
- V.35
- EIA/TIA-530

In North America, the connecting device is called a CSU/DSU. The CSU connects to the service provider network, while the DSU connects to the network device serial interface. The CSU/DSU is a device (or sometimes two separate digital devices) that adapts the media format from a serial DTE device, such as a router, to the media format of the service provider equipment, such as a WAN switch, in a switched carrier network. The CSU/DSU also provides signal clocking for synchronization between these devices. The figure shows the placement of the CSU/DSU.

It is increasingly common to have direct connections to the carrier transport network using fractional or complete T1/E1 circuits. In this case, a CSU provides demarcation and logical termination between the service provider network and the customer network. Direct T3/E3 and Synchronous Digital Hierarchy/SONET (SDH/SONET) connectivity may also be available for organizations requiring higher data rates.

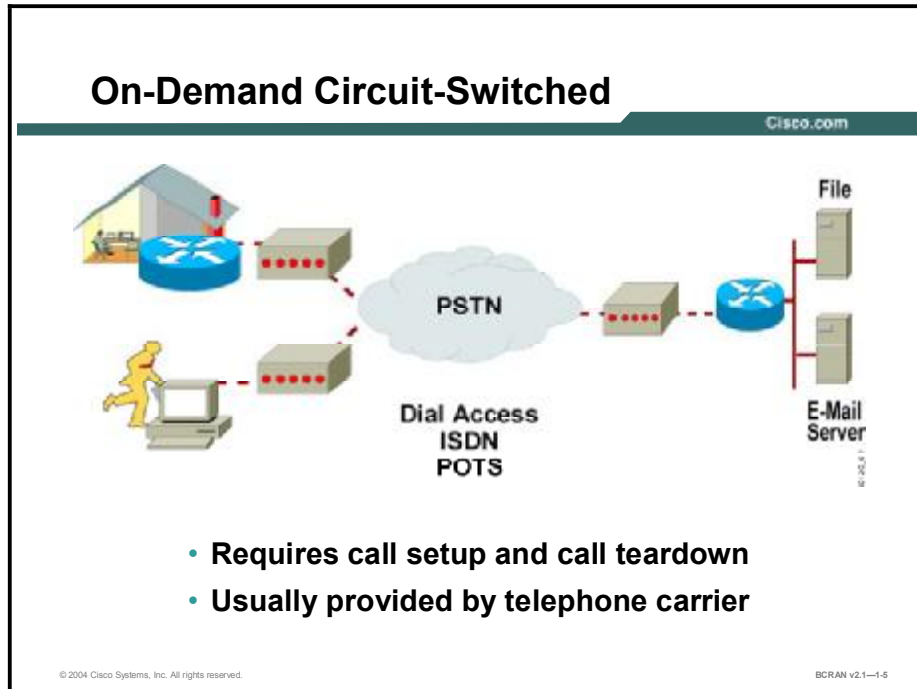
The private nature of a dedicated connection allows better control over the WAN connection. Dedicated connections also offer high speeds beyond T3/E3 levels using SDH/SONET. Dedicated connections are ideal for high-volume environments with steady-rate traffic patterns or high-peak demands of critical traffic. However, because the line is not shared, dedicated connections tend to be more costly.

As a general rule, dedicated connections are most cost-effective in these situations:

- Long connect times
- Short distances
- Critical traffic requirements that must be guaranteed

On-Demand Circuit-Switched Connections

This topic describes various switched connections.



On-demand circuit switching is a WAN transport method in which a dedicated physical circuit is established, maintained, and terminated through a public switched telephone network (PSTN) for each communication session. Initial signaling at the setup stage determines the endpoints and the connection between the two endpoints.

Typical circuit-switched connections are:

- Asynchronous modem
- ISDN BRI and ISDN PRI

Advantages of on-demand connection types include dynamic selection of the circuit endpoint and the accumulation of charges for transport only while connections are active. Costs are directly related to connection time and distance for each plain old telephone service (POTS) line or ISDN bearer (B) channel. As traffic between endpoints increases in volume, the duration of the connection increases.

Asynchronous modem connections require minimal equipment cost and use the existing telephone network. Users can easily access a central site from any location that has a telephone connection into a telephone network.

The nature of asynchronous connections allows you to configure the connection to be enabled—only when you need the service—by using dial-on-demand routing (DDR) through the modem using an asynchronous serial interface. DDR is ideal when you need short-term access only.

You should enable DDR on your asynchronous interface when:

- **Traffic volume is low or traffic is periodic:** Calls are placed and connections are established when only the router detects traffic marked as “interesting.” Periodic broadcasts, such as routing protocol updates, should be prevented from triggering a call.
- **You need a backup connection for redundancy or load sharing:** DDR can be used to provide backup load sharing and interface failure backup.

A router acts as an access server, which is a concentration point for dial-in and dial-out calls. Mobile users, for example, can call into an access server at a central site to access their e-mail messages.

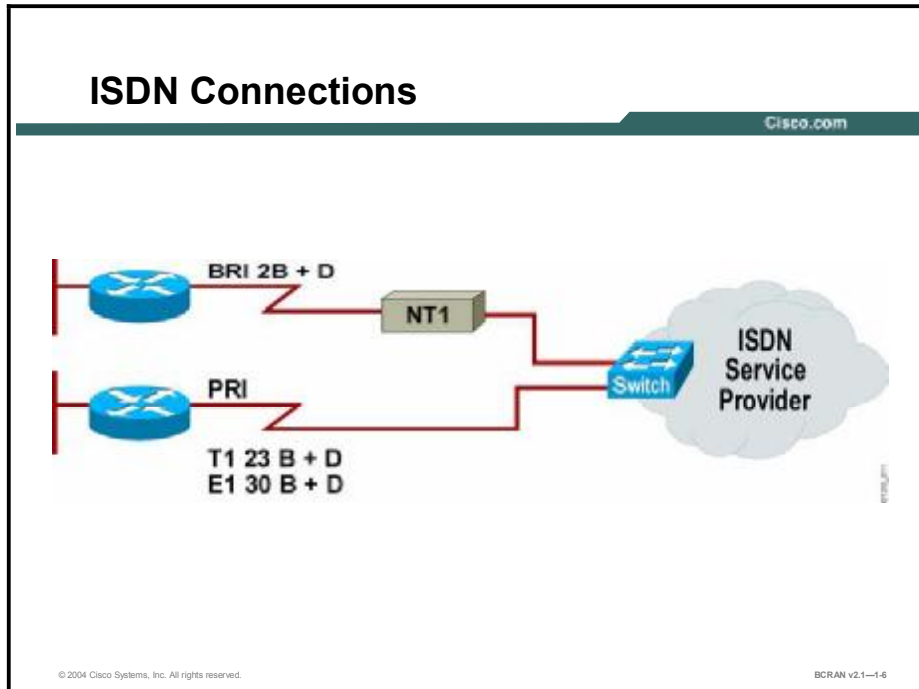
Asynchronous connections are useful in these situations:

- A backup connection required
- Small site
- Short-term on-demand access
- Periods of lower network traffic and fewer users

Asynchronous connections through the PSTN require modems at each end of the connection to convert digital data signals to analog signals that can be transported over the telephone network. Modem speeds typically vary from 19.2 kbps to 56 kbps, depending on line quality. The slower bandwidth speeds limit the amount of traffic you may want to send over an asynchronous line. To place or receive an asynchronous serial call, equip a Cisco router with an asynchronous serial interface. The serial standard to attach to an external modem is the EIA/TIA-232 standard. The interface to the telephone company varies by country. Within the United States, a standard RJ-11 adapter connects the modem to the telephone outlet.

ISDN Connections

This topic describes ISDN circuit-switched connections.



ISDN connections are typically switched connections that, like asynchronous connections, provide WAN access when needed rather than through a dedicated link. ISDN offers increased bandwidth over a typical dialup connection, faster setup, and is intended to carry data, voice, and other traffic across a telephone network.

To place an ISDN BRI call, you should equip your router with a BRI interface. You may also need an ISDN terminal adapter, which is a device that is used to connect ISDN BRI connections to other interfaces, such as EIA/TIA-232. A terminal adapter is essentially an ISDN modem. You should also consult your telephone company for information specific to your connection.

Note Generally, in Europe, the service provider supplies the Network Termination 1 (NT-1). In North America, the customer supplies the NT-1.

ISDN PRI is configured over connections such as T1 and E1 technologies. To place an ISDN call, equip your router with the proper connection. T1 is used in the United States, and E1 is common in other countries.


As with asynchronous connections, you can also configure DDR to control access for specific periods of time.

Packet-Switched Virtual Connections

This topic describes packet-switched virtual connections.

Packet-Switched Connections

Cisco.com



The diagram illustrates a packet-switched network. It features three blue routers with white 'X' marks on their faces. Two routers are positioned on the left side, and one is on the right. A central grey cloud represents the network fabric. Red lines with zig-zag patterns connect each router to the cloud, indicating virtual circuits. The Cisco logo is visible in the bottom right corner of the diagram area.

- **Virtual circuits are established.**
- **Packet-switched networks generally share bandwidth statistically.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-1-7

Packet switching is a method in which a network device uses a single point-to-point link to a service provider to transport packets intended for one or more destinations across a carrier network. Packet switching is a networking technology that is based on the transmission of data in packets. Dividing a continuous stream of data into small units (packets) enables data from one or more sources to one or more destinations to share the communication channels within the transport network.

Packet-switched networks use virtual circuits that provide end-to-end connectivity. Statically programmed switching devices accomplish physical connections. Packet headers identify the circuit and may change on each network link that is traversed. Packet switching requires the use of precise switching information throughout the transport network.

Packet-switched networks can be either privately or publicly managed. The underlying switching fabric is transparent to the network user, and the switches are responsible for the internal delivery of data across the packet-switched network only. Packet switching is implemented at the data-link layer of the Open System Interconnection (OSI) reference model.

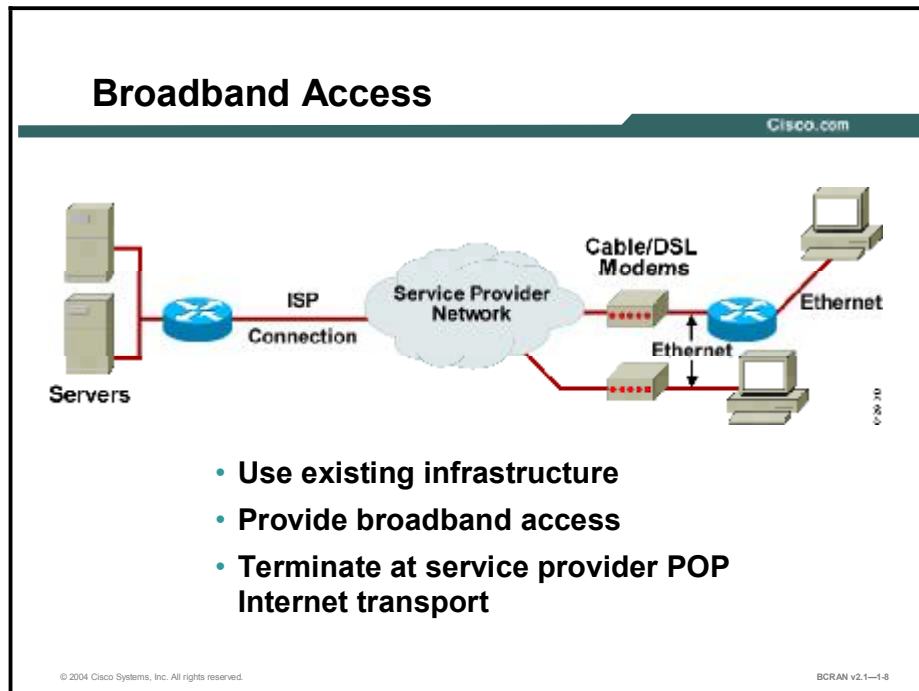
Packet-switched networks offer an administrator less control than a point-to-point connection, and the bandwidth is shared statistically. However, the cost is generally less than for a leased line. With WAN speeds comparable to those of leased lines, packet-switched networks are generally suitable for links between two large sites that require high-link utilization or present high peaks of critical traffic.

As a general rule, packet-switched connections are most cost-effective in networks with these characteristics:

- Long connect times
- Large geographic distances
- High-link utilization
- High peaks of critical traffic

Broadband Access

This topic describes two broadband access technologies.



Internet access is moving from dialup modems and slow connections to broadband access, using a variety of technologies. The technology takes advantage of existing telephone and cable television distribution infrastructures to provide broadband access to the Internet. While there is no universal definition of broadband, the Federal Communications Commission (FCC) considers advanced telecom or high speed to be defined as 200 kbps or greater. Generally, a speed of 128 kbps is adequate for most users. Broadband can allow remote office staff and small office, home office (SOHO) users to connect to the central site at higher data rates than are available with traditional on-demand technologies.

High-speed broadband access to the Internet through a broadband point of presence (POP) and then to corporate networks using secure Virtual Private Networks (VPNs) is a reality for many users in the networked world today. This broadband access has the potential to directly improve employee productivity and to provide a foundation for new voice and video business services over the Internet.

Many corporations and educational institutions have instituted broadband solutions for access by suppliers, customers, and staff. The use of the Internet for secure site-to-site connectivity using VPNs is increasing, especially for less critical traffic.

Broadband access options, in addition to the legacy dedicated circuit-switching and packet-switching technologies, include digital subscriber line (DSL) and cable modems. The most common problem in offering these broadband services to remote users is the lack of coverage because of infrastructure deficiencies.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **WAN connection types are dedicated, circuit-switched, packet-switched, and broadband.**
- **A WAN can be characterized by connection duration, type of switching, form of synchronization, data rate, termination, and media type.**
- **Dedicated serial connections are continuously available, typically using a CSU/DSU to connect to service provider TDM network.**
- **Asynchronous circuit-switched connections use a process like DDR when there is a backup connection needed.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1-9

Summary (Cont.)

Cisco.com

- **Circuit-switched ISDN connections use Link Access Procedure on the D channel for BRI signaling and use T1/E1 facilities for PRI connections.**
- **Packet-switched connections establish virtual circuits using packet headers to identify network destinations.**
- **Broadband allows increased bandwidth and new services such as VPN while using existing infrastructure via DSL or cable modem.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1-10

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which major WAN connection characteristic includes consideration of the elapsed connection time?
- A) data rate
 - B) termination
 - C) transmission media
 - D) connection duration
- Q2) Dedicated lines are also known as _____?
- A) honor lines
 - B) committed lines
 - C) leased lines
 - D) agreed lines
- Q3) Which type of router interface port is used to make dedicated permanent connections?
- A) Ethernet ports
 - B) synchronous serial ports
 - C) console ports
 - D) ISDN BRI B channels
- Q4) Which of the following conditions is appropriate for asynchronous serial connections?
- A) Your network would use them as its primary WAN connections for sending huge amounts of data traffic.
 - B) Your network needs a very reliable high-speed connection.
 - C) Your network is a small remote site and does not require a high-speed WAN connection.
 - D) Your network has five users and they send large files to a central site that is located more than 35 miles away.
- Q5) Which of the following is considered an on-demand connection?
- A) 100-Mbps LAN connection
 - B) broadband connection
 - C) T1 synchronous serial connection
 - D) ISDN BRI connection

- Q6) What physical connection is used for high-speed ISDN access in the United States?
- A) a 23B + 1D channelized T1 line
 - B) a 2B + 1D channelized BRI
 - C) a 30B + 1D channelized E1 line
 - D) an ISDN network terminal adapter
- Q7) What form does the transmission of data take in packet switching?
- A) indices
 - B) time slices
 - C) bit streams
 - D) small units
- Q8) What is the most common problem a remote user typically encounters in obtaining broadband access service?
- A) lack of area coverage by broadband providers
 - B) large initial connection fee charged by broadband providers
 - C) high cost of connections compared to other dedicated WAN services
 - D) reduced bandwidth compared to on-demand WAN services

Quiz Answer Key

- Q1) D
Relates to: WAN Connection Characteristics
- Q2) C
Relates to: Dedicated Circuit-Switched Connections
- Q3) B
Relates to: Dedicated Circuit-Switched Connections
- Q4) C
Relates to: On-Demand Circuit-Switched Connections
- Q5) D
Relates to: ISDN Connections
- Q6) A
Relates to: ISDN Connections
- Q7) D
Relates to: Packet-Switched Virtual Connections
- Q8) A
Relates to: Broadband Access

Defining WAN Encapsulation Protocols

Overview

This lesson describes the various WAN encapsulations and explains the advantages and disadvantages of each.

Relevance

It is important to understand how to select the appropriate WAN encapsulation type to provide the correct access and security level for the customer.

Objectives

Upon completing this lesson, you will be able to:

- Explain the various WAN encapsulation types that are available
- Describe the advantages of PPP encapsulation
- Describe the advantages of Frame Relay encapsulation

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

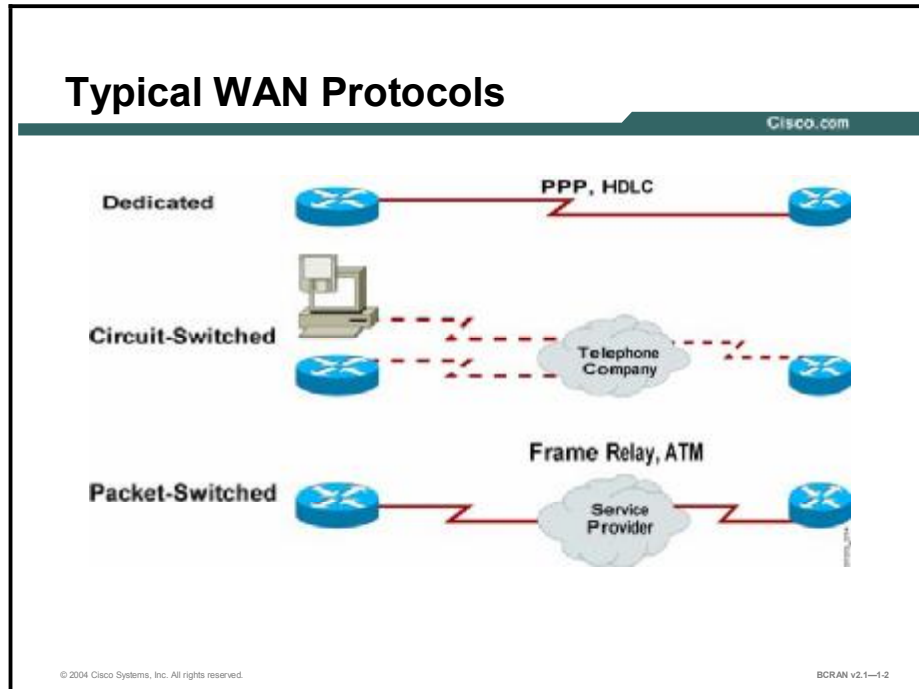
Outline

This lesson includes these topics:

- Overview
- WAN Encapsulation Protocols
- PPP Encapsulation
- Frame Relay Encapsulations
- Summary
- Quiz

WAN Encapsulation Protocols

This topic describes various WAN encapsulation protocols.



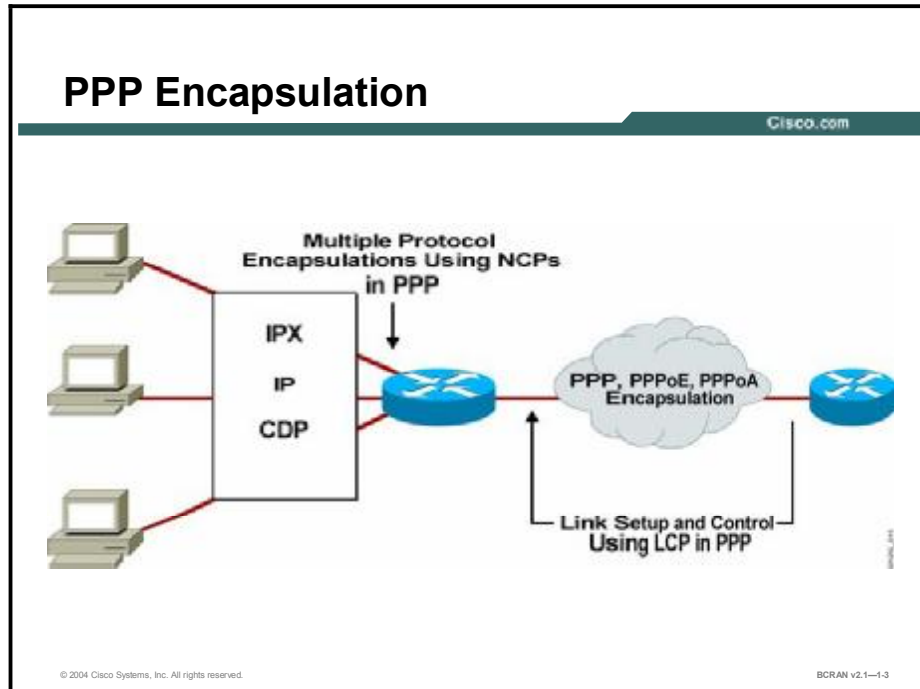
Each WAN connection uses an encapsulation protocol to encapsulate traffic while it is crossing the WAN link. To ensure that you use the correct encapsulation protocol, you must configure the Layer 2 encapsulation type to use. The choice of encapsulation protocol depends on the WAN technology and the communicating equipment. Typical WAN protocols include:

- **PPP:** PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, and error detection. In addition, PPP established option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible link control protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. The broadband connection type that is used will determine the use of Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA).
- **High-Level Data Link Control (HDLC):** HDLC is the default encapsulation type for Cisco routers on point-to-point dedicated links. It is a bit-oriented synchronous data-link layer protocol. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. HDLC is a standard that is open for interpretation. As a result, there are different versions of HDLC. If you are communicating with a device from another vendor, synchronous PPP is a more viable option.
- **Frame Relay:** Frame Relay is a high-performance packet-switched WAN protocol that operates at the physical and data-link layers of the OSI reference model. Frame Relay was originally designed for use across ISDN interfaces. Today, it is used over a variety of other network interfaces and typically operates over WAN facilities that offer more reliable connection services and a higher degree of reliability.

- **ATM:** ATM is the international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

PPP Encapsulation

This topic describes PPP encapsulation.



PPP is an international standard encapsulation that is used for these types of connections:

- Asynchronous serial
- ISDN
- Synchronous serial
- Broadband

PPP (RFC 1331) provides a standard method of encapsulating higher-layer protocols across point-to-point connections. PPP extends the HDLC packet structure with a 16-bit protocol identifier that contains information on the content of the packet.

Because it is standardized, PPP supports vendor interoperability. PPP uses its NCP component to encapsulate multiple protocols.

PPP uses another of its major components, the LCP, to negotiate and set up control options on the WAN data link. Some of the PPP LCP features covered in this course are:

- Authentication
- Compression
- Multilink

PPPoE provides the ability to connect a network of hosts to an access concentrator over a simple bridging access device. With this model, a host uses its own PPP stack, and the user is presented with a familiar user interface. Access control, billing, and type of service can be done on a per-user, rather than a per-site, basis.

PPPoA was primarily implemented as part of asymmetric DSL (ADSL) technology. It relies on RFC 1483 (now RFC 2686), operating in either logical link control/Subnetwork Access Protocol (LLC/SNAP) or virtual circuit multiplexing (VC mux) mode. Customer premises equipment (CPE) will encapsulate a PPP session based on this RFC for transport across the ADSL loop and the digital subscriber line access multiplexer (DSLAM).

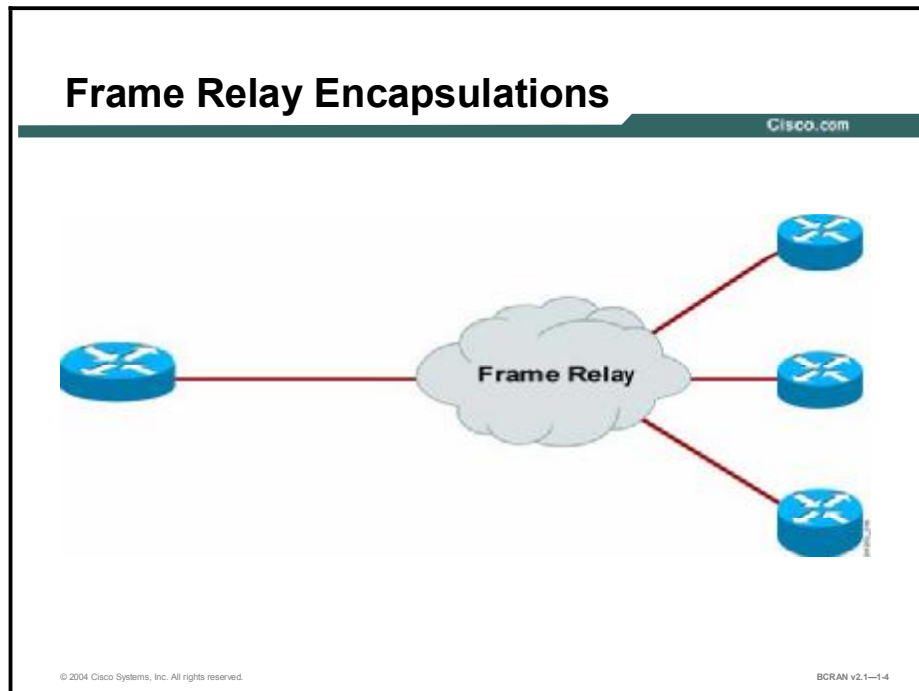
In these architectures, IP address allocation is based on IP Control Protocol (IPCP) negotiation, which follows the same principle as PPP in dial mode.

In PPPoE, the source of IP address allocation depends on the type of service to which the subscriber has subscribed and where the PPP sessions are terminated. PPPoE makes use of the dial-up networking feature of Microsoft Windows, and the IP address assigned is reflected within the PPP adapter. PPPoE can be used on existing CPE (that cannot be upgraded to PPP or that cannot run PPPoA), extending the PPP session over the bridged Ethernet LAN to the PC. PPPoE can also be configured on the CPE to terminate the PPP session and use Network Address Translation (NAT) for workstation access to the Internet.

Although PPPoA does not require host-based software, it does require that each CPE device have a username and password for authentication to a central site. The PPP sessions initiated by the subscriber are terminated at the service provider that authenticates users via a local database on the router or through a RADIUS server. The PPPoA session authentication is based on Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The service provider must assign only one IP address for the CPE, and the CPE can be configured for NAT.

Frame Relay Encapsulations

This topic describes Frame Relay encapsulations.



Frame Relay is an industry-standard data-link layer protocol that is commonly used in packet-switched networks. Frame Relay supports technological advances such as fiber-optic cabling and digital transmission. Frame Relay can eliminate time-consuming processes (such as error correction and flow control) that are necessary when using older, less reliable WAN media and protocols.

When purchasing bandwidth, customers buy a committed information rate (CIR) from the carrier to ensure that their minimum bandwidth requirements will be met. Adding an additional channel or data-link connection identifier (DLCI) will provision a new virtual circuit and set of connection characteristics. Adding more channels to an existing DLCI, where the physical facilities support it, adds bandwidth. Channels can be added easily in this manner to meet growth requirements.

Because a public network is being used, a service provider must be consulted to obtain information specific to a link.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Each WAN connection uses an encapsulation protocol to encapsulate traffic while it is crossing the WAN link.
- PPP is an international standard encapsulation used for asynchronous serial, ISDN, synchronous serial, and broadband connections.
- Frame Relay is an industry-standard data-link layer protocol commonly used in packet-switched networks.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1.5

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the fixed length of an ATM cell?
- A) 128 bytes
 - B) 56 bytes
 - C) 53 bytes
 - D) 64 bytes
- Q2) Which component does PPP use to negotiate and set up control options on the WAN data link?
- A) NCP
 - B) LCP
 - C) FTP
 - D) TFTP
- Q3) In Frame Relay, what is a DLCI?
- A) data-link control identifier
 - B) data-level control identifier
 - C) data-link connection identifier
 - D) data-level connection identifier

Quiz Answer Key

Q1) C

Relates to: WAN Encapsulation Protocols

Q2) B

Relates to: PPP Encapsulation

Q3) C

Relates to: Frame Relay Encapsulations

Determining the WAN Type to Use

Overview

This lesson describes how to select the appropriate WAN connection for a given situation.

Relevance

When you design internetworks, you must make several key decisions concerning connectivity among different users or groups in your WAN environment.

Objectives

Upon completing this lesson, you will be able to:

- Describe the various aspects of selecting the correct WAN connection
- Distinguish among various WAN connections by speed and cost
- Describe the requirements of a central site
- Describe the requirements of a branch office site
- Describe the requirements of a SOHO site
- Select the appropriate WAN equipment for a CO site
- Select the appropriate WAN equipment for a branch office site
- Select the appropriate WAN equipment for a SOHO site
- Identify the appropriate interfaces that will support your WAN connection
- Verify that the router components are installed and functioning properly

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- WAN Connection Types
- WAN Connection Speed Comparison
- WAN Connection Summary
- Site Requirements
- Central Site Considerations
- Central Site Router Equipment
- Branch Office Considerations
- Branch Office Router Equipment
- SOHO Site Considerations
- SOHO Site Router Equipment
- Summary
- Quiz

WAN Connection Types

This topic describes how to select a WAN connection.

Connection Selection Considerations

Cisco.com

- **Availability**
- **Bandwidth**
- **Cost**
- **Ease of management**
- **Application traffic**
- **QoS and reliability**
- **Access control**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-1-2

When you design internetworks, you must make several key decisions concerning connectivity among different users or groups of users in your WAN environment.

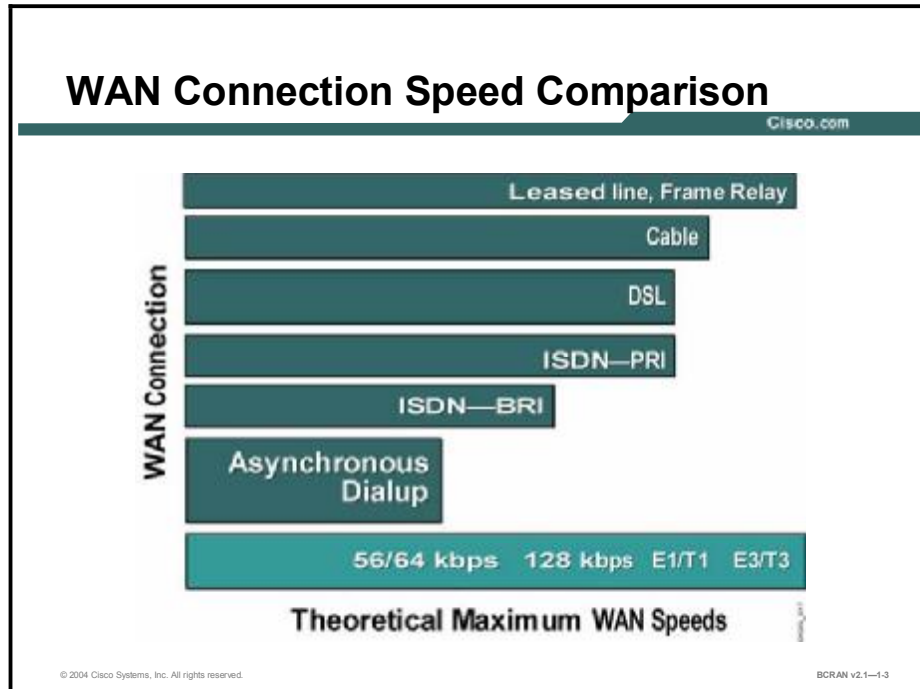
When selecting a WAN connection, you should consider these factors:

- **Availability:** Each method of connectivity has limits to its availability that is inherent in its design, usage, and implementation. For example, Frame Relay is not available in all geographic regions.
- **Bandwidth:** WAN bandwidth is expensive, and organizations do not want to pay for more bandwidth than they need. Determining usage over the WAN is a necessary step in evaluating the most cost-effective WAN services for your needs.
- **Cost:** WAN usage costs are typically 80 percent of the entire information services budget. Cost is a major consideration when different WAN services and different service providers are being evaluated. If, for example, you use the line for only 1 hour a day, you may want to select a DDR connection such as an asynchronous or ISDN connection.
- **Ease of management:** Network designers are often concerned about the degree of difficulty associated with managing connections. Connection management refers to both the initial configuration at startup and the ongoing configuration tasks of normal operation. Traffic management is the ability of the connection to adjust to different rates of traffic, regardless of whether the traffic is steady or bursty in nature. Dedicated lines are often easier to manage than shared lines.
- **Application traffic:** The application traffic may be many small packets, such as a terminal session, or very large packets, such as a file transfer.

- **Quality of service (QoS) and reliability:** How critical is the traffic that is intended to travel over the link? A backup connection may be necessary.
- **Access control:** A dedicated connection may help control access, but electronic commerce cannot occur on a wide scale unless consumers can access some portion of your network.

WAN Connection Speed Comparison

This topic describes various WAN speeds.



The figure illustrates the WAN speeds for typical technologies. Network administrators must select a WAN option based on the required bandwidth.

The speeds, costs, and availability of WANs vary internationally. For example, in North America, high-bandwidth speeds such as T1 are easily available at reasonable prices. Europe offers comparable speeds, such as E1, but prices tend to be higher. Other parts of the world offer limited WAN services with lower speeds, typically up to 64 kbps, and the costs are higher.

Broadband options include DSL and high-speed cable modems.

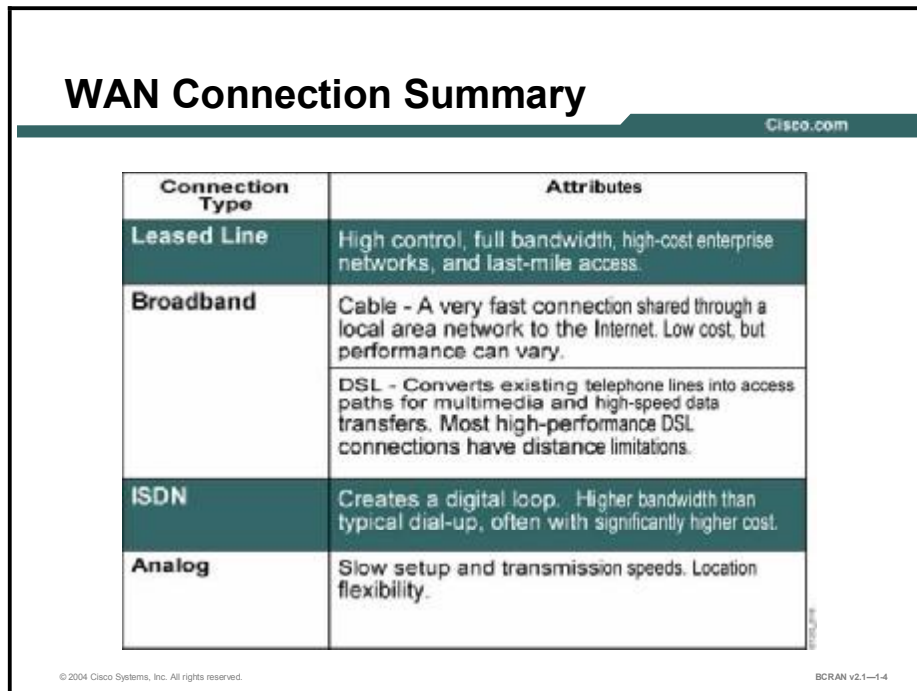
Broadband is generally defined as any sustained speed above 128 kbps. However, that definition may soon change. Broadband access can allow remote office staff and small office, home office (SOHO) users to connect to the central office LAN at high speeds.

A cable modem can provide up to 90 times the speed (4 Mbps) for remote access.

DSL is a technology that operates over unused bandwidth on a regular telephone line to deliver fast digital data transmission up to 25 times the speed (approximately 1 Mbps) without affecting the analog telephone service that is used.

WAN Connection Summary

This topic discusses a summary of WAN connections.



The figure is a table titled "WAN Connection Summary" with a Cisco.com logo in the top right corner. The table has two columns: "Connection Type" and "Attributes". It lists five types of WAN connections: Leased Line, Broadband (Cable and DSL), ISDN, and Analog, each with a brief description of its characteristics.

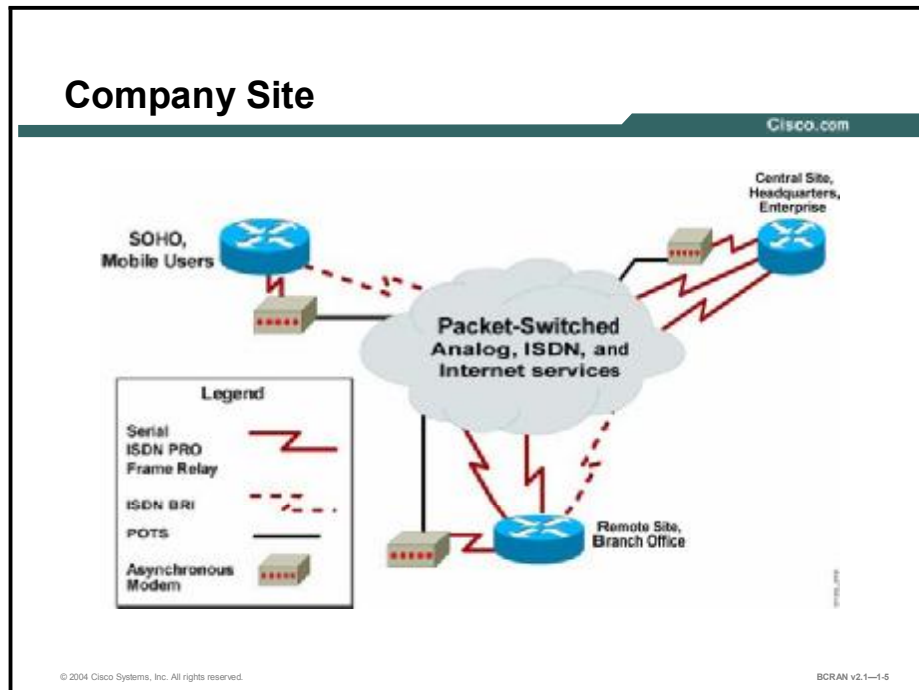
Connection Type	Attributes
Leased Line	High control, full bandwidth, high-cost enterprise networks, and last-mile access.
Broadband	Cable - A very fast connection shared through a local area network to the Internet. Low cost, but performance can vary.
	DSL - Converts existing telephone lines into access paths for multimedia and high-speed data transfers. Most high-performance DSL connections have distance limitations.
ISDN	Creates a digital loop. Higher bandwidth than typical dial-up, often with significantly higher cost.
Analog	Slow setup and transmission speeds. Location flexibility.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-14

The figure compares the attributes of various types of WAN connections. Each WAN connection has advantages and disadvantages. For example, setting up a dialup asynchronous connection will offer limited bandwidth only. However, a user can call into the office from anywhere over the existing telephone network.

Site Requirements

This topic describes the factors that a network administrator must evaluate for central site, branch office, and SOHO WAN connections.



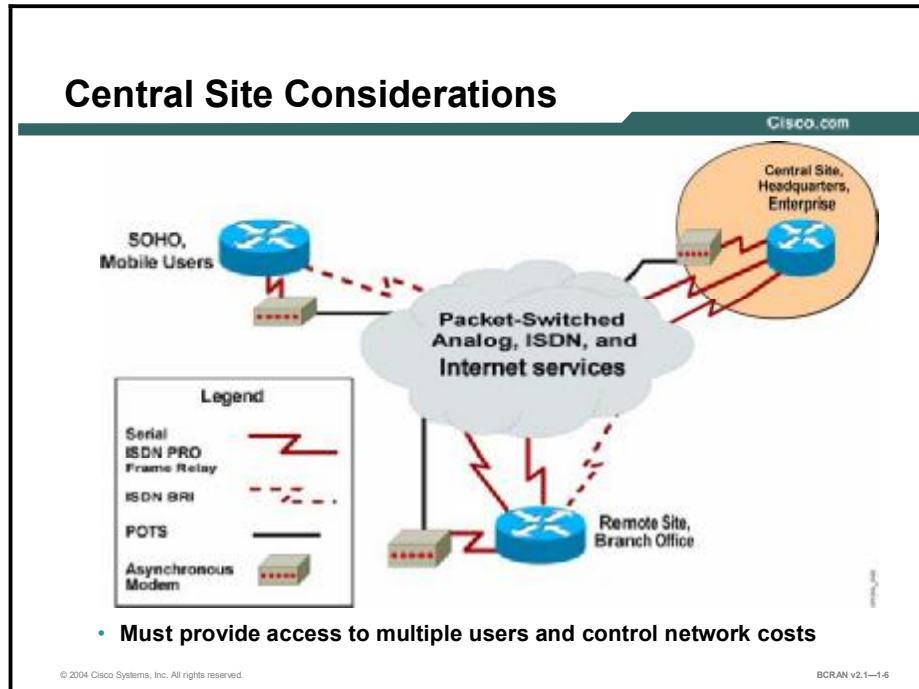
A company with multiple sites that vary in size will need a remote network to connect the various locations. Typical locations include these sites:

- **Central site:** The central site is a large site that is often the corporate headquarters or a major office. Regional offices and SOHOs may need to connect to this site for data and information. Because users may access this site via multiple WAN technologies, it is important that the central site accommodate many types of WAN connections from remote locations. The central site is often referred to as headquarters, the enterprise, or corporate.
- **Remote site:** The remote site is a smaller office that generally accommodates employees who have a compelling reason to be located away from the central site, such as a regional salesperson. Remote site users must be able to connect to the central site to access company information. Remote sites are sometimes called branch offices, remote offices, or sales offices. Small and medium-size businesses can benefit from high-speed Internet access, VPN connectivity to corporate intranets, telecommuting capabilities for work-at-home employees, interactive television, and economical PSTN-quality voice and fax calls over the managed IP networks. Employees of large and small businesses who work from their homes need secure high-speed remote access to the corporate intranet and need access to the Internet for e-mail communication with customers and suppliers.

- **SOHO site:** This SOHO site is a small office with one to several employees or the home office of a telecommuter. Telecommuters may also be mobile users, that is, users who need access while traveling or who do not work at a fixed company site. Depending on the amount of use and the WAN services available, telecommuters working from home tend to use dialup and broadband services. Mobile users tend to access the company network via an asynchronous dialup connection through the telephone company or may access the corporate intranet using VPN client software on their laptops. Telecommuters working from home may also use a VPN tunnel gateway router for encrypted data and voice traffic from the company intranet. These solutions provide simple and safe access for branch offices or SOHOs to the corporate network site, according to the needs of the users at the sites.

Central Site Considerations

This topic describes central site considerations.



The central site WAN connection is a critical focal point for a company. Because many other sites and users access this site in a variety of ways, it is important that your central site solution have a modular design that can accommodate many types of WAN connections from remote locations.

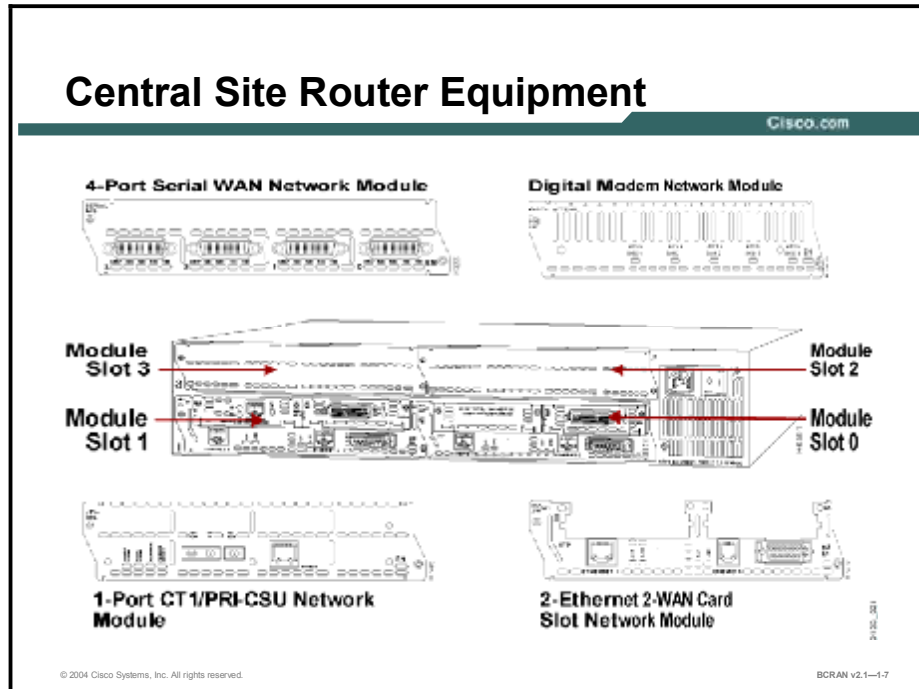
The architecture of a WAN that is used to connect company campuses must optimize bandwidth, minimize costs, and maximize the effective service to end users. Considerations to keep in mind for a central site WAN include:

- **Multiple access connections:** Users will connect to the central site using various media. Central site WANs must allow for multiple media options and simultaneous access by multiple users.
- **Cost:** Keep costs low while maintaining a satisfactory level of service. For example, some WAN charges are based on usage, such as ISDN. Features such as DDR and compression ensure that WAN costs are kept to a minimum. As another example, leased lines are generally charged at a fixed rate, so you may want to consider this service only if the line will sustain high use. Broadband connections such as cable and DSL offer a low-cost, high-speed solution.
- **Access control:** Company information must be restricted, allowing users access only to the areas in the network for which they are authorized. Access lists can prevent unauthorized data flow between offices. For PPP network links, PAP or the superior CHAP can identify the remote entity to prevent unauthorized network connection. SOHO and branch office users can gain access to secure sites through the use of VPN technologies.
- **QoS:** It is important to set priorities for traffic over the link and manage traffic flow so that bursty traffic does not slow mission-critical traffic.

- **Redundancy and backup:** Because a link may fail or usage may be high at certain peak times during the day, the connection to the central office should be backed up. Avoid backing up links using the same service provider.
- **Scalability:** The network must be able to grow with the company.

Central Site Router Equipment

This topic introduces Cisco central site router equipment.



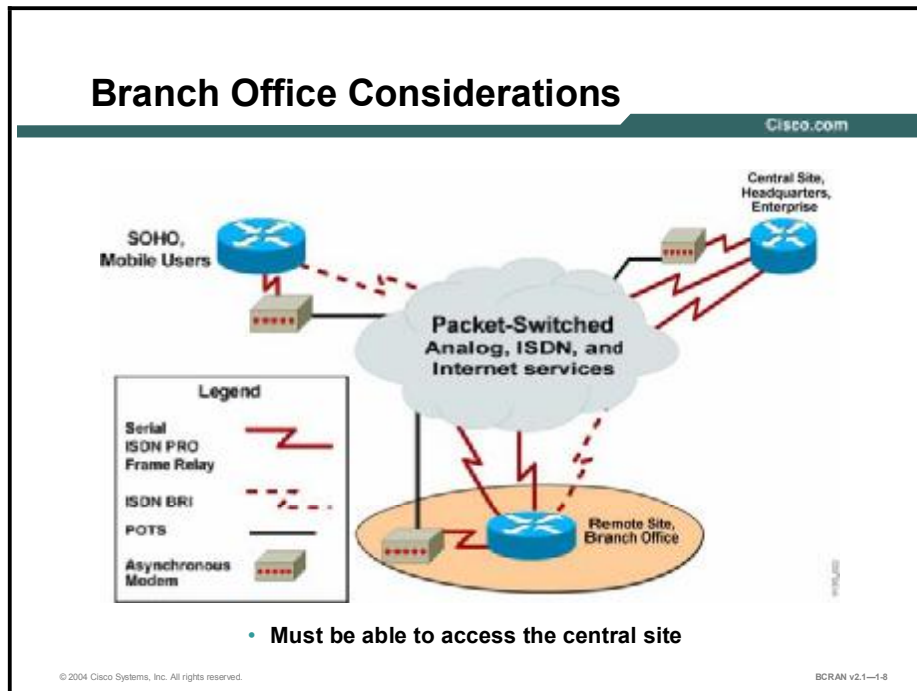
Choose the router that supports the WAN protocols that you will use. As illustrated in the figure, the router and network modules will support the interfaces in the network topology that are used in this course.

These routers are typical Cisco Systems equipment for a central site:

- Cisco 2600 Series
- Cisco 3600 Series
- Cisco 3700 Series
- Cisco 7200/7500 Series

Branch Office Considerations

This topic describes branch office considerations.



A remote site or branch office typically has fewer users than the central site, and therefore needs a smaller WAN connection.

Remote sites connect to the central site and to some other remote sites. Telecommuters may also require access to the remote site. A remote site can use the same or different media.

Remote site traffic can vary, but is typically sporadic. The network designer must determine whether it is more cost-effective to offer a permanent or dialup solution.

The remote site must have a variety of equipment, but does not require as much as the central site. Typical WAN technologies connecting a remote site to the central site include:

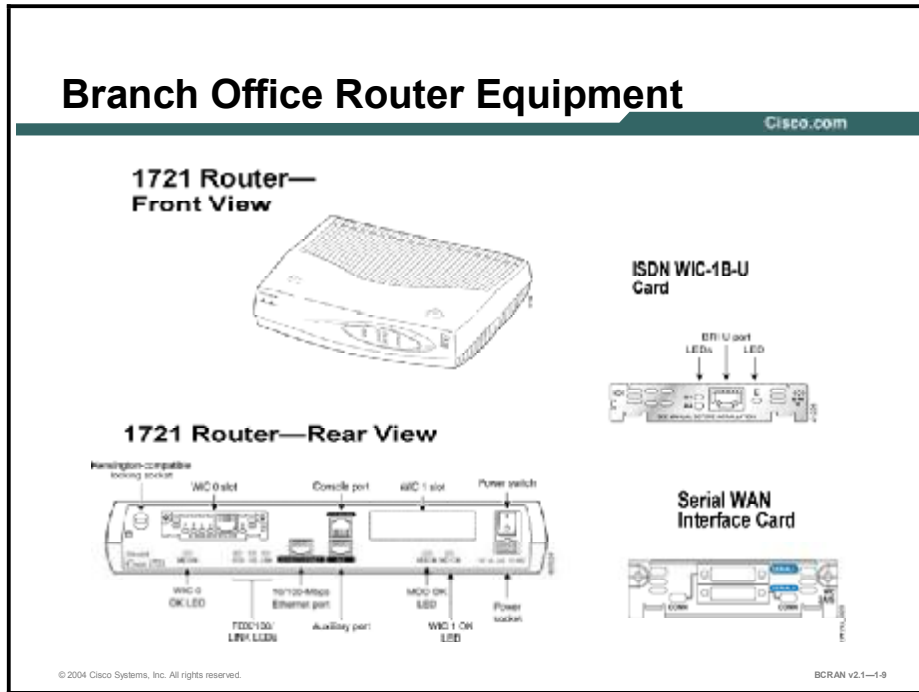
- Leased line
- Frame Relay
- ISDN
- Broadband services (cable or DSL)

Typical considerations for setting up a remote site WAN connection are:

- **Multiple access connections:** Users will connect to the branch site using various media. Branch site WANs must allow for multiple media options and simultaneous access by multiple users. It must also have the connectivity to the Central or SOHO site.
- **Cost:** Sometimes called path cost, cost is an arbitrary value that is typically based on hop count, media bandwidth, or other measures. Cost is assigned by a network administrator to compare various paths through an internetwork environment. Cost values are used by routing protocols to determine the most favorable path to a particular destination; the lower the cost, the better the path.
- **Access control:** To prevent unauthorized traffic, routers and firewalls use a set of rules that permit or deny certain traffic. Access control is commonly applied to router interfaces and can be configured to control which data sessions can pass and which can fail. Users can gain secure access by using VPN solutions to connect to corporate intranets.
- **Redundancy:** In internetworking, duplicate devices, services, or connections can perform the work of original devices, services, or connections in the event of a failure.
- **Authentication:** The remote site must be able to authenticate itself to the central site.
- **Availability:** Service providers may not offer certain WAN services in some regions. This consideration generally becomes more critical as sites are set up in more remote locations.

Branch Office Router Equipment

This topic introduces Cisco branch office router equipment.



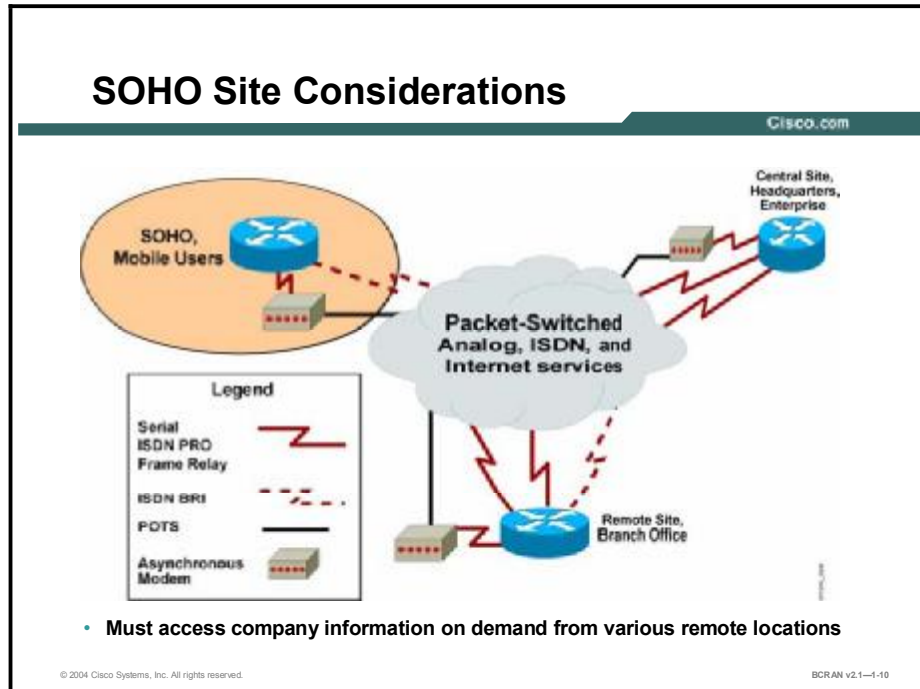
Choose a router that supports the WAN protocols and interfaces that you will use. The Cisco 1700 Series router and the WAN interface cards shown in the figure will support the interfaces that are required for a branch office in the network topology used in this course.

The following routers are typical Cisco equipment for a branch office:

- Cisco 1600 Series
- Cisco 1700 Series
- Cisco 2500 Series
- Cisco 2600 Series

SOHO Site Considerations

This topic describes telecommuter site considerations.



Improvements in WAN technologies allow many employees to do their jobs almost anywhere. The growth in the number of SOHO and small company sites has exploded. As with central and remote sites, WANs for SOHO sites must balance cost and bandwidth requirements.

An asynchronous dialup solution using the existing telephony network and an analog modem is often the solution for SOHOs because it is easy to set up and the telephone facilities are already installed. As usage and bandwidth requirements increase, other remote access technologies should be considered.

The needs of mobile users make an asynchronous dialup connection a good remote solution. Employees on the road can use their PCs with modems and the existing telephone network to connect to the company.

The typical WAN connections employed at SOHO sites are:

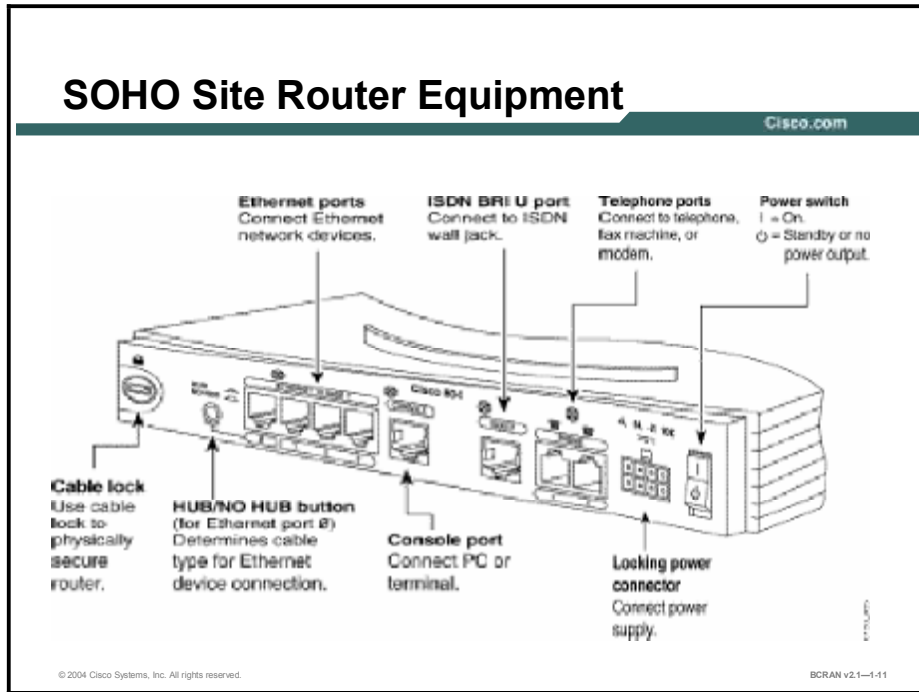
- Asynchronous dialup
- ISDN BRI
- Broadband
- Frame Relay

The typical considerations for a remote site WAN connection are:

- Cost
- Authentication
- Availability

SOHO Site Router Equipment

This topic describes Cisco SOHO site router equipment.



Choose the router that supports the WAN protocols and interfaces that you will use. As illustrated in the figure, the Cisco 800 Series router is an example of a SOHO site router that will support the interfaces required in the network topology that is used in this course.

The following routers are typical Cisco Systems equipment for a SOHO site:

- Cisco 800 Series
- Cisco 1700 Series

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Selecting a WAN connection involves considering such things as availability, bandwidth, cost, and management ease.**
- **Each WAN connection has advantages and disadvantages.**
- **The central site should be designed to accommodate many different types of WAN connections from remote locations.**
- **The type of equipment used will depend upon the needs of a particular site.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—1-12

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What percentage of the information services budget do WAN costs typically constitute?
- A) 10 percent
 - B) 25 percent
 - C) 50 percent
 - D) 80 percent
- Q2) Which of the following is an advantage of using an asynchronous dialup connection?
- A) its high speed
 - B) the ability to connect to the WAN from any active telephone line
 - C) its always-*on* state
 - D) the ability to use the telephone connection for voice calls at the same time
- Q3) Which of the following sites will most users connect to for data and information?
- A) branch site
 - B) SOHO site
 - C) central site
- Q4) Which of the following technologies would be used by SOHO and branch office users to gain access to a very secure central site?
- A) VPN technologies
 - B) standard password authentication protection technologies
 - C) unsecured high-speed broadband connection technologies
 - D) slower-speed asynchronous dialup technologies
- Q5) Which of the following is most typically used to permit or deny traffic on a network?
- A) access control lists
 - B) password authentication
 - C) accounting software
 - D) record management software
- Q6) Which Cisco Systems router would be typical for a central site?
- A) Cisco 1700 Series
 - B) Cisco 1600 Series
 - C) Cisco 2600 Series

- Q7) Which of these technologies can be used at a remote site to connect to the central site?
- A) leased line
 - B) Frame Relay
 - C) ISDN
 - D) broadband services (cable or DSL)
 - E) all of the above
- Q8) Which Cisco routers are typically used for a branch office?
- A) Cisco 7000 Series
 - B) Cisco 4000 Series
 - C) Cisco 3600 Series
 - D) Cisco 2600 Series
- Q9) Which is the most typical WAN connection type for a SOHO user who will require connectivity from a different site to a central site every day?
- A) dedicated serial connection
 - B) circuit-switched connection
 - C) broadband connection
 - D) asynchronous dialup connection
- Q10) Which Cisco routers are typical for a SOHO site?
- A) Cisco 7000 Series
 - B) Cisco 4000 Series
 - C) Cisco 2600 Series
 - D) Cisco 800 Series

Quiz Answer Key

- Q1) D
Relates to: WAN Connection Types
- Q2) B
Relates to: WAN Connection Speed Comparison
- Q3) C
Relates to: WAN Connection Summary
- Q4) A
Relates to: Site Requirements
- Q5) A
Relates to: Central Site Considerations
- Q6) C
Relates to: Central Site Router Equipment
- Q7) E
Relates to: Branch Office Considerations
- Q8) D
Relates to: Branch Office Router Equipment
- Q9) D
Relates to: SOHO Site Considerations
- Q10) D
Relates to: SOHO Site Router Equipment

Selecting Cisco Products for Remote Connections

Overview

Cisco offers many different routing platforms, interface modules, and cables to provide remote access. This lesson introduces the Cisco WAN solutions that are used to connect various company sites.

Relevance

Selecting appropriate equipment is critical to creating an internetwork.

Objectives

Upon completing this lesson, you will be able to

- Select appropriate equipment
- Select appropriate fixed and modular interfaces
- Select appropriate cables to build an internetwork
- Interpret the meaning of various LED indicators on a Cisco router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

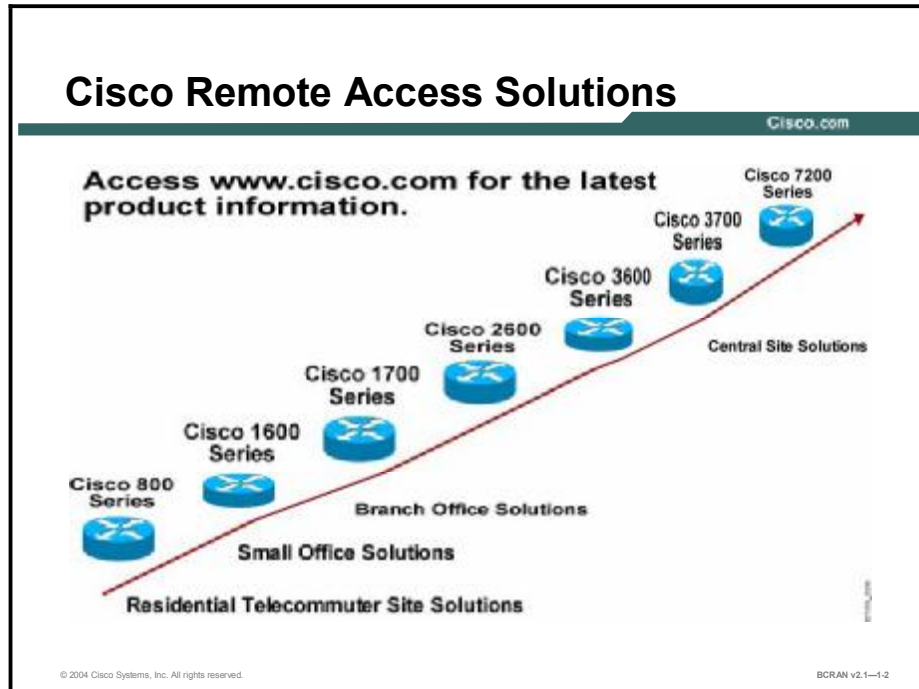
Outline

This lesson includes these topics:

- Overview
- Cisco Remote Access Solutions
- Interfaces: Fixed Interface
- Interfaces: Modular Interface
- Network Cabling and Assembly
- Verification of Network Installation
- Verification of Branch Office Installation
- Verification of SOHO Installation
- Products with Cisco Product Selection Tools
- Summary
- Quiz

Cisco Remote Access Solutions

This topic describes Cisco devices and their possible use.



Cisco Systems offers access servers, routers, and other equipment that allows connection to the WAN service. The figure highlights some of the products that are best suited for various company sites.

The Cisco 800 Series routers are the lowest-priced Cisco routers, using a nonmodular fixed configuration, but based on Cisco IOS software. The Cisco 800 Series access routers provide big-business networking benefits to small offices and corporate telecommuters. The Cisco 800 Series offers secure, manageable, high-performance solutions for Internet and corporate LAN access.

The Cisco 1600 Series routers have a slot that accepts a WAN interface card (WIC). These cards are shared with the Cisco 1700, 2600, and 3600 Series routers and will be shared in future modular branch office products.

The Cisco 1700 Series access routers deliver optimized security, integration, and flexibility in a desktop form factor for small and medium-size businesses and small branch offices that want to deploy Internet/intranet access or VPNs. The Cisco 1721 access router features two modular WAN slots that support WICs (as is common in other 1600, 2600, and 3600 Series access routers) and an autosensing 10/100-Mbps Fast Ethernet LAN port to provide investment protection and flexibility for growth.

The Cisco 2600 Series routers feature single or dual fixed LAN interfaces. A network module slot and two WIC slots are available for WAN connections.

The Cisco 3700 Series multiservice access routers also offer an integrated solution for dialup and permanent connectivity over asynchronous, synchronous, and ISDN lines. Up to four network module slots are available for LAN and WAN requirements.

The Cisco 7200 Series routers are also very high-performance, modular, central-site routers that support a variety of LAN and WAN technologies. The Cisco 7200 Series is targeted at large regional offices that require high-density solutions.

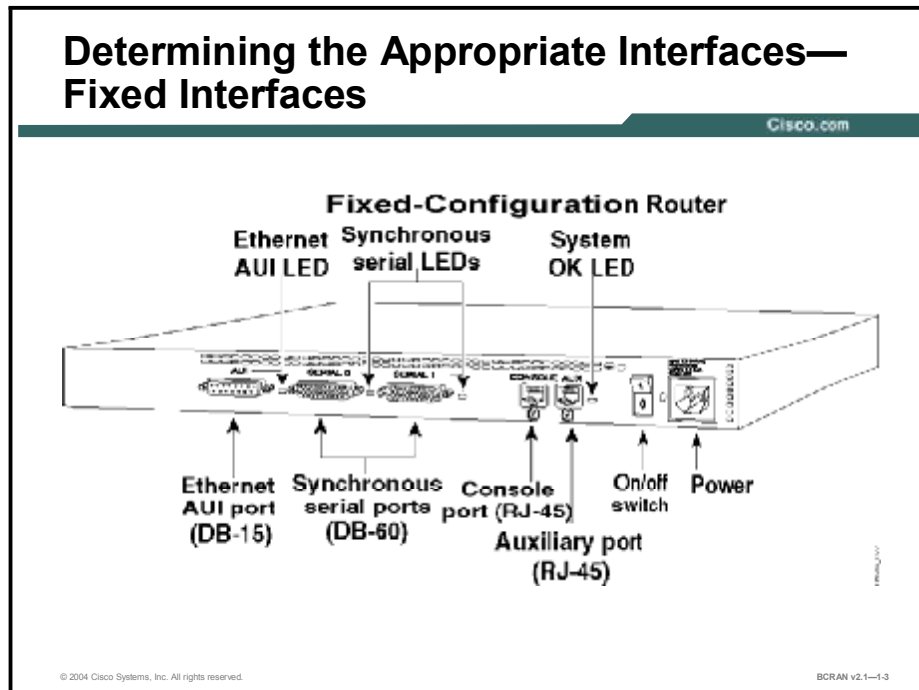
The table highlights some of the features and WAN options for each series of routers.

Cisco Routers	Features
800 Series	ISDN BRI, serial connections, basic telephone service ports, broadband port, entry-level Cisco IOS software
1600 Series	ISDN BRI, one WIC slot
1700 Series	Two WIC slots
2600 Series	Various fixed LAN interface configurations, one network module slot, two WIC slots
3700 Series	Two slots (the 3725) or four slots (the 3745)
AS5000 Series	Access server with multiple T1/E1 ISDN PRI and modem capabilities
7200 Series	Supports a wide range of WAN services, with the high port density necessary for a scalable enterprise WAN

Note A “power branch” is a branch office that offers enhanced capabilities, such as those included in the Cisco 3700 Series routers. Because of their expandability, the Cisco 3700 Series routers are common today in branch offices. Refer to Cisco.com for the most up-to-date information on Cisco equipment.

Interfaces: Fixed Interface

This topic describes various fixed WAN connection types. When selecting interfaces to support a WAN, you can choose between fixed interfaces and modular interfaces.



The router that you select for your WAN connection must offer the interfaces that will support your WAN connection.

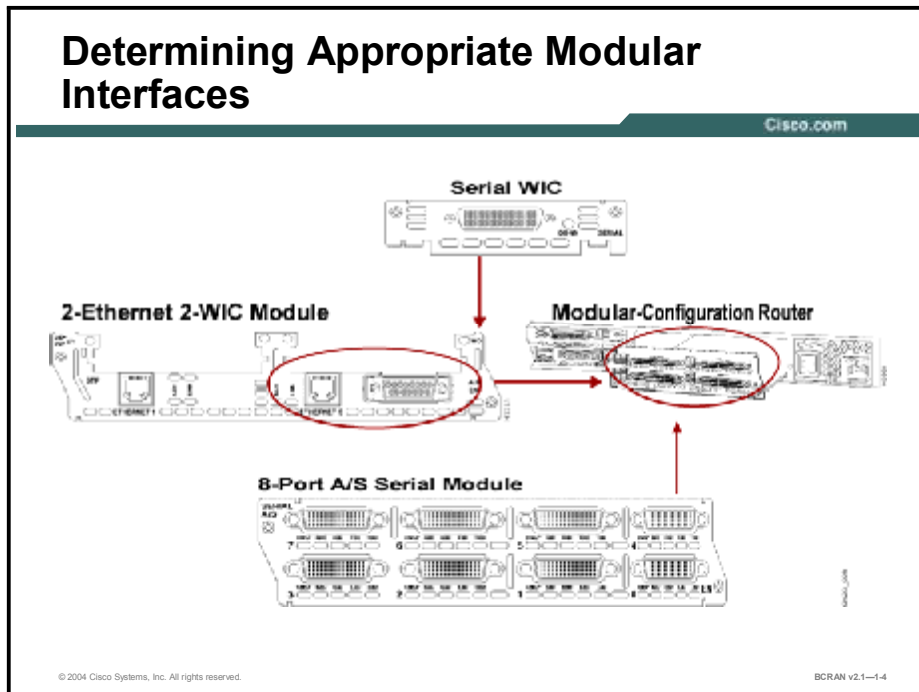
Typical interfaces that are found on a Cisco router (along with the typical WAN connections) support the following:

- **Asynchronous serial:** Used with a modem, supports asynchronous dialup connections
- **Synchronous serial:** Supports connections such as leased lines and Frame Relay
- **Ethernet:** Supports Broadband connections
- **BRI:** Supports ISDN BRI connections
- **Channelized T1 or E1:** Supports connections such as leased lines, dialup, ISDN PRI, and Frame Relay

Fixed-configuration routers are available with predetermined fixed LAN and WAN interface options. Fixed-configuration routers do not require additional WICs or network modules. However, after they are purchased, the interfaces available are limited to only those that were factory installed.

Interfaces: Modular Interface

This topic describes various modular WAN connection types. When selecting interfaces to support a WAN, you can choose between fixed interfaces and modular interfaces.

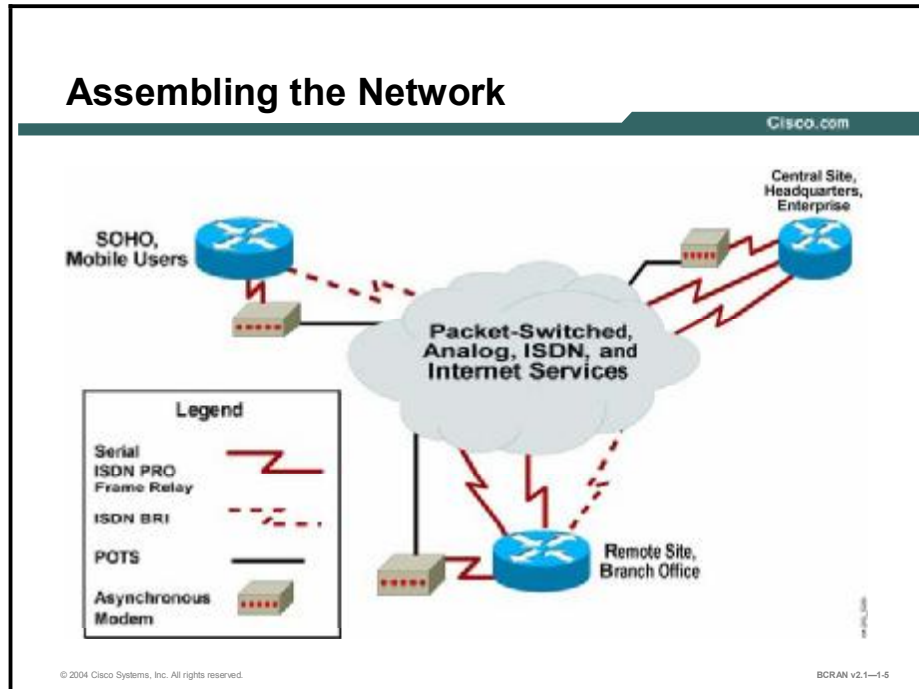


If you select a fixed-configuration router, you receive the router with the interfaces already installed on the box. However, you cannot add or change interfaces on a fixed-configuration router.

Modular routers and access servers such as the Cisco 3600 Series are built with one or more slots that allow you to customize the box. You can determine the types of interfaces on the router by selecting various feature cards, network modules, or WICs to install. Although modular routers require adding equipment to the physical router, they are more scalable as your network grows and your needs change.

Network Cabling and Assembly

This topic describes the cables that are used to connect the network components.



The figure illustrates the cable connections that are available for various WAN types. These include:

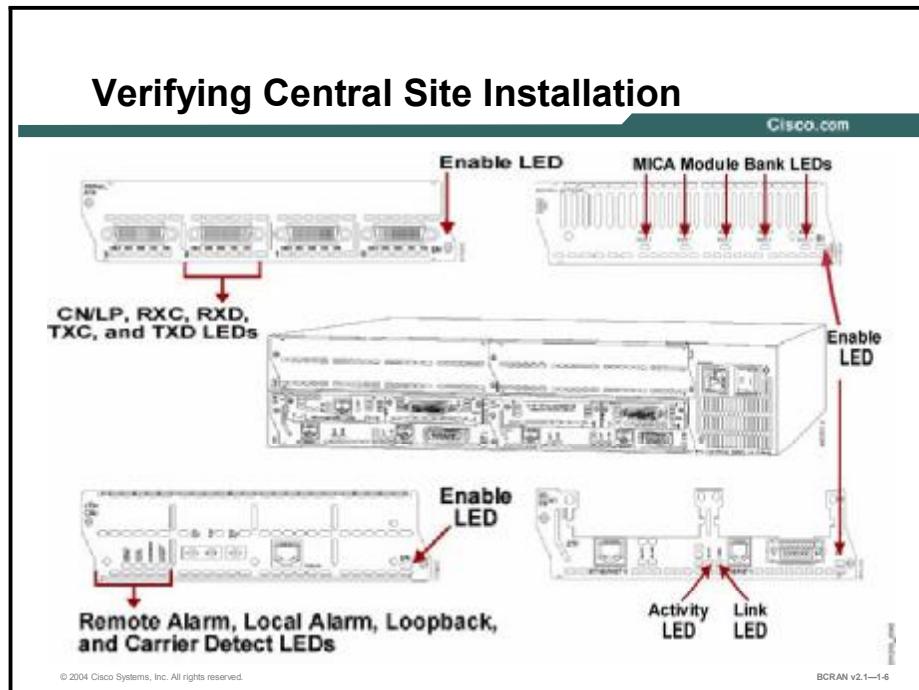
1. **Asynchronous connections:** Asynchronous connections require RJ-11 cables attached from the modem line port to the telephone company jack. If you are using an external modem attached to a Cisco router, you must also use a Cisco EIA/TIA-232 cable to attach the modem to the serial interface of the router. The DB-60 end of the cable connects to the router. The DB-25 end attaches to the modem.
2. **ISDN BRI:** ISDN BRI connection interfaces require RJ-45 cables to connect the BRI interface to the ISDN network. The BRI modules and BRI WICs are available with either an S or T interface that requires an external NT-1 or a U interface with a built-in NT-1.
3. **ISDN PRI (North America):** Channelized T1 (CT1)/PRI modules are available with or without a built-in CSU. If you use an external CSU, attach a female DB-15 cable to the interface of the router. The other end of the straight-through cable will attach to the CSU, which in turn attaches to the ISDN network. Routers with internal CSU modules attach directly to the ISDN network with a standard RJ-48 connector.
4. **ISDN PRI (Europe):** Channelized E1 (CE1)/PRI modules are available with balanced and unbalanced interfaces. CE1/PRI-balanced modules provide a 120-ohm E1 interface for network connections. The unbalanced modules provide a 75-ohm E1 interface for network connections. Four serial cables are available from Cisco for the CE1/PRI module. All four cables have DB-15 connectors on the router end and DNC, DB-15, twinaxial, or RJ-45 connectors on the network end.

5. **Frame Relay:** If you establish a Frame Relay serial connection, Cisco routers support the following signaling standards: EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA-530. Cisco supplies a DB-60 shielded serial transition cable with the appropriate connector for the standard that you specify. The router end of the shielded serial transition cable has a DB-60 connector, which connects to the DB-60 port on the serial interface of the router. The other end of the serial transition cable varies according to the standard that you specify.
6. **Broadband:** Broadband connections will generally require an Ethernet interface port and service provider equipment. Data service is generally provided through equipment from the provider and converted to RJ-45 by the customer.

Note You can use the RJ-48 and DB-15 cables for Frame Relay connections. They can be plugged into a T1 carrier interface. After a channel group is configured, Frame Relay encapsulation can be run over the connection.

Verification of Network Installation

This topic demonstrates how to use the LEDs on your Cisco equipment to verify proper installation.



Each central site router has LED displays that allow you to verify that the router components are installed and functioning properly.

Note For LED information specific to your router, refer to the installation and configuration guide that accompanied your router.

On the Cisco 3600 Series router, the LEDs on the front of the router enable you to determine router performance and operation. The READY LED indicates that a functional module has been installed in the indicated slot. If the LED is *off*, the slot is empty or the module is not functional. The ACTIVE LED blinks to indicate network activity on the module that is installed in the indicated slot.

All network modules have an ENABLE (EN) LED. The ENABLE LED indicates that the module has passed its self-tests and is available to the router.

Each Ethernet port has two LEDs. The ACTIVITY (ACT) LED indicates that the router is sending or receiving Ethernet transmissions. The LINK LED indicates that the Ethernet port is receiving the link integrity signal from the hub (10BASE-T only).

Each PRI network module has four LEDs in addition to the enable LED. These LEDs are:

- **REMOTE ALARM:** Designates a remote alarm condition
- **LOCAL ALARM:** Designates a local alarm condition
- **LOOPBACK:** Designates a loopback condition
- **CARRIER DETECT:** Specifies that you received the carrier on the telephone company link

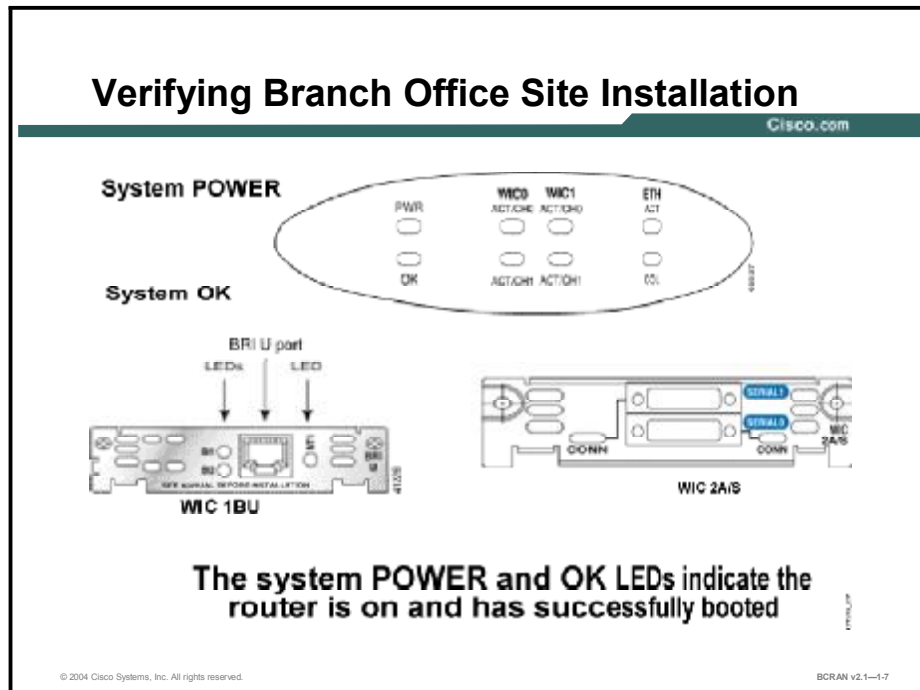
Digital modem modules have five LEDs in addition to the ENABLE LED, one for each Modem ISDN channel aggregation (MICA) technologies module bank. The LEDs blink during initialization. After the ENABLE LED comes on, the MICA module LEDs indicate that the corresponding MICA module is functioning. If a MICA module fails its diagnostics, or if no MICA module is installed in a position, its LED remains *off*.

Each port on the serial network module has additional LEDs. These LEDs are:

- **CN/LP:** Connect when green, loopback when yellow
- **RXC:** Receive clock
- **RXD:** Receive activity
- **TXC:** Transmit clock
- **TXD:** Transmit activity

Verification of Branch Office Installation

This topic discusses the meaning of various LEDs on a Cisco router. Indicator LEDs on a router enable you to verify that the components are installed and functioning correctly.



Each branch office and telecommuter router has LED displays that allow you to verify that the router components are installed and functioning properly.

Note For LED information specific to your router, refer to the installation and configuration guide that accompanied your router.

On Cisco 1721 routers, you can use the LEDs on the front of the router to determine router performance and operation. The LEDs are as follows:

- **PWR:** The green system POWER LED indicates the router is turned *on* and DC power is being supplied.
- **System OK:** The green system OK LED indicates the router has successfully booted. This LED blinks while in the boot cycle.
- **ETH ACT:** The green LAN ACTIVITY LED indicates that data is being sent to or received from the local Ethernet LAN.
- **ETH COL:** A flashing yellow LAN COLLISION LED indicates frame collisions on the local Ethernet LAN.
- **WIC0 ACT/CH0:** The green WIC CONNECTION LED indicates an active connection on this WIC port.
- **WIC0 ACT/CH1:** The green WIC CONNECTION LED indicates an active connection on this WIC port.

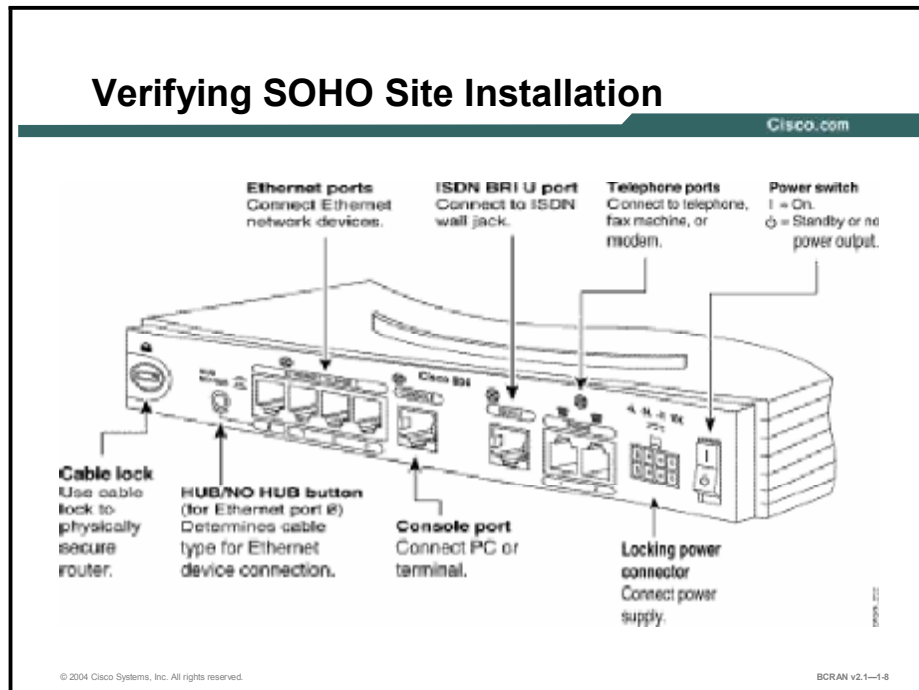
- **WIC1 ACT/CH0:** The green WIC CONNECTION LED indicates an active connection on this WIC port.
- **WIC1 ACT/CH1:** The green WIC CONNECTION LED indicates an active connection on this WIC port.

The serial WIC has several LEDs that indicate data is being sent over the WIC serial ports.

The ISDN BRI U interface card has several LEDs that indicate data is being sent over the WAN ISDN port.

Verification of SOHO Installation

This topic discusses the meaning of various lights on Cisco 800 Series routers. Indicator LEDs on a router enable you to verify that the components are installed and functioning correctly.



Each SOHO router has LED displays that allow you to verify that the router components are installed and functioning properly.

Note For LED information specific to your router, refer to the installation and configuration guide that accompanied your router.

On the Cisco 800 Series routers, you can use the LEDs on the back of the router to determine router performance and operation. The LEDs are shown in the table.

LED Function of 800 Series Router

LED	Color	Function
OK	Green	<i>On</i> when power is supplied to the router and when the router completes the self-test procedure and begins operating.
NT-1	Green	Not applicable for Cisco 801 and 803 routers. <i>On</i> when the internal NT-1 and the ISDN switch are synchronized. Blinks when the internal NT-1 and the ISDN switch are attempting to synchronize.
LINE	Green	<i>On</i> when the ISDN interface and the ISDN terminal device are synchronized.
LAN	Green	<i>On</i> when packets are sent to or received from an Ethernet port.
LAN RXD	Green	Blinks when an Ethernet port receives a packet.
LAN TXD	Green	Blinks when an Ethernet port sends a packet.
LKØ, LK1, LK2, LK3	Green	Cisco 803 and 804 routers only. <i>On</i> when the Ethernet device is connected. <i>Off</i> when the Ethernet device is not connected. Blinks when the connection has a problem.
ETHERNET 1, 2, 3, 4	Green	Cisco 804 IDSL routers only. <i>On</i> when the Ethernet device is connected. <i>Off</i> when the Ethernet device is not connected. Blinks when the connection has a problem.
CH1	Orange	Blinks when placing or receiving a call on the first ISDN B channel. <i>On</i> when a call is connected on the first ISDN B channel. For IDSL routers, see the note following this table.
CH1 RXD	Orange	Blinks when packets are received from the first ISDN B channel.
CH1 TXD	Orange	Blinks when packets are sent from the first ISDN B channel.
CH2	Orange	Blinks when placing or receiving a call on the second ISDN B channel. <i>On</i> when a call is connected on the second ISDN B channel. For IDSL routers, see the note following this table.
CH2 RXD	Orange	Blinks when packets are received from the second ISDN B channel.
CH2 TXD	Orange	Blinks when packets are sent from the second ISDN B channel.
PH1, PH2	Green	Cisco 803 and 804 routers only. <i>On</i> when basic telephone service is in use.
LINK	Green	On back panel of the Cisco 801, 802, and 802 IDSL routers only. <i>On</i> when Ethernet device is connected. Blinks when the connection has a problem.

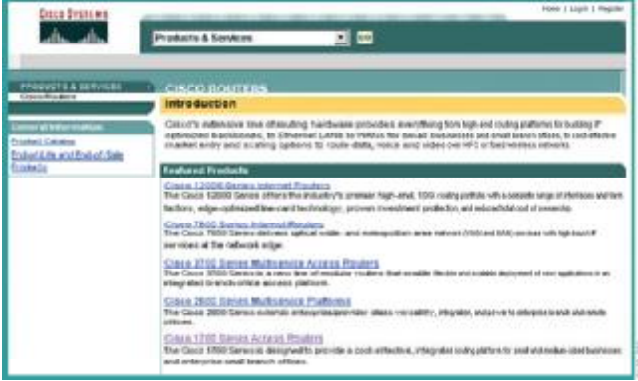
Note On Cisco 802 IDSL and Cisco 804 IDSL routers, either CH1 or CH2 is *on* if the router has an active data connection and the line speed is 64 kbps. CH1 and CH2 are both *on* if the router has an active data connection and the line speed is 128 or 144 kbps.

Products with Cisco Product Selection Tools

This topic discusses the Cisco tools for use in selecting Cisco products.

Selecting Products with Cisco Product Selection Tools

Cisco.com



For up-to-date information, use the online tools at <http://www.cisco.com/en/US/products/hw/routers/index.html>

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1-0

To assist you with product selection, Cisco has extensive documentation and product specifications on its website at <http://www.cisco.com/en/US/products/hw/routers/index.html>.

You will also find product selection and configuration tools on the site. These tools are designed to help you determine the router that best meets your requirements and how to configure it.

Because technology and product offerings change frequently, access this website for the most up-to-date product information.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- The type of Cisco Systems router used will vary depending on where it will be used.
- Select the appropriate fixed and modular interfaces.
- Select the appropriate cables to build an internetwork.
- Each router has LED displays that allow you to verify that the router components are installed and functioning properly.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—1-10

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab 1-1: Using the BCRAN Lab Equipment

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which of these Cisco routers can offer the highest port density?
- A) Cisco 1700 Series
 - B) Cisco 7200 Series
 - C) Cisco 2600 Series
 - D) Cisco 3600 Series
- Q2) Which of these router interfaces support the Frame Relay connection?
- A) synchronous serial
 - B) Ethernet
 - C) BRI
 - D) asynchronous serial
- Q3) What is an advantage of a fixed-configuration router?
- A) You can purchase additional interfaces to expand this router.
 - B) You receive the router with the interfaces you requested.
 - C) You will be able to change the configuration in the future when your needs change.
 - D) Your fixed-configuration router can easily be upgraded in the future.
- Q4) Asynchronous modem connections require which of these cables?
- A) RJ-11 cable
 - B) RJ-45 cable
 - C) DB-15 cable
 - D) fiber-optic cable
- Q5) How many indicator LEDs does each Ethernet port typically have?
- A) 1
 - B) 2
 - C) 3
 - D) 4
- Q6) Which indicator LED on a router typically indicates that the router is turned *on*?
- A) The green system POWER LED
 - B) The green LAN ACTIVITY LED
 - C) The green system OK LED
 - D) A flashing yellow LAN COLLISION LED

- Q7) What does it typically mean when the CH1 RXD indicator LED is orange and blinking?
- A) the connection has a problem
 - B) packets are being received from the first ISDN B channel
 - C) packets are being received from the second ISDN B channel
 - D) packets are being received from the third ISDN B channel

Quiz Answer Key

- Q1) B
Relates to: Cisco Remote Access Solutions
- Q2) A
Relates to: Interfaces: Fixed Interface
- Q3) B
Relates to: Interfaces: Modular Interface
- Q4) A
Relates to: Network Cabling and Assembly
- Q5) B
Relates to: Verification of Network Installation
- Q6) A
Relates to: Verification of Branch Office Installation
- Q7) B
Relates to: Verification of SOHO Installation

Module 2

Supporting Asynchronous Modems

Overview

On completion of this module, you will have configured remote connections via asynchronous modems.

Objectives

Upon completing this module, you will be able to

- Configure an access server for modem connectivity
- Configure a modem manually for basic asynchronous operations via a reverse Telnet
- Configure a router to discover the modem type automatically and configure it
- Configure the router auxiliary port and modem to support remote privileged EXEC access for configuration and remote diagnostics

Outline

The module contains these lessons:

- Connecting and Operating Modems
- Configuring Modems
- Autoconfiguring Modems
- Verifying and Debugging Modem Autoconfiguration

Connecting and Operating Modems

Overview

Modem connections can provide dialup connectivity to a router for out-of-band administration and troubleshooting. This feature allows for a remote connection to a router in the event of primary connection failure. This connection can also be used for dial-out networking and for site-to-site communication. This lesson provides an overview of modem connections and their operation.

Relevance

Using modems is an excellent option for out-of-band management of Cisco Systems routers or dial-in connectivity. You should understand modem operation before you configure these services.

Objectives

Upon completing this lesson, you will be able to:

- Describe the modulation and demodulation process of transmitting and sending data
- Select the appropriate cable for DTE and DCE connections
- List and describe modem modulation standards both proprietary and public
- Troubleshoot speed mismatch in modem communication

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

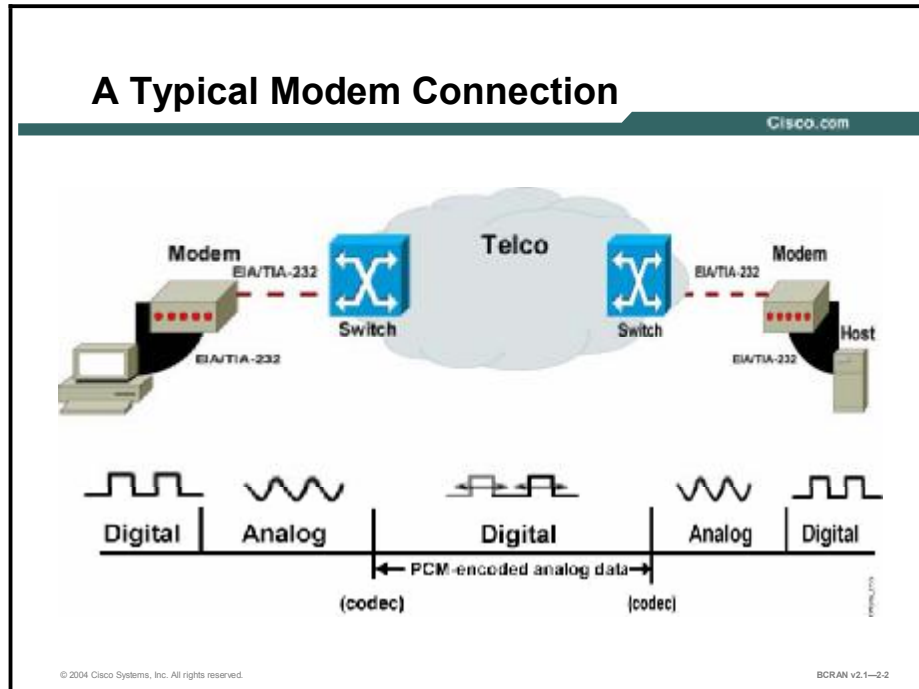
Outline

This lesson includes these topics:

- Overview
- Modem Connections and Operation
- The DTE-DCE Interface
- Modem Signaling—Data
- Modem Signaling—Control
- Modem Control Example
- Modem Operation
- DTE-to-DTE Wiring
- RJ-45 Wiring and Cables
- Working Connections
- Error Control and Data Compression Standards
- Modem Modulation and Standards
- Modem Speed and Compression
- Theoretical Speeds
- Summary
- Quiz

Modem Connections and Operation

This topic describes modulation and demodulation.



A modem converts (modulates) outgoing digital signals from a computer to analog signals for a conventional copper twisted-pair telephone line. When the signal reaches its destination, the destination modem reconverts (demodulates) the incoming analog signal to a digital signal.

The outgoing analog signal generated by the modem is propagated over telephone lines until it reaches a switch at the telco office. A device called a codec converts (codes) the analog signal into a digital format called pulse code modulation (PCM). This signal is then routed over the digital networks of the telco until the signal reaches the destination telco switch, where another codec reconverts (decodes) the digital signal to analog.

The advantage of using analog lines is that no special lines or equipment are required. However, the public switched telephone network (PSTN) local loops are all analog and are prone to line noise and lower data rates.

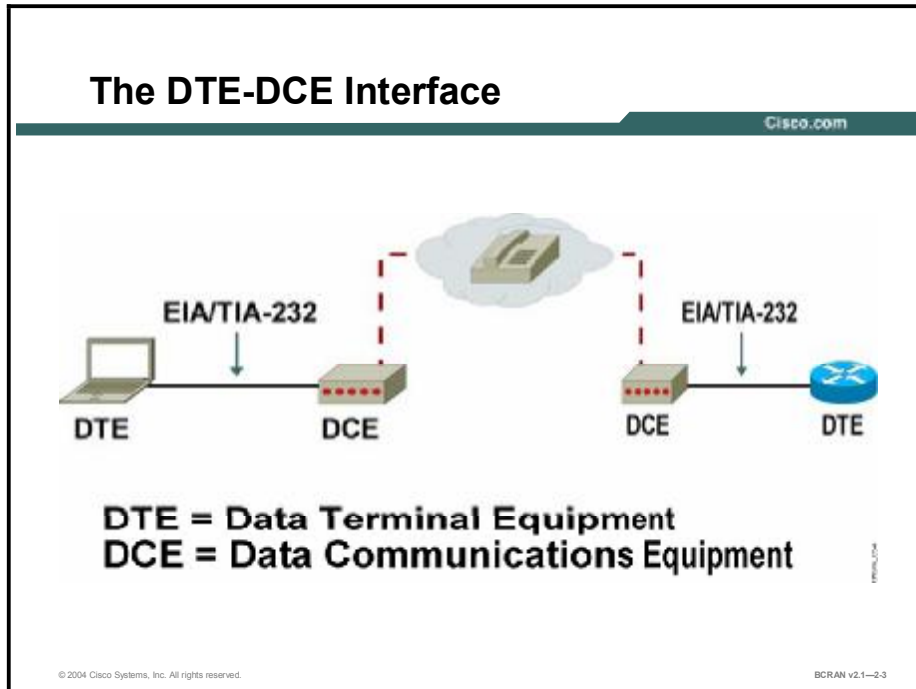
Each analog-to-digital conversion introduces noise into the signal. Amplifying the signal over long distances would also amplify any noise in the signal. Amplifying digital signals simply means recreating the *on* or *off* state of the signal, which drastically reduces line noise. For this reason, telco providers choose to carry data in a digital format. In telecommunications terminology, a digital amplifier is called a regenerative repeater or simply a repeater.

Maximum data rate is usually limited to between 28.8 and 56 kbps. However, the maximum 56 kbps rate is never achieved because of current regulations and analog links.

Note In North America, current regulations limit modem speeds to 53 kbps.

The DTE-DCE Interface

This topic describes DTE and DCE.



End devices, such as PCs, workstations, mainframe computers, and routers, are referred to as data terminal equipment. DTEs communicate with each other through data communications equipment such as modems, CSUs, and DSUs. (The EIA defines DCE as data communications equipment. The International Telecommunication Union-Telecommunication Standardization Sector [ITU-T, formerly known as CCITT] defines DCE as data circuit-terminating equipment.)

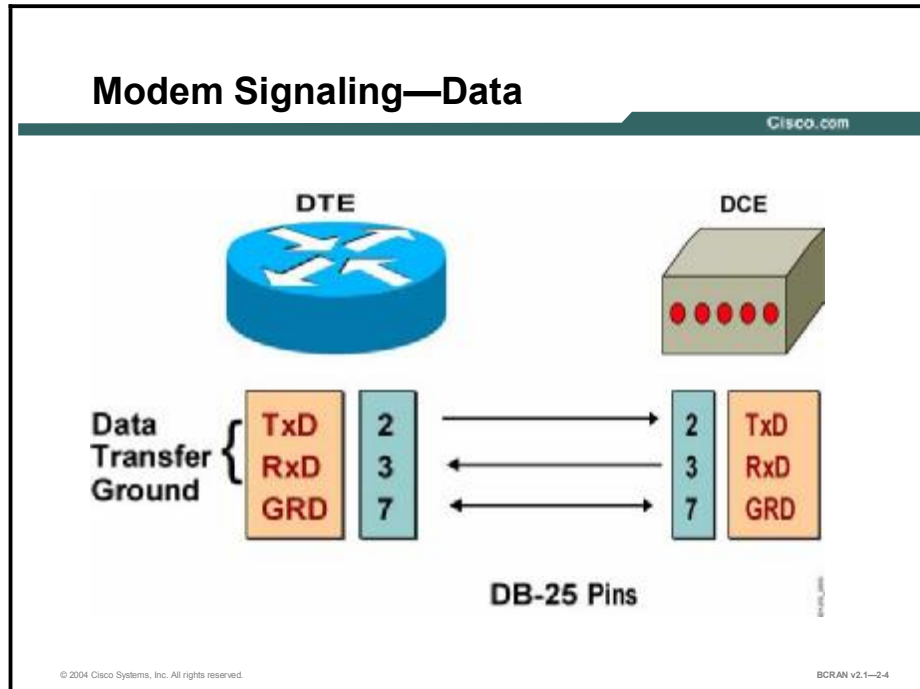
The EIA/TIA-232 standard defines the interface between DTE and DCE.

The end-to-end communication path between two DTEs consists of three segments (refer to the figure shown): DTE-DCE, DCE-DCE, and DCE-DTE. You must administer a set of cabling and configuration elements for each segment.

Note The EIA/TIA-232-C (formerly known as RS-232-C) standard is the most commonly used asynchronous interface for data communications in North America. The RS-232 standard was first issued in 1962, and its third revision, RS-232-C, was issued in August 1969. Although the ubiquitous D-shaped 25-pin connector (DB-25) has become the market standard for EIA/TIA-232-C interfaces, it was not specified in the original RS-232-C standard. Many EIA/TIA-232-C devices use other connectors, such as the DB-9 or RJ-11/RJ-45 modular connectors. X.21 is a European standard that defines the DCE-DTE interface. For more information on these and other standards, refer to Cisco.com or any reliable data communications reference text.

Modem Signaling—Data

This topic describes modem signaling to transmit data.



Although a DB-25 serial connector has 25 pins, only 8 pins are actually used for connecting an access server (DTE) to a modem (DCE). The other 17 signals are not interesting, and are ignored. You can group the eight interesting signals into three categories according to their functionality:

- Data transfer
- Hardware flow control
- Modem control

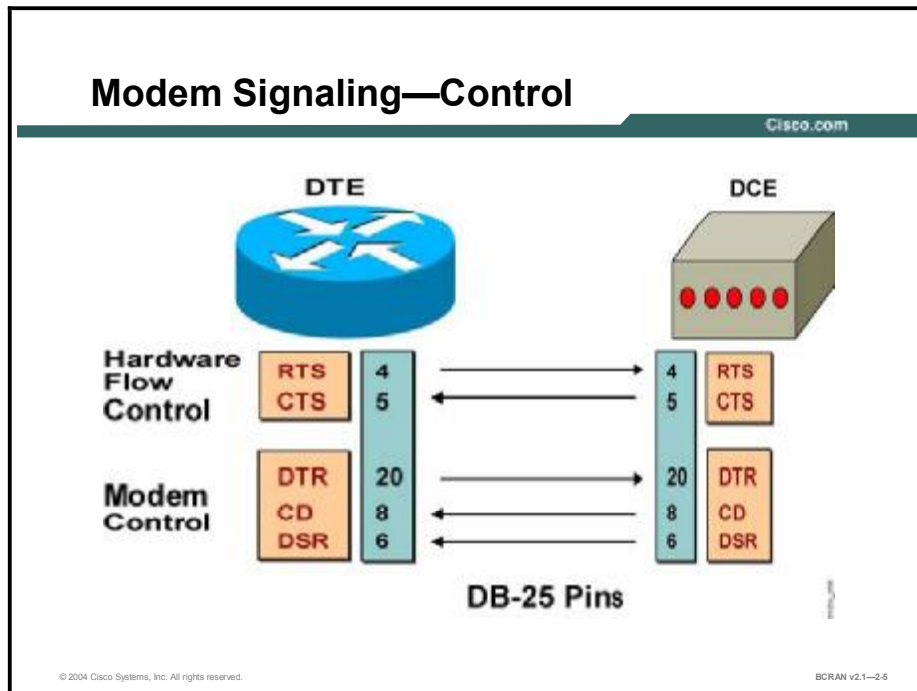
The figure shows the data transfer group:

- **TxD:** Transmit data. The DTE transmits data to the DCE.
- **RxD:** Receive data. The DTE receives data from the DCE.
- **GRD:** Ground (pin 7). This pin provides the ground reference for voltage measurements.

Note The signals and pins shown are for the EIA/TIA -232 specifications.

Modem Signaling—Control

This topic discusses the modem signaling control group.



Modem control consists of several signals between the DTE and DCE that are used to initiate, terminate, and monitor the status of the connection.

The figure shows the remaining two groups of interesting signals between a DTE device and a DCE device:

- Hardware flow control
 - **RTS:** Request To Send. The DTE has buffers that are available to receive from the DCE.
 - **CTS:** Clear To Send. The DCE has buffers that are available to take data from the DTE.
- Modem control
 - **DTR:** Data terminal ready. The DTE indicates to the DCE that it can accept an incoming call.
 - **CD:** Carrier Detect (also referred to as data carrier detect [DCD]). The DCE has established a carrier signal with the remote DCE.
 - **DSR:** Data set ready (pin 6). The DCE is ready for use. This pin is not used on modem connections.

Modem Control Example

This topic describes how to terminate a modem connection.

Terminating a Modem Connection



Cisco.com

DTE-Initiated

- Router drops DTR.
- Modem must be programmed to terminate connection on loss of DTR and restore to saved settings.

DCE-Initiated

- Router detects Carrier Detect (CD) low and terminates connection.
- Modem must be programmed so that CD reflects the state of the carrier.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2-6

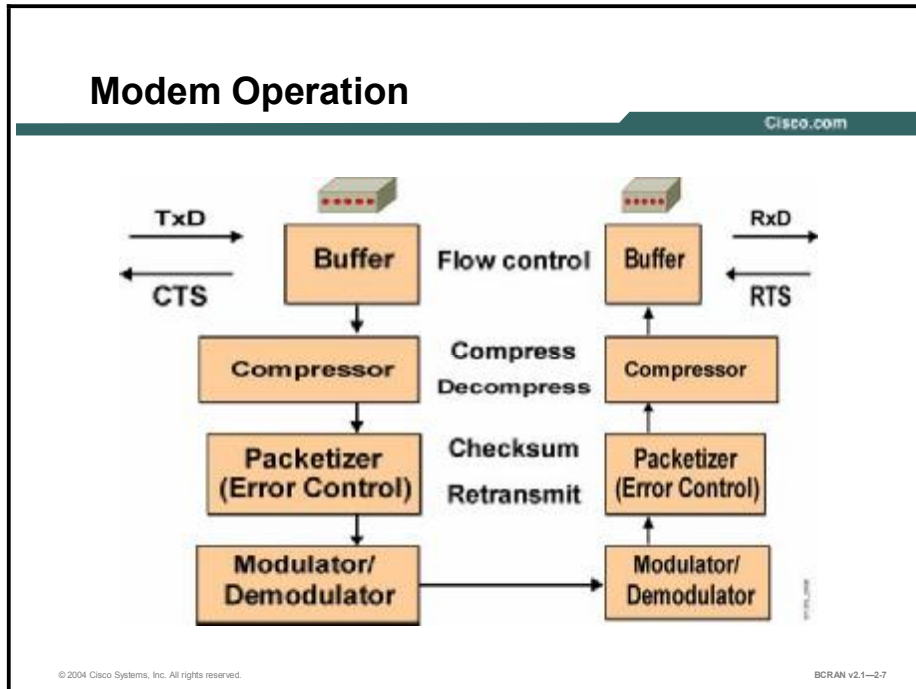
The figure highlights the modem control function for terminating a connection. Either the DTE device or the DCE device may signal for the connection to be terminated. The signals that are used for this function are DTR from the DTE or the modem recognizing the loss of the CD signal.

When modem control is not configured properly, the following symptoms may occur:

- “The modem will not hang up when I quit my session.” DTR is not dropped or recognized.
- “I end up in a session belonging to someone else.” CD is not dropped or recognized.

Modem Operation

This topic describes basic modem operations.



Modems perform their basic operations in one direction:

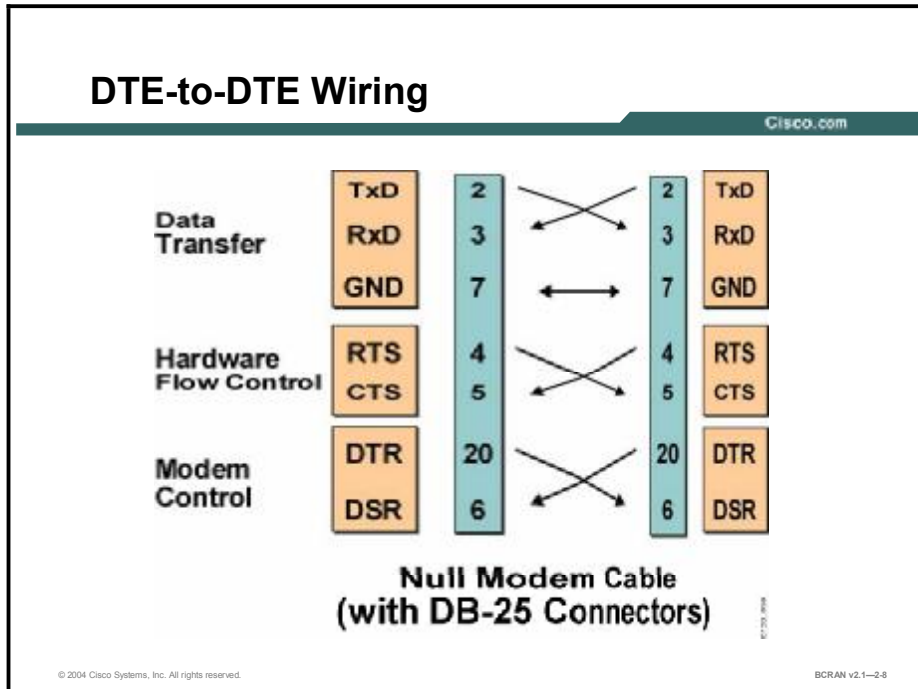
- Outgoing data from an originating DTE comes into the sending modem via the TxD pin.
- If the sending the modem buffer is nearly full, the modem can control flow (via hardware) by lowering the CTS signal, thereby instructing the DTE not to use TxD.
- The data is compressed using a proper algorithm (Microcom Networking Protocol-5 [MNP-5] or V.42bis), which was mutually agreed upon between the two communicating modems when they connected initially.
- The data is then packetized, where windowing, checksum, error control (using MNP-4 or Link Access Procedure for Modems [LAPM]), and retransmission are performed.

Note In this context, the term *packetized* does not refer to an IP packet or Layer 3 protocol data unit (PDU). Packetization and compression are options.

- The digital data is modulated into analog signals and sent out through the telephone network.
- When the data reaches the receiving modem, it goes through the same steps in reverse order. The signal is demodulated, and the data is depacketized, decompressed, and delivered to the destination DTE. The DTE can use RTS to indicate that it is unable to receive data on the RxD pin.

DTE-to-DTE Wiring

This topic describes the pinout of a null modem cable.

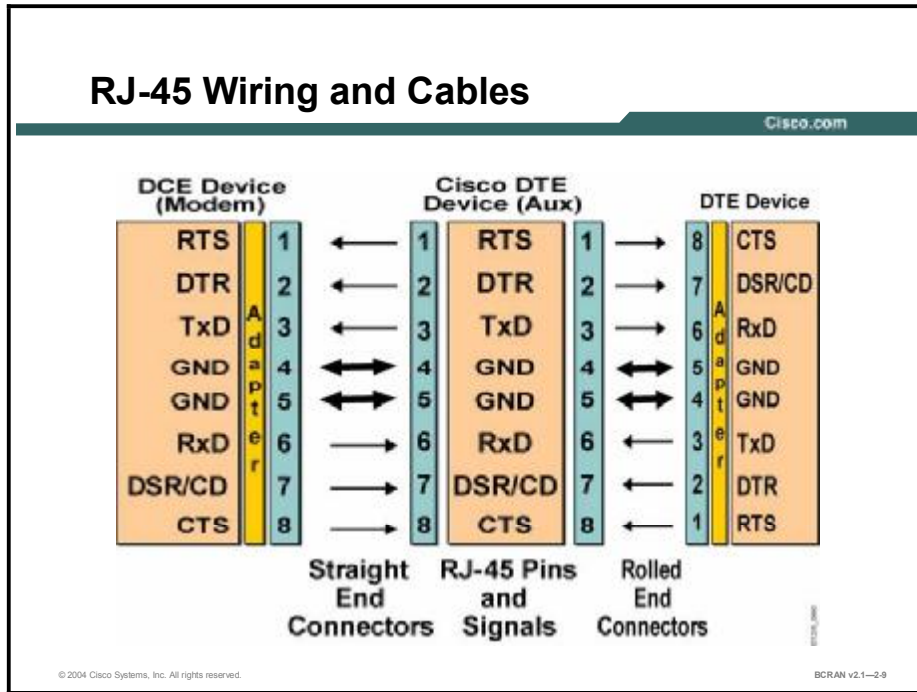


When two DTE devices, such as an access server and a terminal, are near each other, connect them directly without going through a telephone network and two modems. An ordinary EIA/TIA-232 cable will not work in this case, because both DTE devices transmit on the TxD lead (pin 2), and both expect input on the RxD lead (pin 3). A null modem cable is required for the DTE-to-DTE connection.

Null modems crisscross DB-25 pins 2 and 3 and other corresponding pins (as shown in the figure) so that the two DTE devices can communicate. You can configure some devices to operate either as a DTE or a DCE. Configuring a device as a DCE usually means that it receives data on pin 2 and transmits data on pin 3. For example, many serial printers are configured as DCE devices so that you can connect them directly to a DTE (a PC or a terminal server) with an ordinary EIA/TIA-232 cable. This practice eliminates the need for a null modem connection.

RJ-45 Wiring and Cables

This topic describes the Cisco implementation of using RJ-45 ports for various connections.



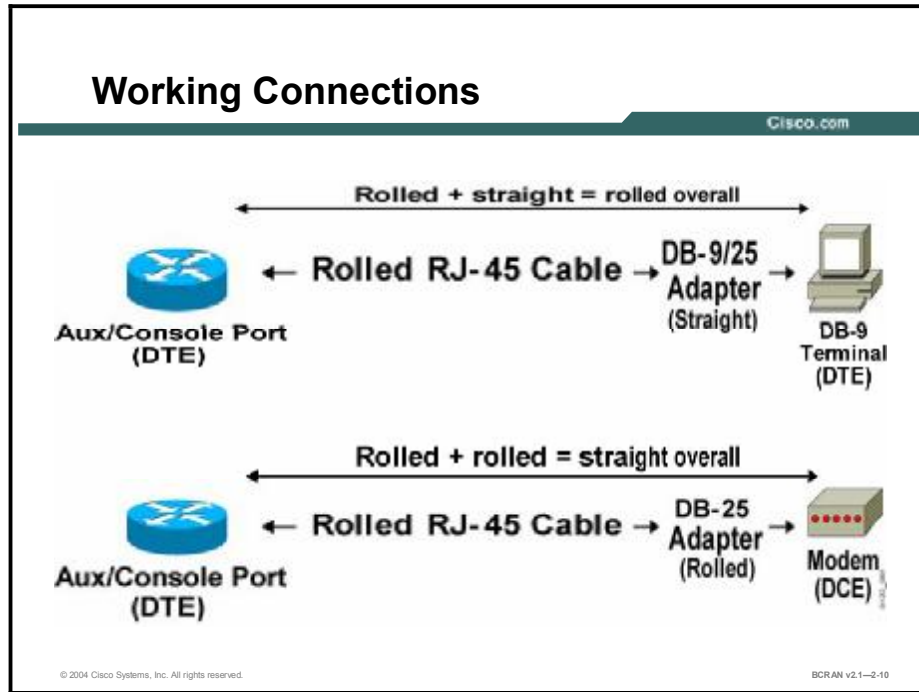
Cisco uses RJ-45 ports and connectors for console, auxiliary, and asynchronous port connections. The specific pinouts to be used on an RJ-45 interface for EIA-232 are not defined by any standards. Cisco defines the RJ-45 pinouts (shown in the figure) as DTE.

Cabling from the access server port (RJ-45) to an external device, such as a modem or terminal, requires the use of two cabling components:

- RJ-45-to-RJ-45 cable: Can be either a rollover cable (reverse pins 1-8, 2-7, 3-6, 4-5) or a straight-through cable (1-1, 2-2, and so forth). To check whether a cable is straight-through or rolled, hold the two connectors (the two ends of the cable) side by side. With the keys at the back and the pins up, compare them by inspecting the color-coded wires inside the connector. If the wires use the same colors on the same pins, it is a straight-through cable. If the wires are a mirror image of each other, it is a rolled cable. The octal cable that is used to connect to the asynchronous ports is the equivalent of a rolled cable.
- RJ-45-to-DB-25 adapter: Also straight-through or rolled.
 - Male DTE (MDTE) or female DTE (FDTE) adapter. Straight-through.
 - Male DCE (MDCE) or female DCE (FDCE) adapter. Rolled.
 - MMOD (male modem-style) adapter. Rolled. This adapter supports only modems that are modified from MDCE connectors by wiring DB-25 pin 8 to DSR, instead of pin 6.

Working Connections

This topic describes how to connect devices to a Cisco router.



This figure displays the working connections between an access server and various types of end devices.

The auxiliary and console ports are configured as DTE devices on Cisco access servers. Terminals are also DTE devices. As noted earlier, two DTE devices cannot be directly connected unless the signals are rolled exactly one time. You must, therefore, roll the pins in either the cable or the DB-25 adapters, but not both. The “formula for success” is as follows:

- DTE + rolled RJ-45 cable + straight DB-25 adapter + DTE = OK
- DTE + straight RJ-45 cable + rolled DB-25 adapter + DTE = OK

When connecting a DTE to a DCE, however, you should have either no rolls or two rolls in the cable and the connector. The “formula for success” is as follows:

- DTE + rolled RJ-45 cable + rolled DB-25 adapter + DCE = OK
- DTE + straight RJ-45 cable + straight DB-25 adapter + DCE = OK

The part number for the rolled RJ-45-to-RJ-45 cable is CAB-500RJ.

When you order access servers with asynchronous ports, you must order the corresponding cable accessories. Order one CAB-OCTAL-KIT (an 8-lead octal cable and eight male DB-25 modem connectors) for each 68-pin asynchronous connector on the access server. If the modem uses an RJ-45 connector, order one CAB-OCTAL-ASYNC (a rolled 8-lead octal cable with RJ-45 connectors). Special adapters might be required.

Note Connecting a modem to the console port of a router is a security risk because it initially has no protection or security features enabled.

Cisco routers typically ship with a console and auxiliary port cabling kit that may include the following components:

- RJ-45-to RJ-45 rollover cable
- RJ-45-to-DB-9 FDTE adapter (labeled TERMINAL)—primarily used to connect to a PC being used as a console terminal
- RJ-45-to-DB-25 FDTE adapter (labeled TERMINAL)—can be used to connect a computer terminal or an older computer to the console or auxiliary port
- RJ-45-to-DB-25 MDCE adapter (labeled MODEM)—used to connect the auxiliary port to a modem.

The table presents the port types for console and auxiliary ports on Cisco routers.

	DB-25	RJ-45
Console port	DCE	DTE*
Auxiliary port	DTE	DTE


*DCE in the Cisco 1700 Series

Error Control and Data Compression Standards

This topic describes error control and data compression.


Error Control and Data Compression Standards

Cisco.com



Error Detection/Correction

- **Microcom Networking Protocol (MNP)**
 - MNP 2–4 in public domain
 - MNP 10 for cellular
- **CCITT V.42**
 - LAPM
 - MNP 4



Data Compression

- **MNP-5:** 2:1 ratio
- **V.42bis:** 4:1 ratio
- **V.44:** 6:1 ratio

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2-11

Error detection and correction methods have been developed to ensure data integrity at any speed. Some widely used methods include MNP and LAPM.

Compression algorithms typically require error-correction algorithms. So compression under V.42*bis* and MNP-5 is usually run over LAPM or MNP-4. V.42 and V.42*bis* are not limited to V.32 and V.34 modems. They can also be implemented in lower-speed equipment. The 4:1 compression ratio provided by V.42*bis* is theoretical and rarely achieved.

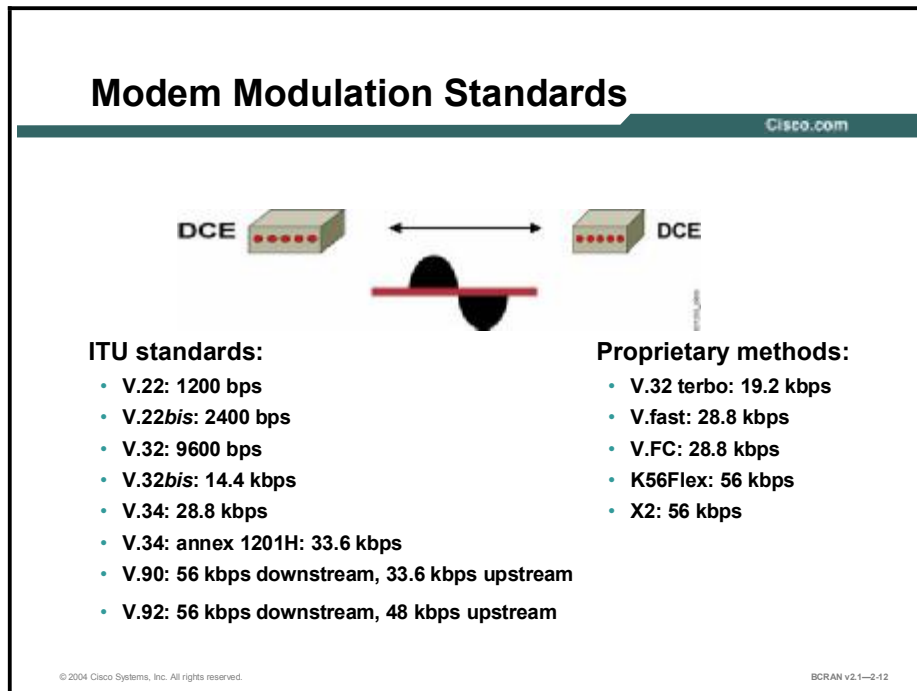
V.44 is the newest compression standard that is designed to be used by V.90. V.44 offers up to a 6:1 compression ratio, compared to the 4:1 maximum compression from V.42*bis*. This 20-to-60 percent increase in throughput is due to a new compression algorithm that is optimized for typical web content.

The modern data compression technique is analogous to the video-compression or disk-packing algorithms that are used in computers. The compression efficiency is highly dependent on data content. Some data (such as ASCII files) compresses readily; other data compresses very little.

Some application software supports data compression. However, it is usually better to let the modem compress transmitted data. Data compression algorithms that operate in modem hardware are faster than those performed by host software. If two modems have agreed on V.42*bis* compression, you must disable the compression capability of the application. This modem-provided compression means transferring data at a higher speed on the interface between the DTE and the DCE.

Modem Modulation Standards

This topic describes modem modulation standards.



The function of a modem is to convert digital signals (DTE to DCE) into analog signals (DCE to DCE), and vice versa. The ITU-T has defined and introduced several modem modulation standards over the years. However, various modem manufacturers have also marketed their own proprietary versions of modems. Interoperability among various types of modems can be a challenge, sometimes even for modems from the same vendor.

Some of the more commonly used standards are:

- The V.32bis standard supports 14.4-kbps transmit (downstream) and receive (upstream) connections. It was finalized in July 1991.
- The V.34 standard supports 28.8-kbps transmit and receive connections. It was finalized in June 1994.
- The V.34 annex 12 standard supports 33.6-kbps transmit and receive operation. If compression is used, up to 133.8 kbps is possible if the DTE-to-DCE connection can support this speed.
- The V.90 standard support connections with 56-kbps transmit and up to 33.6-kbps receive. Most modem manufacturers have a V.90 product, even though the actual maximum data rate allowed by government regulating bodies is usually 53 kbps.
- The V.92 standard support connections with 56-kbps transmit and up to 48-kbps receive. It offers improved features such as Quick Connect, which dramatically improves the speed at which users can connect with an Internet service provider (ISP), and Modem on Hold, which enables users to suspend and reactivate their dialup modem connection to either receive or initiate a telephone call. V.92 and its companion compression standard, V.44, were officially adopted by the ITU in July 2000.

With proper configuration, V.90 modems can intelligently adapt to line conditions during a transition. Two communicating modems will initially attempt to set up a call at 56.6 kbps. If line conditions do not allow a transmission at this speed, the modems fall back to the next-highest speed in steps of 2.4 kbps (possibly down to 2.4 kbps if necessary). Alternatively, if line conditions improve, the modems can increase the speed.

If you are using two V.90 modems between two routers, the maximum speed will be no greater than 33.6 kbps. Modems operating at 33.6 kbps function under the assumption that the connection between the user and the ISP is totally analog. Modems operating at 56 kbps treat the telephone network as a partially digital connection. In fact, the connection between the PSTN and the ISP must be digital to support a data transfer rate greater than 33.6 kbps.

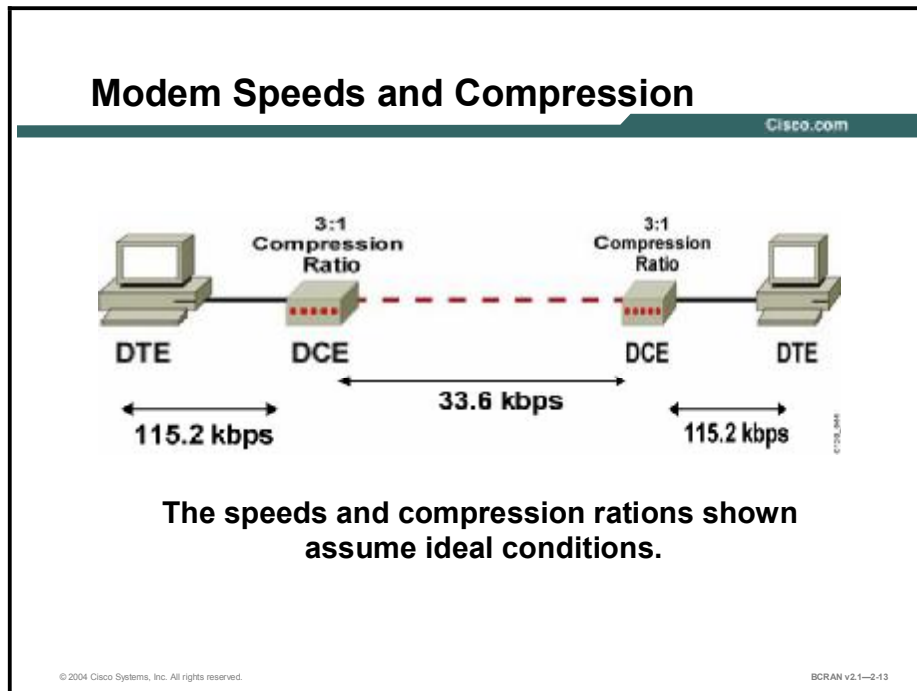
The codec located at the PSTN converts analog signals into digital pulses and vice versa. These digital pulses, or PCM, are transmitted at a rate of 64 kbps. A 56-kbps modem transmits and receives data asymmetrically. The upstream is limited to 33.6 kbps. The downstream is limited to 53333 bps in the United States by the U.S. Federal Communications Commission (FCC). Downstream data flow is the advantage of 56 kbps and PCM. The conversion from digital to analog causes less complication for a PCM modem (a 56-kbps modem) than the conversion from analog to digital. A 56-kbps modem cannot establish a transfer rate greater than 33.6 kbps downstream if more than one conversion exists on the telephone network between the ISP and user.

Older modems negotiate a fixed transmission rate during handshaking, but after that, communications continue at the same speed. If line quality deteriorates below a certain threshold, the connection is lost. Older modems cannot take advantage of any increased bandwidth later, when the line quality improves.

The access server is unaware of modulations because it is directly involved with only DTE-to-DCE communication. However, the access server-to-modem speed must account for modulation speed and compression ratio for optimal end-to-end performance.

Modem Speed and Compression

This topic describes how to calculate true modem speed with compression.



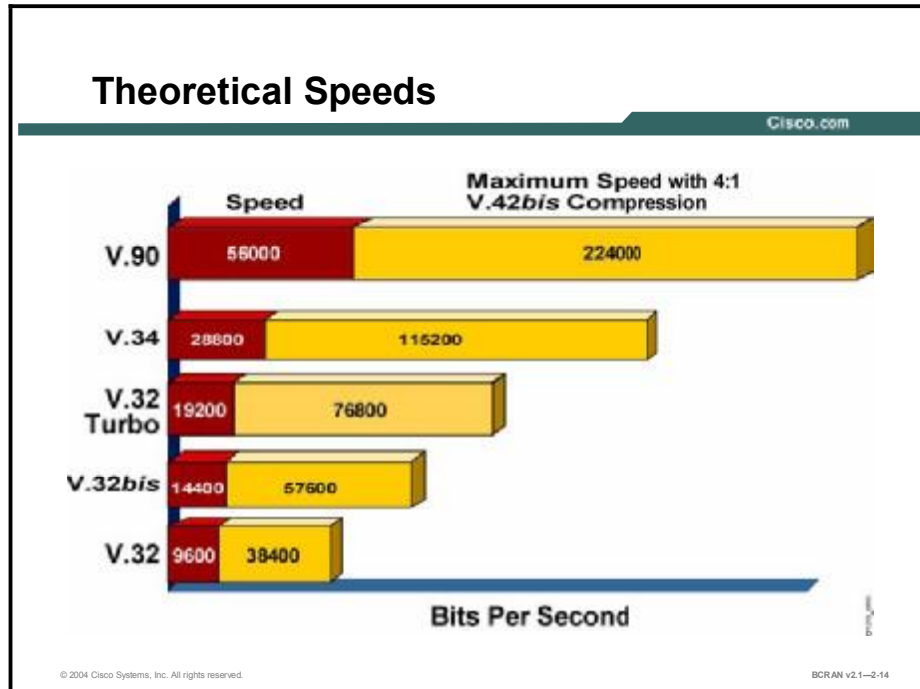
The difference between the DCE-to-DCE modulation speed and DTE-to-DCE speed is often a source of confusion. The former represents how fast the modems communicate with each other across the telephone network. The latter represents how fast your computer communicates with the attached modem.

In an ideal situation, to gain full benefits from compression, the DTE (for example, a PC) must send to the DCE (a modem) at speeds matching the potential compression ratio. However, the EIA/TIA-232 serial interface commonly found on PCs and some Macintosh computers (the COM port) might operate considerably more slowly than the full potential speed of V.34. The problem is that some PCs and Macs use the EIA/TIA-232 serial interface with a combination of Universal Asynchronous Receiver/Transmitters (UARTs) and character-oriented communications software packages, which are not reliable at higher data rates. In a PC, DTE should be set to clock the modem at its fastest rate to take advantage of compression.

An improperly configured modem might automatically adjust DTE-to-DCE speeds to match the established DCE-to-DCE speeds. This state is often called speed mismatch. To avoid speed mismatch, you must lock the DTE-to-DCE speed so that it remains constant, as originally configured. This speed-locking mechanism is called speed conversion (also known as port-rate adjustment or buffered mode).

Theoretical Speeds

This topic describes various theoretical modem speeds.



This figure displays the maximum theoretical speeds possible for selected modem modulation standards. Also displayed are the possible speeds if V.42bis compression is used with the same standards.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Modem connections can provide dialup connectivity to a router for out-of-band administration and troubleshooting.**
- **Modems convert outgoing digital signals to analog, and convert incoming analog signals back to digital.**
- **Cisco uses RJ-45 ports and connectors for console, auxiliary, and asynchronous port connections.**
- **Various modem standards are used, such as V.34 and V.90.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—2-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) The process of converting an analog signal into a digital format is known as ____.
- A) codec
 - B) PCM
 - C) modulation
 - D) amplification
- Q2) Which device is an example of data terminal equipment?
- A) switch
 - B) PC
 - C) TSU
 - D) modem
- Q3) Which pin provides the ground reference for modem communication?
- A) 1
 - B) 2
 - C) 3
 - D) 7
- Q4) Which DTE pin indicates to the DCE that it can accept an incoming call?
- A) 4
 - B) 6
 - C) 8
 - D) 20
- Q5) If you dial into an access server and end up in a session initiated by someone else, what is the most likely cause?
- A) DTR not being dropped
 - B) CD not implemented
 - C) DST not being raised
 - D) ground fault occurring in the circuit

- Q6) If the sending modem buffer is nearly full, the modem can control flow by lowering which signal?
- A) RTS
 - B) CD
 - C) CTS
 - D) Rx
- Q7) Which type of cable is used to connect two DTE devices?
- A) null modem
 - B) rolled
 - C) straight-through
 - D) modem
- Q8) If you are going to connect a PC to a router auxiliary port, which type of cable should you use?
- A) null modem
 - B) straight-through
 - C) modem
 - D) rolled
- Q9) Which type of cable is used to connect a modem to the auxiliary port of a Cisco router?
- A) null modem
 - B) straight-through
 - C) modem
 - D) rolled
- Q10) Which type of file achieves the greatest modem compression?
- A) JPEG
 - B) MP3
 - C) text
 - D) ZIP
- Q11) Which ITU modem standard can successfully negotiate a lower speed if line conditions deteriorate?
- A) V.92
 - B) X2
 - C) 56Flex
 - D) V.94

- Q12) What DTE speed must you set to take advantage of compression?
- A) four times the modem speed
 - B) the modem speed
 - C) half of the modem speed
 - D) the highest possible speed that the DTE will support
- Q13) What is the maximum possible speed with the V.90 standard and V.42*bis* compression?
- A) 224000
 - B) 115200
 - C) 56000
 - D) 38400

Quiz Answer Key

- Q1) C
Relates to: Modem Connections and Operation
- Q2) B
Relates to: The DTE-DCE Interface
- Q3) D
Relates to: Modem Signaling—Data
- Q4) D
Relates to: Modem Signaling—Control
- Q5) B
Relates to: Modem Control Example
- Q6) C
Relates to: Modem Operation
- Q7) A
Relates to: DTE-to-DTE Wiring
- Q8) D
Relates to: Working Connections
- Q9) B
Relates to: RJ-45 Wiring and Cables
- Q10) C
Relates to: Error Control and Data Compression Standards
- Q11) A
Relates to: Modem Modulation and Standards
- Q12) D
Relates to: Modem Speed and Compression
- Q13) C
Relates to: Theoretical Speeds

Configuring Modems

Overview

This lesson contains descriptions of modem configuration methods and commands.

Relevance

Modem configuration is considered to be complex and error prone. If you use modems for dial-in, or out-of-band access, this lesson will show you the basics of how to configure your Cisco device and modem for that purpose.

Objectives

Upon completing this lesson, you will be able to:

- Connect to a modem from a router using reverse Telnet
- Utilize commands to determine line numbering on a Cisco router
- Configure a modem using standard initialization strings
- Configure a modem using nonstandard initialization strings

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

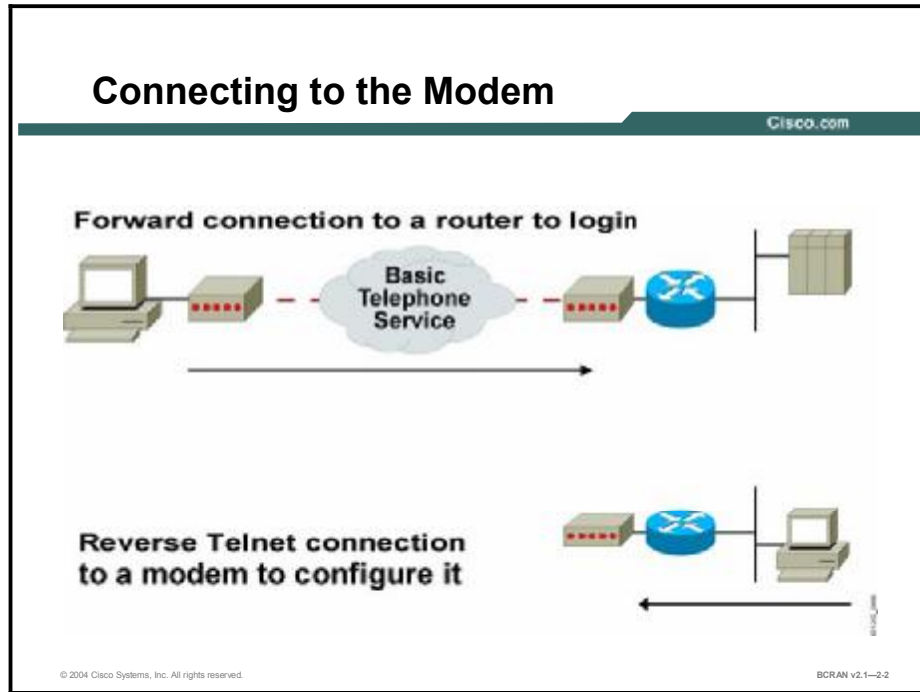
Outline

This lesson includes these topics:

- Overview
- Modem Connections
- EXEC Connection Commands
- Sample Output for the **show line** Command
- Line Types and Numbering
- Interface Asynchronous and Line Configuration
- Basic Modem Configuration
- Standard Modem Commands
- Nonstandard Modem Commands
- Modem Initialization Strings
- Summary
- Quiz

Modem Connections

This topic describes how to connect from a router to a modem.



Cisco routers support both incoming asynchronous line connections (forward connections) and outgoing asynchronous line connections (reverse connections). For example, a remote terminal user dialing into the router through an asynchronous line makes a forward connection. In a reverse connection, a user connects through a router to an attached modem to configure the modem.

A host can make reverse Telnet connections to various types of devices that are attached to a Cisco router. Different port numbers (20xx, 40xx, and 60xx) are used because different data type and protocol negotiations will take place for different types of devices that are attached to the router.

The remote host must specify a particular TCP port on the router to connect with individual lines or to a rotary group. In the lower part of the figure, the remote host makes a reverse Telnet connection to the modem using port address 2007. Note that TCP port number 2007 specifies a Telnet protocol connection (TCP port 2000) to line 7. The individual line number is added to the end of the port number type.

The table displays services provided and TCP port numbers for individual lines and rotary groups.

TCP Port Services

Services Provided	Base TCP Port for Individual Lines	Base TCP Port for Rotary Groups
Telnet protocol	2000	3000
Raw TCP protocol (no Telnet)	4000	5000
Telnet protocol, binary mode	6000	7000
XRemote protocol	9000	10000

Use the **transport input** command to specify which protocol to allow for connections. For example, the **transport input all** command allows all of the following protocols to be used for the connection:

lat | mop | nasi | none | pad | rlogin | telnet | v120

Each of these command options can also be specified individually.

EXEC Connection Commands

This topic illustrates an example of the commands that are needed to make a reverse Telnet connection from a router to a modem.

EXEC Connection Commands

Cisco.com

Router>#telnet [host] [port]

- Makes a connection with the Telnet protocol

Router>disconnect [session-number]

- Disconnects the specified session or all sessions

Router>ctrl-shift-6 x

- Suspends a session

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-3

Use the EXEC commands shown in the figure and the table to initiate and control a reverse Telnet terminal session to a modem.

Telnet-Related Commands

Command	Description
telnet [host] [port] [/debug]	Makes a Telnet connection to a host (and optionally to a certain port). You can specify the target host either by a host name or an IP address. The optional debug switch provides useful information about the connection by displaying the informational level of logging messages. Additionally, you can simply type the name of the host to which you wish to make the connection, and by default, an attempt to establish a Telnet session is started. The interface through which the connection is made provides the source IP address for that connection.
disconnect [session-number]	Disconnects the specified connection or the most recent connection if not specified.
Ctrl-Shift-6 x	To suspend the current session, simultaneously press the Ctrl , Shift , and 6 keys, followed by the x key.

Some additional commands that are useful for controlling and using remote connections include those shown in this table.

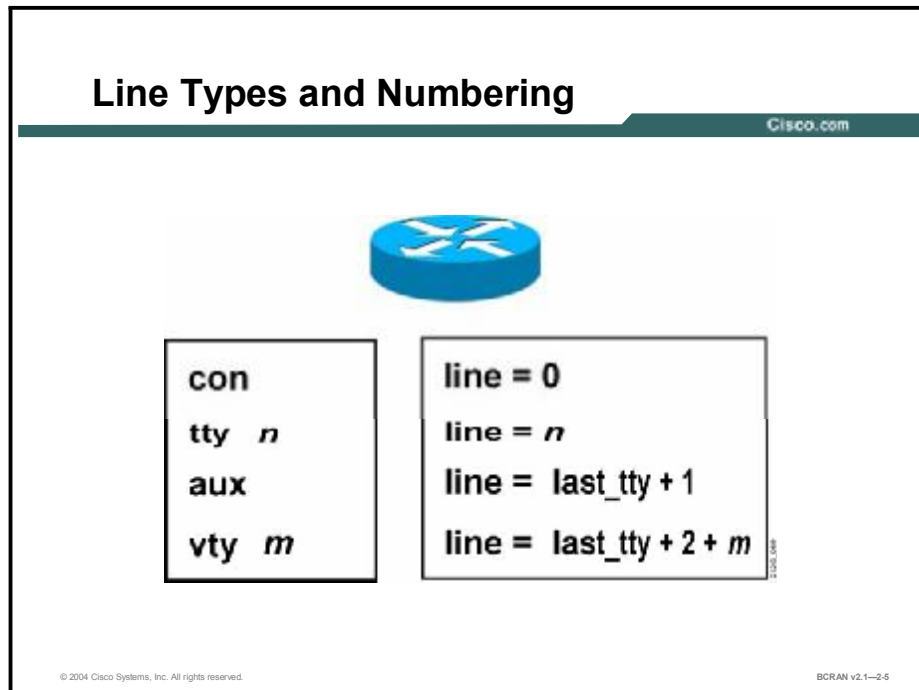
Additional Telnet-Related EXEC Commands

Command	Description
show session	Displays the current connections (sessions) for this user. The older version of this command was the where command.
show users	Displays all current users and their ports.
clear line [number]	Resets a line/port to an idle state and disconnects any sessions associated with that line.

- **Roty:** Rotary group configured for the line.
- **AccO, AccI:** Output or input access list number configured for the line.
- **Uses:** Number of connections established to or from the line since the system was restarted.
- **Noise:** Number of times noise has been detected on the line since the system was restarted.
- **Overruns:** Hardware (UART) overruns or software buffer overflows, both defined as the number of overruns or overflows that have occurred on the specified line since the system was restarted. Hardware overruns are buffer overruns indicating that the UART chip has received bits from the software faster than it can process them. A software overflow occurs when the software has received bits from the hardware faster than it can process them.

Line Types and Numbering

This topic describes the concept of line numbering for reverse Telnet among various router platforms.



Line numbering varies among router platforms. TTY lines correspond to asynchronous interfaces on a one-to-one basis; vty lines are virtual lines that are dynamically assigned to the synchronous interfaces. Usually, vty lines are associated with incoming Telnet sessions.

In the figure shown, m refers to the number of the vty lines. For example, the vty 0 line corresponds to line 10 on a router with eight TTY ports (`con` = line 0, `tty` = lines 1 through 8, `aux` = line 9, `vty` = lines 10 through 14).

Connections to an individual line are most useful when a dial-out modem, parallel printer, or serial printer is attached to that router line. To connect to an individual line, the remote host or terminal must specify a particular TCP port on the router. If the Telnet protocol is used, that port is 2000 plus the line number. For example:

```
telnet 131.108.30.40 2001
```

This command initiates a Telnet connection to line 1 ($2000 + 1$).

The following line types are used:


- **CON:** Console port (available on all Cisco routers)
- **TTY:** Asynchronous port.
- **AUX:** Auxiliary port (available on most Cisco routers except the Cisco 600, 700, 800, 1000, and 1600 platforms).
- **VTY:** Virtual terminal (for incoming Telnet, local-area transport [LAT], or X.25 packet assembler/disassembler [PAD] connections).

Interface Asynchronous and Line Configuration

This topic describes line configuration and asynchronous interface configuration.

Interface Asynchronous and Line Configuration

Cisco.com



Logical Configuration

```
Router(config)#interface async 8
Router(config-if)#encapsulation ppp
Router(config-if)#async dynamic address
Router(config-if)#peer default ip address 10.2.3.4
Router(config-if)#async mode interactive
Router(config-if)#ppp authentication chap
```

Physical Configuration

```
Router(config)#line 8
Router(config-line)#login local
Router(config-line)#modem inout
Router(config-line)#speed 115200
Router(config-line)#flowcontrol hardware
Router(config-line)#autoselect ppp
```

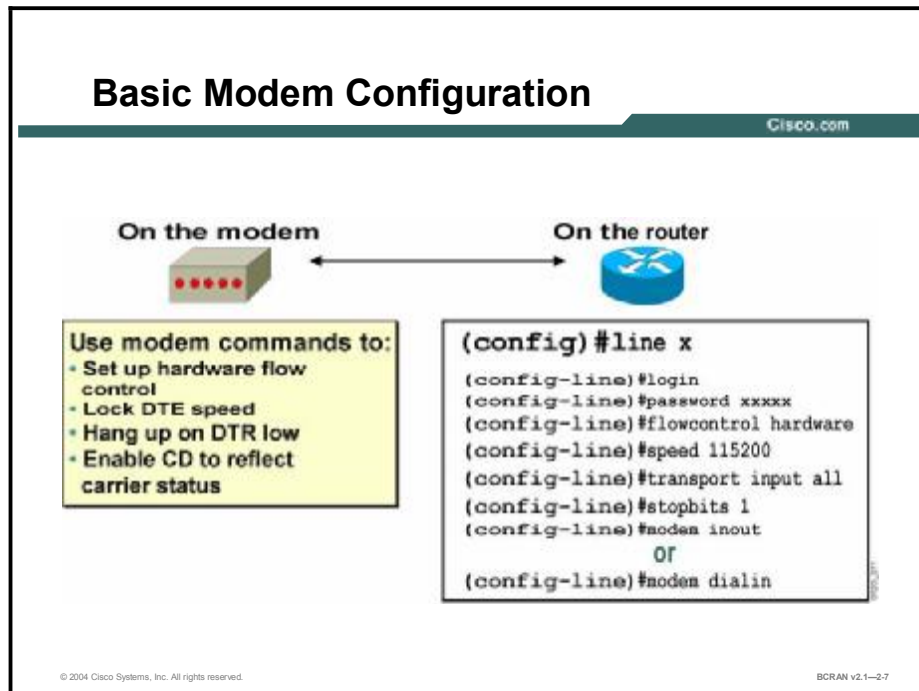
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.6

There is often confusion about the difference between the **interface async** and **line** commands. The major difference is that the **interface async** command lets you configure the protocol (logical) aspects of an asynchronous port, while the **line** command lets you configure the physical aspects of the same port. The **async** commands are internal, while the **line** commands configure external characteristics of the configuration.

For example, you configure the basic modem-related parameters on a router using the **line** command. However, you configure the protocol encapsulation and authentication schemes with the **interface async** command.

Basic Modem Configuration

This topic describes the basic modem configuration on a Cisco router.



To make a successful asynchronous connection, you must configure the modem and the router properly.

A modem must be configured to do the following:

- Perform hardware flow control.
- Lock DTE speed to ensure that the modem will always communicate with the router at the specified speed (in this case, 115.2 kbps). The router **speed** command sets both transmit and receive speeds.
- Hang up when you quit a session.
- Have the CD signal reflect the carrier state truthfully.

On the router, use the commands in the table to configure the line to which the modem is attached.

Line Commands

Command	Description
exec	Allows the EXEC process on this line.
login	Sets a login password on this line. Without the password, no connection is allowed.
password	Sets the password to be used when logging in to this line.
flowcontrol hardware	Uses RTS/CTS for flow control.
speed 115200	Sets the maximum speed (in bits per second) between the modem and the router. The speed command sets both the transmit and receive speed.
transport input all	Allows all protocols to be passed to the router through this line.
stopbits	Sets the number of stop bits transmitted per byte.
modem inout	Uses the modem for both incoming and outgoing calls.
modem dialin	Uses the modem for incoming calls only (the default).

Note Software flow control (xon and xoff characters) is not recommended with modems and Cisco routers.

Standard Modem Commands

This topic describes how to configure the most common modem commands.

Standard Modem Commands

Cisco.com

Action intended	Command
Loads factory default settings	AT&F
Auto answer	ATS0=n
CD truly reflects line state	AT&C1
Hangs up at DTR low	AT&D2
Ignore "+++" (in-band signaling)	ATS2=255
Echo off	ATE0
Turn off speaker	ATM0

Saving the configuration AT&W

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1-2-8

Attention commands for the modem have an AT prefix. In general, each modem vendor has its own modem command set that differs from other vendor command sets.


However, some modem commands are common among most vendors, as described in the table.

Common Modem Commands

Command	Description
AT&F	Loads the factory default settings (read only).
ATS0=1	Sets the modem to answer all incoming calls automatically on the first ring (recommended to be set to 2 for lines with caller ID).
AT&C1&D3	Sets up modem control (CD and DTR).
ATS2=255	Ignore the +++ command. The +++ characters set the modem to command mode. You may need to configure the far-end modem to ignore +++ because the +++ command issued to the near-end modem will be transmitted to the far-end modem. The far-end modem may interpret it and cause the connection to hang. This is a bug in the far-end modem. Many modems are affected.
ATE0	When echo <i>off</i> is set, the modem will not echo keystrokes.
ATM0	Turns off the external audio output from the modem.
AT&W	Saves the modem configuration into nonvolatile memory.

Nonstandard Modem Commands

This topic describes the nonstandard modem commands for proper modem operation.

Nonstandard Modem Commands			
	Microcom	Hayes	USR
 Hardware flow control	AT\Q3	AT&K3	AT&H1&R2
Lock DTE speed	AT\J0	AT&Q6	AT&B1
Error correction	AT\N6	AT&Q5	AT&M4
Compression	AT%C1	AT&Q9	AT&K1
Show configuration	AT\S1	AT&V	ATI4
Getting help	AT&H	AT&H	AT&
Saving the configuration	AT&W	AT&W	AT&W

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.9

Many modem commands are not standardized and vary from one vendor to another. The following modem configurations and commands are essential for modems that are attached to Cisco routers:

- **Hardware flow control:** Use CTS and RTS.
- **Lock DTE speed:** Sets the serial port of the modem to a fixed data transfer rate. Locking the speed between the modem and DTE device prevents the speed from being negotiated down during the initial call setup.
- **Error correction:** Sets error control.
- **Compression:** Uses the best compression algorithm that can be negotiated between the two communicating modems.
- **Show configuration:** Shows current modem settings.
- **Getting help:** Shows all of the AT commands for your specific modem.
- **Saving the configuration:** Saves the configuration you just entered in the NVRAM of the modem.

For nonstandard modem commands, refer to the vendor user manual that comes with each modem you have purchased.

Modem Initialization Strings

This topic describes modem initialization strings for proper modem operation.

Modem Initialization Strings

Cisco.com

U.S. Robotics (USR) Courier

`at&fs0=1&c1&d3&h1&r2&b1&m4&k1&w`

Hayes Optima/Accura

`at&fs0=1&c1&d2&k3&q9&w`

Microcom QX4232 series

`at&fs0=1&c1&d2\q3\j0\n6%c1&w`

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—2-10

Initialization strings are used to send commands to modems before they dial out. The figure displays some examples of modem initialization strings.

Command strings differ from vendor to vendor, model to model, and even from one firmware version to another. Always refer to the user manual from your modem vendor for the proper modem commands to use.

Note A good exercise is to decode the initialization strings in the figure to see exactly what is and what is not turned *on*, and to see how the command strings differ from vendor to vendor.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configuring a modem is complex task.**
- **Several commands can be used to determine line numbering on a Cisco router.**
- **Initialization strings can differ from vendor to vendor and model to model.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2-11

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which type of connection does a remote terminal user make when dialing into the router through an asynchronous line?
- A) forward connection
 - B) reverse connection
 - C) moving connection
 - D) stopped connection
- Q2) Which command displays all current users and their ports?
- A) **show people**
 - B) **show session**
 - C) **show users**
 - D) **show staples**
- Q3) Which command displays more detailed information on the specified line?
- A) **show line *detailed***
 - B) **show line line-number**
 - C) **show line *information detailed***
 - D) **show *detailed line***
- Q4) What is a vty line?
- A) virtual line dynamically assigned to the synchronous interface
 - B) permanent connection between two switches
 - C) very tight yellow line used for RJ-45 cables
 - D) a high-speed broadband connection cable
- Q5) Which command lets you configure the protocol (logical) aspects of an asynchronous port?
- A) **line**
 - B) **enable password**
 - C) **enable secret port**
 - D) **interface async**

- Q6) When in (config-line)# mode, what does the router **speed** command set?
- A) the boot time of the router
 - B) the data speed of the Ethernet port
 - C) transmit and receive speeds
 - D) the amount of bandwidth that you are requesting from your service provider at peak usage periods
- Q7) What does AT stand for in modem commands?
- A) at time commands
 - B) async T1 commands
 - C) autotransmit commands
 - D) attention commands
- Q8) Which command signals are involved in hardware flow control?
- A) DTE and DCE
 - B) VTP and FTP
 - C) CTS and RTS
 - D) OPP and POP
- Q9) What do modem initialization strings do?
- A) send commands to modems before they dial out
 - B) send e-mail attachments to modems before they dial out
 - C) send printer requests to the video monitor so that the modem will process them first
 - D) secure a modem to the back of a computer properly

Quiz Answer Key

- Q1) A
Relates to: Modem Connections
- Q2) C
Relates to: EXEC Connection Commands
- Q3) B
Relates to: Sample Output for the **show line** Command
- Q4) A
Relates to: Line Types and Numbering
- Q5) D
Relates to: Interface Asynchronous and Line Configuration
- Q6) C
Relates to: Basic Modem Configuration
- Q7) D
Relates to: Standard Modem Commands
- Q8) C
Relates to: Nonstandard Modem Commands
- Q9) A
Relates to: Modem Initialization Strings

Autoconfiguring Modems

Overview

Modem autoconfiguration simplifies the process of adding a modem for out-of-band management or remote dial-in connectivity. This lesson contains descriptions of modem autoconfiguration methods and commands to reduce the complexity of modem initialization.

Relevance

This lesson describes the process of modem autoconfiguration. Modem autoconfiguration eliminates the process of manually issuing the initialization strings on a modem.

Objectives

Upon completing this lesson, you will be able to:

- Configure modem autoconfiguration with a generic modem type
- Configure modem autoconfiguration with a specified modem type
- Verify the modemcap database
- Configure the modemcap database with a custom modemcap

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Cisco Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Modem Autoconfiguration
- Automatic Modem Configuration
- Modem Autodiscovery
- Modem Autoconfiguration: Configuring
- Modem Autodiscovery: Configuring
- Known Modem Initialization String
- Modemcap Database
- Modemcap Database Management
- Modemcap Entries: Viewing
- Custom Modemcap Entry: Creating and Editing
- Custom Modemcap Entry: Viewing
- Summary
- Quiz

Modem Autoconfiguration

This topic describes modem autoconfiguration.

Using Modem Autoconfiguration

Cisco.com

Autoconfiguration is used to:

- **Configure modems without using modem configuration commands**
- **Autodiscover modems**

Operational areas:

- **Automatic modem configuration**
- **Modem autodiscovery**
- **Modemcap database management**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-2.2

Modem autoconfiguration facilitates the configuration of modems on routers. To set up a modem using modem autoconfiguration, connect the phone line and power cable to the modem, and use the **modem autoconfigure** command on the line with the modem. No other setup function is required for most modems.

You can use the modem autoconfiguration feature when you want to:

- Configure a modem without sending modem configuration commands directly to the modem
- Use the asynchronous interface to autodiscover the modem type

To better understand modem autoconfiguration, consider its properties and characteristics:

- **Automatic modem configuration:** You can configure a line to use a specified modem type.
- **Modem autodiscovery:** You can configure a line to automatically attempt to discover the type of modem on the line and to use that modem configuration.
- **Modem capability database (modemcap file in Cisco IOS software):** A modemcap is a database of modems and their modem configuration command strings.

Automatic Modem Configuration

This topic describes the process of modem autoconfiguration.

Automatic Modem Configuration

Cisco.com

With modem autoconfiguration, modems:

- **Are reconfigured each time the line is reset (AT commands are sent)**
- **Can use a customized line configuration**
- **Are configured to match current line settings**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—2.3

With automatic modem configuration, each time a modem is reset, a chat script is executed that sends a string of modem configuration commands (AT commands) to the modem. This modem configuration command string is generated automatically whenever the modem is recycled.

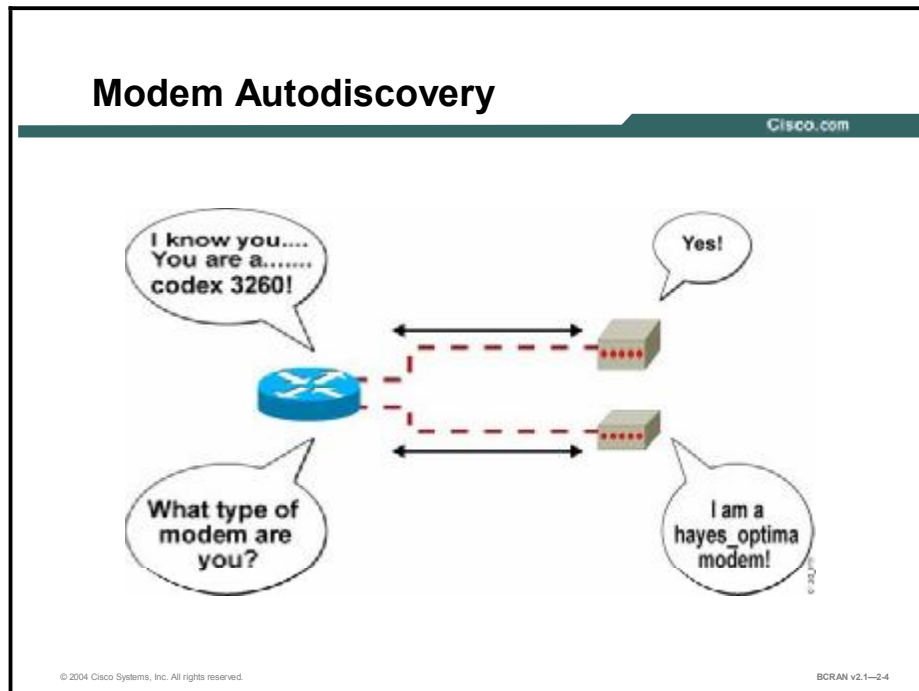
For example, an IP dial-in modem configured with flow control would receive this command sequence:

- Return to factory defaults
- Use hardware flow control
- Other modem configuration commands

In addition, the line configuration may be changed if the speed specified for the modem DTE differs from the current configuration on the line.

Modem Autodiscovery

This topic discusses modem autodiscovery in determining a specific modem model.



You can configure a line to expect a specific modem mode. If no modem is specified, the router attempts to autodiscover the type of modem to which it is attached. The router determines the type of modem by sending AT commands to the modem and evaluating the response. The router includes a modemcap database with information on the following modems:

- **Codex 3260:** codex_3260
- **U.S. Robotics Courier:** usr_courier
- **U.S. Robotics Sportster:** usr_sportster
- **Hayes Optima:** hayes_optima
- **Global Village:** global_village
- **Viva:** viva
- **Telebit t3000:** telebit_t3000
- **Microcom:** microcom_hdms, microcom_server
- **NEC:** nec_v34, nec_v11, nec_piafs
- **Cisco Systems:** mica, cisco_v110

The specific modemcap entries found on a particular system will be determined by the hardware and Cisco IOS software version that is installed.

Note Whenever possible, configure the modem to eliminate the overhead of modem autodiscovery.

Any modems that are not currently supported in the list can be manually added to the list to be autodiscovered in future communication.

Here is a sample debug of how a router establishes synchronization with a modem:

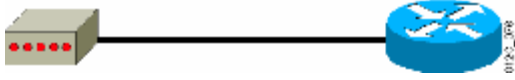
```
RTA#
6d19h: TTY1: Line reset by "Virtual Exec"
6d19h: TTY1: Modem: IDLE->HANGUP
6d19h: TTY1: destroy timer type 0
6d19h: TTY1: destroy timer type 1
6d19h: TTY1: destroy timer type 3
6d19h: TTY1: destroy timer type 4
6d19h: TTY1: destroy timer type 2
6d19h: TTY1: dropping DTR, hanging up
6d19h: TTY1: Set DTR to 0
6d19h: tty1: Modem: HANGUP->IDLE
6d19h: TTY1: restoring DTR
6d19h: TTY1: Set DTR to 1
6d19h: TTY1: autoconfigure probe started
6d19h: TTY1: Modem command: --AT&F&C1&D2S0=1H0--
6d19h: TTY1: Modem configuration succeeded
6d19h: TTY1: Detected modem speed 38400
6d19h: TTY1: Done with modem configuration
```

Modem Autoconfiguration: Configuring

This topic describes the process of configuring modem autoconfiguration.

Configuring Modem Autoconfiguration

Cisco.com



The diagram illustrates a connection between a modem and a Cisco router. On the left is a grey modem with four red indicator lights. A black line connects it to a blue Cisco router on the right, which has a white 'X' on its top surface and the text '0123_200' on its side.

Configuration may include:

- Configuring modem autodiscovery

or

- Specifying a specific modem type
- Managing the modemcap database

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-2-5

Modem autoconfiguration includes the following tasks:


- **Configuring modem autodiscovery:** You can configure the line to detect the type of modem connected to the line.
- **Specifying a modem to be used on the line:** Whenever the line resets, the line automatically sends the correct initialization command string to the modem.
- **Managing the modemcap database, including:**
 - Viewing the types of modems that are in the modemcap database.
 - Displaying and modifying modemcap entry command strings.
 - Creating and viewing a variant modemcap entry.
 - Use the **show modemcap** command to view the types of modems that are in the modemcap file. The **show modemcap *modem-type*** command allows you to view the initialization string for the specific modem type entered.

Modem Autodiscovery: Configuring

This topic describes the commands that are used to implement modem autodiscovery.

Configuring Modem Autodiscovery

Cisco.com



```
Router#configure terminal
Router(config)#line 1 16
Router(config-line)#modem autoconfigure discovery
Router(config-line)#end
Router#copy running-config startup-config
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-2.6

As shown in the figure, the **modem autoconfigure discovery** command configures modem autodiscovery.

This command instructs the router to do the following on lines 1 through 16:

- Send the AT string at various baud rates until it receives an OK
- Send a variety of AT commands, attempting to receive a complete identification of the modem identified in the router modemcap

The default modem entry is used if the router cannot determine the modem type.

If you know that your modem can be configured using an initialization string from one of these scripts, you can issue the modem **autoconfigure type type** command, where **type** is one of the strings in the modemcap list. Initialization proceeds more quickly if you list a specific modem type.

Note To eliminate the overhead of modem autodiscovery and to avoid modem configuration ambiguity that is caused by modem autodiscovery, configure the modem type using the **autoconfigure type** command whenever possible.


It may be necessary to manually configure the modem or change the modemcap database if none of the strings properly initialize the modem.

Known Modem Initialization String

This topic describes the commands that are used to configure modem autodiscovery with a specified modem model.

Specifying a Known Modem Initialization String

Cisco.com



```
Router#configure terminal
Router(config)#line 1
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#end
Router#copy running-config startup-config
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.7

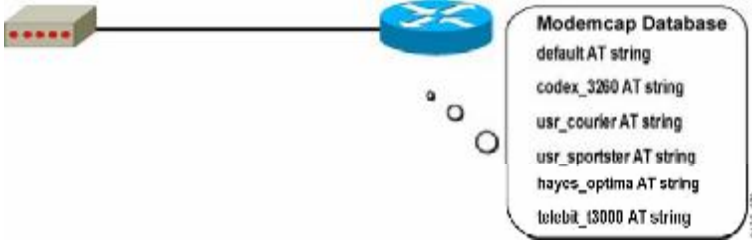
In the figure shown, the router is configured to send an initialization string for a U.S. Robotics Sportster modem on line 1.

Modemcap Database

This topic describes the purpose of a modemcap database on a Cisco router.

Modemcap Database

Cisco.com



You can:

- View the modemcap database
- Add entries to the modemcap database

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.8

The modemcap is a list of modems with a known set of AT configuration commands for setting the attributes for each modem type. For example, many modems use the string **AT&F** to reset the modem to its factory default attributes.

Modem attributes have a full name and a two- or three-letter abbreviation. Factory default, for example, is also referred to as FD. For normal operation, you do not need to know these abbreviations. If you are familiar with the modem abbreviations, you can add entries to the modemcap database.


Modemcap Database Management

This topic describes the commands for managing the modemcap database.

Managing the Modemcap Database

Cisco.com

```
Router#show modemcap
default
codex_3260
usr_courier
usr_sportster
hayes_optima
global_village
viva
telebit_t3000
microcom_hdms
microcom_server
nec_v34
nec_v11
nec_pi4fs
cisco_v110
mica
```



© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.8

The modemcap database contains entries for supported modems. Complete these tasks to manage a modemcap database entry:

- View modem entries in the modemcap database with the **show modemcap command**, as shown in the figure.
- View the contents of a modem modemcap entry.
- Modify a modem modemcap entry.
- Create a modem database entry.

Modemcap Entries: Viewing

This topic describes the concepts and commands for viewing modemcap entries.

Viewing Modemcap Modem Entries

Cisco.com

```
Router#show modemcap codex 3260
Modemcap values for codex_3260
Factory Defaults (FD): &F
Autocanswer (AA): &Q=1
Carrier detect (CD): &C1
Drop with DTR (DTR): &D2
Hardware Flowcontrol (HFL): *FL3
Lock DTE speed (SPD): *SC1
Best Error Control (BER): *SM3
Best Compression (BCP): *DC1
No Error Control (NER): *SM1
No Compression (NCP): *DC0
No Echo (NEC): E0
No Result Codes (NRS): Q1
Software Flowcontrol (SFL): [not set]
Caller ID (CID): &S1
Miscellaneous (MSC): [not set]
Template entry (TFL): default
```

• **AT commands for a specific modem**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1--2-10

The **show modemcap** command displays the modems in the modemcap database. In addition, with the modem type specified, the command shows a complete list of the specified modem modemcap entry that includes these fields:

- Command description
- Command abbreviation (with colon separator)
- Command string

The figure shows the **AT** command string attributes and their values for the Codex 3260 modem.

The default modem type has modemcap values for a few of the most common attributes. It does not contain strings for attributes that vary widely by modem type, such as locking speeds, setting hardware flow control, or dealing with compression and error correction.

You can use the **modemcap entry *modem-name*** command or the **show modemcap *modem-name*** command to see the contents of a modem modemcap entry. The **modemcap entry *modem-name*** command displays modemcap values in a truncated form.

You can also create variant modemcap entries to add new modems or extend the functionality of a modem in the modemcap database. How these entries are created is discussed in subsequent topics in this lesson.

Custom Modemcap Entry: Creating and Editing

This topic describes the commands that are necessary to create and edit a modemcap entry.

The screenshot shows a Cisco router configuration terminal with the following commands and output:

```
Router#config terminal
1 Router#(config)modemcap edit usr_new caller-id *U1
2 Router#(config)modemcap edit usr_new speed &B1
3 Router#(config)modemcap edit usr_new template usr_courier
```

The output of the `show modemcap` command is:

```
Router#show modemcap
codex_3260
usr_courier
usr_sportster
hayes_optima
global_village
usr_new
...
```

An arrow labeled "New Entry" points to the `usr_new` entry in the output.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.11

Use the **modemcap edit *new-modem-name*** command to complete these tasks:

- Add a new entry to the modemcap database. Note that in performing this task, you must specify an attribute for the new modem entry; otherwise, use **modemcap entry *new-modem-name*** without attributes.
- Add new attributes to an existing modem entry in the modemcap database.

The figure displays the following uses of the **modemcap edit *usr_new*** command:

1. This command creates the **usr_new** entry in the modemcap database and sets the **caller-id** for the **usr_new** modem to ***U1**.
2. This command locks the DTE speed on this modem.
3. This command points to another modemcap entry to be used as a template. As a result, any value not found in the current modemcap entry is set by the template modemcap entry. In this example, the **usr_courier** modemcap entry is the template. You can have up to four layers of templates.

You can use these additional commands when creating variant modem cap entries:

- Use the **modemcap edit** command to edit user-created modemcap entries only.
- Use the **show modemcap** command to verify the new router modemcap entry.
- Use the **no modemcap entry *modem-name*** command to remove the specified modem from the modemcap database.
- Use the **no modemcap entry *modem-name attribute*** command to remove a modem attribute from a modem modemcap entry.

Custom Modemcap Entry: Viewing

This topic contains concepts and commands for viewing a modemcap entry.

Viewing a Custom Modemcap Entry

Cisco.com

```
Router#show modemcap usr_new
Modemcap values for usr_new
Factory Defaults (FD): &F
Autoanswer (AA): S0=1
Carrier detect (CD): &C1
Drop with DTR (DTR): &D2
Hardware Flowcontrol (HFL): &H1&R2
1 Lock DTE speed (SPD): &B1
Best Error Control (BER): &M4
Best Compression (BCP): &K1
No Error Control (NER): &M0
No Compression (NCP): &K0
No Echo (NEC): E0
No Result Codes (NRS): Q1
Software Flowcontrol (SFL): [not set]
2 Caller ID (CID): *U1
Miscellaneous (MSC): [not set]
3 Template entry (TPL): usr_courier
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2.12

After configuring a modemcap entry with the **modemcap edit** command, use the **show modemcap *modem-name*** command to verify the new modemcap attribute values.

The figure shows the output for the new modemcap created in the previous topic. The numbers in the figure correspond to the numbers that are used in the previous topic with each **modemcap edit** command.

Specifically, the **usr_new** modemcap shown in the figure is identical to the **usr_courier** entry with the following exceptions:

- The DTE speed lock
- The caller ID field
- The template

If you used the **show running-config** command, the **usr_new** information for the configuration on the previous page would appear as a line in the configuration:

```
modemcap entry usr_new SPD=&B1:CID=*U1:TPL=usr_courier
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Modem autoconfiguration simplifies the process of adding a modem for out-of-band management or remote dial-in connectivity.**
- **Automatic modem configuration executes a chat script that sends a string of configuration commands to the modem.**
- **The modem capability database is a list of modems with a known set of configuration commands for setting each modem type attribute.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—2-13

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is a modem chat script?
- A) instructions for a modem to self-destruct
 - B) a string of text that defines the handshaking that occurs between two DTE devices
 - C) a set of commands that enable any modem to achieve a doubling of its maximum bandwidth speed
 - D) a session involving the video monitor, keyboard, and printer
- Q2) What is a database of modems and their modem configuration command strings called in Cisco IOS software?
- A) modeminfo
 - B) modemcap
 - C) modemdata
 - D) modemconfigs
- Q3) How does the router determine the type of modem used?
- A) The router sends AT commands to the modem and evaluates the response.
 - B) The router detects the specific modem cable used.
 - C) The router does not need to know the modem type.
 - D) The phone number dialed has a special code for the modem.
- Q4) Which command is used to view the types of modems that are in the modemcap file?
- A) **show modem all**
 - B) **show modem types**
 - C) **show modemcap**
 - D) **show modemfile**
- Q5) Which command do you issue if you know that your modem can be configured using an initialization string from one of the modemcap scripts?
- A) **modem autoconfigure type *type***
 - B) **modem configure**
 - C) **modem configureauto**
 - D) **modem type auto**

- Q6) Which router configuration mode is used in configuring a modem?
- A) router#
 - B) router(config)#
 - C) router(config-line)#
 - D) router(config-if)#
- Q7) Which modem string is typically used to reset the modem to its factory default attributes?
- A) AT&D
 - B) AT&K
 - C) AT&H
 - D) AT&F
- Q8) What does the modemcap database contain?
- A) entries for supported printers
 - B) entries for supported modems
 - C) entries for supported switches
 - D) entries for supported video monitors
- Q9) How do you add new modems or extend the functionality of a modem in the modemcap database?
- A) by purchasing older slower modems for your network
 - B) by creating variant modemcap entries
 - C) by using different modem cables
 - D) by using a printer cable for a modem cable
- Q10) Which command is used to add a new entry to the modemcap database?
- A) router# **show modemcap**
 - B) router# **config line modemcap**
 - C) router# **line modemcap**
 - D) router# **modemcap entry usr_new**
- Q11) After configuring a modemcap entry with the **modemcap edit** command, which of the following commands should be used to verify the new modemcap attribute values?
- A) **show modembase** *modem-name*
 - B) **show modemcap** *modem-name*
 - C) **show modemdata** *modem-name*
 - D) **show modeminfo** *modem-name*

Quiz Answer Key

- Q1) B
Relates to: Modem Autoconfiguration
- Q2) B
Relates to: Automatic Modem Configuration
- Q3) A
Relates to: Modem Autodiscovery
- Q4) C
Relates to: Modem Autoconfiguration: Configuring
- Q5) A
Relates to: Modem Autodiscovery: Configuring
- Q6) C
Relates to: Known Modem Initialization String
- Q7) D
Relates to: Modemcap Database
- Q8) B
Relates to: Modemcap Database Management
- Q9) B
Relates to: Modemcap Entries: Viewing
- Q10) D
Relates to: Custom Modemcap Entry: Creating and Editing
- Q11) B
Relates to: Custom Modemcap Entry: Viewing

Verifying and Debugging Modem Autoconfiguration

Overview

After you connect the modem hardware, you may experience issues with modem autoconfiguration. This lesson explains how to verify and debug modem autoconfiguration.

Relevance

After you configure modem autoconfiguration, it is helpful to know how to troubleshoot and verify the proper operation in the context of dial-in and dial-out services.

Objectives

Upon completing this lesson, you will be able to:

- Issue commands to debug modem autoconfiguration
- Troubleshoot modem autoconfiguration
- Create a chat script for modem initialization

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Verification of Modem Autoconfiguration Operation
- Modem Autoconfiguration Troubleshooting
- Chat Scripts for Asynchronous Lines
- Summary
- Quiz

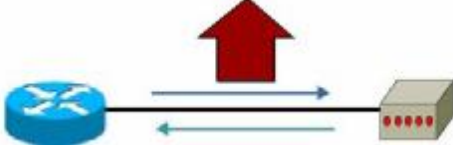
Verification of Modem Autoconfiguration Operation

This topic describes the commands that are used to debug modem autoconfiguration.

Verifying Modem Autoconfiguration Operation

Cisco.com

```
Router#debug confmodem
TTY97: detection speed (115200) response ---OK---
TTY97: Modem command: --AT--
TTY97: Modem configuration succeeded
TTY97: Detected modem speed 115200
TTY97: Done with modem configuration
TTY97: detection speed (115200) response ---OK---
TTY97: Modem command: --AT&F&C1&D2&H1&R2&M4&K1&B1&S0=1H0--
TTY97: Modem configuration succeeded
TTY97: detection speed (115200) response ---OK---
TTY97: Done with modem configuration
```



© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-2.2

The **debug confmodem** command displays the modem configuration process. For example, the figure shows a router modem configuration process on line 97 with a U.S. Robotics Sportster modem attached.

You can also use these commands to verify operation:


- The **show line** command shows the type of modem configured on a line.
- The **clear line** command returns a line to its idle state. Normally this command returns the line to its conventional function as a terminal line, with the interface left in a down state.

Modem Autoconfiguration Troubleshooting

This topic describes the commands that are used to troubleshoot modem autoconfiguration.

Troubleshooting Modem Autoconfiguration

Cisco.com



Common problems with modem autoconfiguration:

- The modem does not respond.
- The modem is not recognized by modem autodiscovery.
- There is an original modemcap entry problem.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—2-3

To troubleshoot modem autoconfiguration, consider the following conditions and solutions:

- Modem not responding
 - Is the modem power supply connected and turned on?
 - Is the power-up configuration set to factory default?
 - Can you connect using reverse Telnet?
 - Do you have dial tone at the phone jack?
- Modem not recognized by modem autoconfigure discovery
 - Use the **show line** command to verify the modem configuration that the line is using.
 - Check to see if the Cisco router recognizes the modem.
 - Use the **modem autoconfigure type *modem-name*** command.

Note Use the **show modemcap** command to verify modemcap support for this modem.

- Original modemcap entry problem
 - If you configured your own modemcap entry, and reconfiguration appears to function, verify that the DTR attribute is *not* set to &D3.


Remember that you can also check the manual supplied by the modem manufacturer.

Chat Scripts for Asynchronous Lines

This topic describes the concepts and commands that are needed to create a chat script.

Chat Scripts for Async Lines

Cisco.com



```
Router(config)#chat-script script-name expect-string send-string
```

- Modem configuration
- Dialing and remote login commands
- Failure detection

```
Router(config)#chat-script Central ABORT ERROR ABORT BUSY  
" " "ATZ" OK "ATDT \T" TIMEOUT 30 CONNECT \c
```

- Sample chat script

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-2.4

The Cisco IOS software autoconfigure feature is sufficient for most modem connections. Occasionally, however, custom chat scripts may have to be written to perform certain tasks.

A chat script provides a way to customize how the DTE interacts with the DCE. It is a string of text that defines the handshaking that occurs between two DTE devices or between a DTE and its directly attached DCE. The chat script consists of expect-send pairs that define the string the local DTE system expects to see from the remote DCE device and that specify which reply the local system should send.

For example, you can configure chat scripts for these tasks:

- Initializing the directly attached modem
- Instructing the modem to dial out
- Logging in to a remote system

The sample chat script command in the figure is described in the table.

Chat Script Commands

Command	Description
Central	Defines the name of this chat script as Central.
ABORT ERROR	Stops the chat script if an error is encountered.
ABORT BUSY	Stops the chat script if a busy signal is encountered.
“”	Expects a null string. Therefore, expect no input string.
“ATZ”	Without expecting an input string, sends the AT command to reset the modem to its stored profile.
OK “ATDT \T”	When the input string OK is seen, sends the AT command to instruct the modem to dial the telephone number in the dialer string or start-chat command.
TIMEOUT 30 CONNECT	Waits up to 30 seconds for the input string CONNECT.
\c	Indicates the end of the chat script.

You can use the **start-chat** command to manually test a chat script on any asynchronous line that is not currently active.

Chat scripts can also be activated by any of the following five events, each corresponding to a different version of the **script** command:

- **Line activation:** Starts a chat script on a line when the line is activated (every time a command EXEC is started on the line).
- **Connection:** Starts a chat script on a line when a network connection is made to the line: triggered by outgoing traffic (reverse Telnet).
- **Startup:** Triggered when the system starts up.
- **Dialer:** Triggered by dial-on-demand routing (DDR).
- **Line reset:** Triggered by asynchronous line reset.

Refer to Cisco.com for more information on chat scripts and the **script** command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The debug confmodem command displays the modem configuration process.**
- **Use the show line command to verify the modem configuration that the line is using.**
- **A chat script provides a way to customize how the DTE interacts with the DCE.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-2-5

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-1: Configuring Asynchronous Connections with Modems

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which of the following commands displays the modem configuration process?
- A) **show line**
 - B) **clear line**
 - C) **show modem process**
 - D) **debug confmodem**
- Q2) What can a network administrator do as a last resort when troubleshooting modem autoconfiguration?
- A) check the manual supplied by the router manufacturer
 - B) check the manual supplied by the modem manufacturer
 - C) check the manual supplied by the hub manufacturer
 - D) check the manual supplied by the switch manufacturer
- Q3) A chat script provides a way to customize how the _____.
- A) DTE interacts with the DTE
 - B) DTE interacts with the DCE
 - C) DCE interacts with the DTE
 - D) DCE interacts with the DCE

Quiz Answer Key

Q1) D

Relates to: Verification of Modem Autoconfiguration Operation

Q2) B

Relates to: Modem Autoconfiguration Troubleshooting

Q3) B

Relates to: Chat Scripts for Asynchronous Lines

Module 3

Configuring PPP Features

Overview

This module reviews PPP and provides additional information on link control protocol (LCP) options of authentication, callback, compression, and Multilink PPP (MLP).

Objectives

Upon completing this module, you will be able to:

- Configure PPP features at a central site and a branch office to allow exchange of data between the sites
- Configure PAP or CHAP authentication to allow access to a secure site
- Configure and verify callback and compression
- Configure and verify MLP
- Verify and troubleshoot an incorrect configuration so data travels as intended across the PPP link

Outline

The module contains these lessons:

- Describing PPP Features
- Configuring Basic PPP
- Configuring LCP Options: Authentication with PAP and CHAP
- Configuring LCP Options: Callback and Compression
- Configuring LCP Options: Multilink PPP
- Verifying and Debugging PPP

Describing PPP Features

Overview

PPP is an RFC standard that provides interoperability among WAN devices of multiple vendors. This WAN protocol operates at the physical and data-link layers of the Open System Interconnection (OSI) model. This lesson describes PPP operation.

Relevance

PPP is a key WAN protocol implemented at many sites. You should understand how PPP operates before you configure its services.

Objectives

Upon completing this lesson, you will be able to:

- Describe how remote nodes can connect using PPP
- Describe the properties of PPP
- Compare and contrast HDLC and PPP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

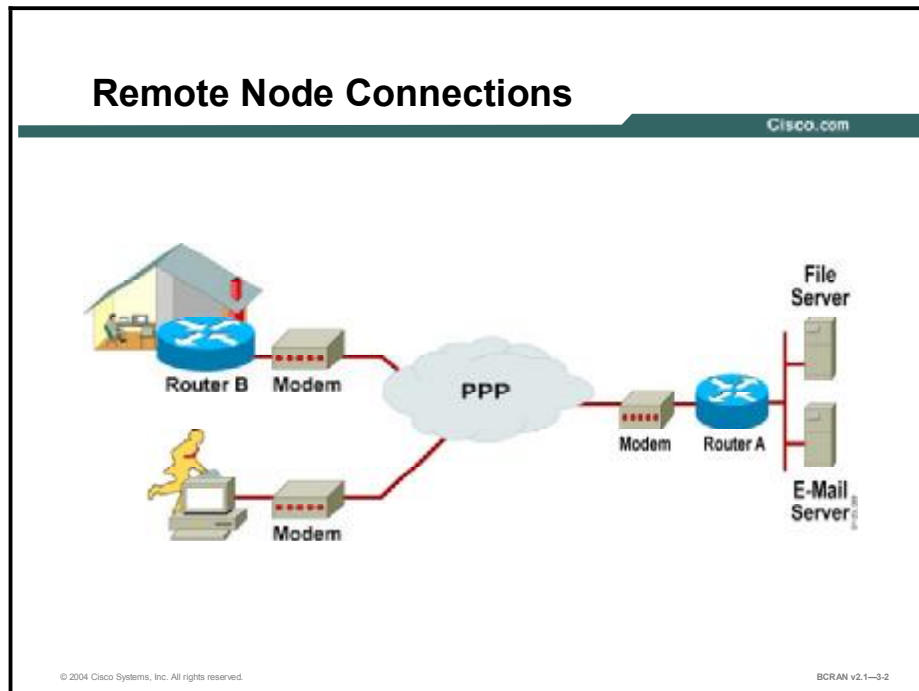
Outline

This lesson includes these topics:

- Overview
- Remote Node Connections
- PPP Architecture
- HDLC and PPP Frames
- Summary
- Quiz

Remote Node Connections

This topic describes how remote node connections can be made using PPP.



Remote access is an integral part of the corporate mission. Traveling salespeople, executives, remote office staff, and small office, home office (SOHO) users all need to communicate by connecting to the central office LAN. The proliferation of laptops in the workplace has increased the need to remotely access electronic information.

To support remote connections, remote node users will use network application software (FTP, Telnet), protocol stacks (TCP/IP), and link-layer drivers (PPP) installed on their own remote devices. The higher-layer protocols are encapsulated in the link-layer protocols (such as PPP) when transmitted across the dialup line.

Point-to-point links between LANs, hosts, terminals, and routers can provide sufficient physical connectivity in many application environments. Many regional and commercial network services provide access to the Internet and point-to-point links, which provide an efficient way to access the service provider locally.

The Internet community has adopted schemes for the transmission of IP datagrams over serial point-to-point lines. One of the schemes, PPP, is a modern transmission method that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.

Although PPP was designed with IP in mind, you can use PPP for other network-layer protocols such as Internetwork Packet Exchange (IPX) and AppleTalk. Moreover, PPP supports essential features such as dynamic address allocation, Password Authentication Protocol (PAP) authentication, Challenge Handshake Authentication Protocol (CHAP) authentication, and Multilink PPP (MLP).

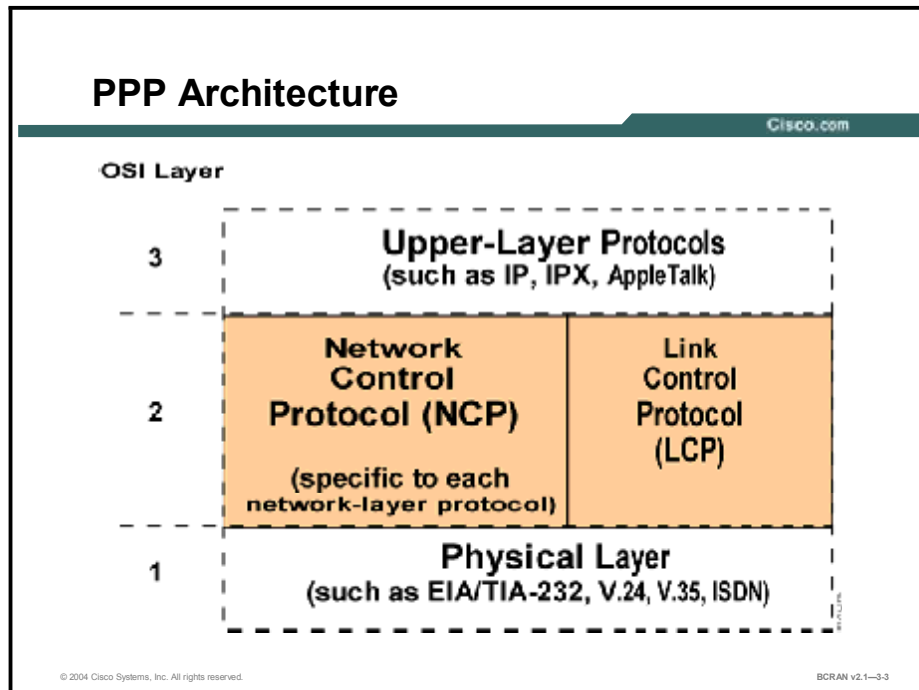
Note The AppleTalk Remote Access Protocol (ARA Protocol) and Serial Line Internet Protocol (SLIP) are not used very frequently in current network configurations, and, as such, they are not covered in this course. For additional configuration information, refer to the Cisco Documentation CD-ROM or Cisco.com.

High-Level Data Link Control (HDLC) is the default encapsulation for ISDN and serial interfaces on a Cisco Systems router. Although HDLC is a default encapsulation, Cisco HDLC is not necessarily compatible with the HDLC implementations of other vendors because it contains a network-layer protocol identifier field. PPP implementations follow open standards and should always be compatible. Therefore, PPP is the protocol of choice when configuring serial links in a multivendor environment.

It is important to note that PPP actually uses HDLC as a basis for encapsulating datagrams. However, PPP is more robust than HDLC because it adds extensions (features) to the link layer.

PPP Architecture

This topic describes the PPP architecture at Layer 2 of the OSI model. PPP is an RFC standard protocol.



PPP is a nonproprietary protocol that is defined by a series of open Internet standards called RFC standards. For this reason, PPP is referred to as a standards-based protocol.

PPP also describes mechanisms for the following features:

- Network-protocol multiplexing
- Link configuration
- Link-quality testing
- Authentication
- Header compression
- Error detection
- Link-option negotiation

PPP also includes these functional components:

- Method for encapsulating datagrams over serial links, based on the International Organization for Standardization (ISO) HDLC protocol (not Cisco HDLC)
- Link control protocol (LCP) for establishing, configuring, and testing the data-link connection
- PPP IP Control Protocol (IPCP), for managing TCP header compression and IP address negotiation
- Authentication
- Network Control Protocols (NCPs) for establishing and configuring various network-layer protocols such as IP, IPX, and AppleTalk (for example, IPCP is the NCP for IP)

Note Authentication level for access control is optional.

The following is a partial list of RFCs of interest for access products:

- RFC 1220: “Point-to-Point Protocol Extensions for Bridging”
- RFC 1332: “PPP IP Control Protocol (IPCP)”
- RFC 1378: “PPP AppleTalk Control Protocol (ATCP)”
- RFC 1492: “Access Control Protocol or TACACS+”
- RFC 1549: “PPP in HDLC Framing”
- RFC 1552: “The PPP Internetwork Packet Exchange Control Protocol (IPXCP)”
- RFC 1570: “PPP LCP Extensions”
- RFC 1661: “The Point-to-Point Protocol (PPP)”
- RFC 1990: (Replaces RFC 1717): “The PPP Multilink Protocol (MP)”

HDLC and PPP Frames

This topic describes the similarities and differences between HDLC and PPP frames.

Comparing HDLC and PPP Frames

Cisco.com

HDLC ISO Frame

Flag	Address	Control	Data (Payload)	FCS	Flag
1 byte	1 byte	1 or 2 bytes	1500 bytes	2 (or 4) bytes	1 byte

PPP Frame

Flag	Address	Control	Protocol	LCP	FCS	Flag
1 byte	1 byte	1 byte	1 or 2 bytes	Up to 1500 bytes	2 (or 4) bytes	1 byte

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3-4

As mentioned earlier, the PPP frame format is based on the HDLC frame format put forth by the ISO. But unlike the ISO HDLC frame, the PPP frame defines two additional fields. The protocol and LCP fields are the keys to the features of PPP.

PPP can negotiate link options dynamically and can support multiple Layer 3 protocols, such as IP, IPX, and AppleTalk. PPP accomplishes these two tasks by encapsulating Layer 3 datagrams with a specialized frame.

The protocol field is used to identify various Layer 3 protocols, such as IP or IPX. The LCP field allows for such features as authentication, callback, compression, and MLP. The address field consists of a broadcast address (all ones), because there is no station address in PPP.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Point-to-point links between LANs, hosts, terminals, and routers can provide sufficient connectivity in many application environments.**
- **PPP is a nonproprietary protocol that is defined by a series of open Internet standards.**
- **PPP can negotiate link options dynamically and can support multiple Layer 3 protocols.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-5

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which upper-level protocols are supported by PPP?
- A) IP
 - B) IPX
 - C) AppleTalk
 - D) all of the above
- Q2) Which of the following protocols is referred to as a “standards-based protocol”?
- A) HDLC
 - B) SLIP
 - C) ARA Protocol
 - D) PPP
- Q3) Which field of the PPP frame identifies various Layer 3 protocols?
- A) flag
 - B) address
 - C) control
 - D) protocol

Quiz Answer Key

Q1) D

Relates to: Remote Node Connections

Q2) D

Relates to: PPP Architecture

Q3) D

Relates to: HDLC and PPP Frames

Configuring Basic PPP

Overview

You can use PPP to connect your LAN to the WAN of your service provider. This lesson describes how to use this protocol to encapsulate both data-link layer and network layer information over serial links and how to configure PPP.

Relevance

You may have PPP connections within your network or between your network and a service provider. You should know how to configure the serial ports for PPP encapsulation.

Objectives

Upon completing this lesson, you will be able to:

- Use the Cisco IOS software commands to configure serial interfaces using PPP encapsulation for leased-line connections
- Enable autoselection of PPP encapsulation on an asynchronous interface
- Configure Layer 3 addressing on a serial interface
- Describe the various LCP options for PPP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- PPP: Enabling
- PPP Session and EXEC Session
- PPP and Asynchronous Interface: Enabling Commands
- Autoselect
- Asynchronous Interface Commands for Addressing
- Summary
- Quiz

PPP: Enabling

This topic describes the commands to enable PPP encapsulation.

Enabling PPP

Cisco.com

```
Router(config-if)# encapsulation ppp
```

- Defines encapsulation type

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3.2

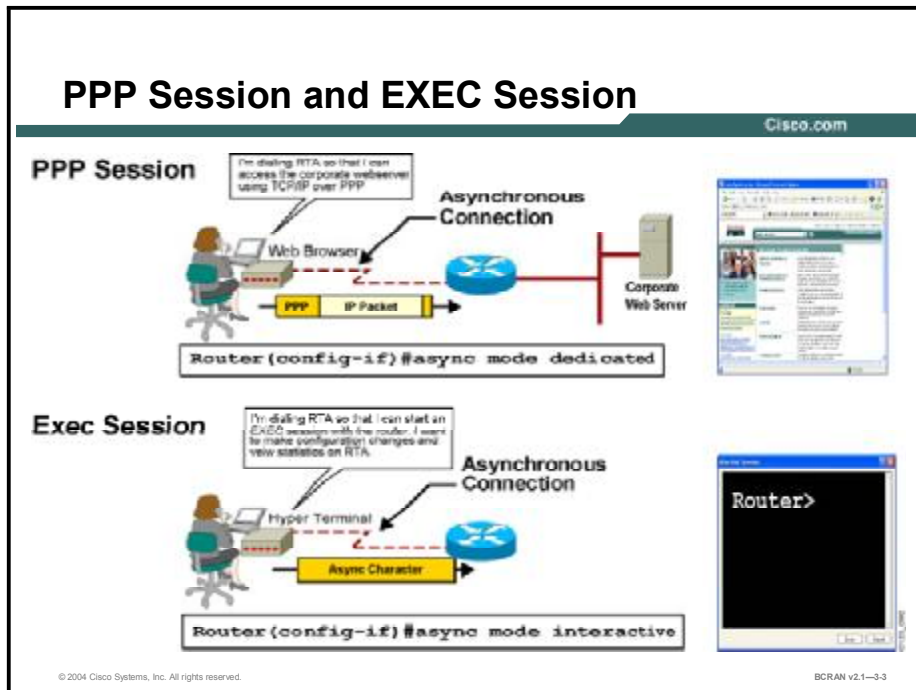
PPP can be enabled on various types of interfaces, including synchronous, asynchronous, serial, ISDN BRI, and ISDN PRI interfaces. The syntax to enable PPP is the same, regardless of interface.

An example of configuring PPP on a synchronous interface would be:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

PPP Session and EXEC Session

This topic describes the concepts of initiating PPP via an in-band PPP session and an out-of-band EXEC session.



You can use asynchronous connections as either an in-band PPP session or an out-of-band EXEC session.

An in-band PPP session is the most common type of connection because it provides users access to network resources such as web servers and mail servers. You can configure PPP in-band as a dedicated session (dedicated mode) or an interactive session (interactive mode). In dedicated mode, an interface is automatically configured for PPP connections. In interactive mode, the user can choose between an in-band and an out-of-band session.

Generally, you will want to restrict the ability of remote users to start EXEC sessions with your router. Typical end users do not require access to the router interface. Instead, they need a Layer 3 protocol (IP and so on) connection to the corporate network or the Internet. In most cases, you should force the asynchronous interface to use PPP and not allow an EXEC connection.

To ensure that the dial-in user must run PPP on the specified line, use the **async mode dedicated** command:

```
Router(config-if) # async mode dedicated
```

An out-of-band EXEC session is typically configured to allow administrators and power users to access the router command-line interface (CLI). This feature allows remote users to log in to the router and issue commands as if the user were connected to the console port. IP addressing or PPP encapsulation is not necessary for this type of connection. Data is sent as asynchronous characters.

PPP and Asynchronous Interface: Enabling Commands

This topic describes the steps that are necessary to correctly enable PPP on an asynchronous interface.

Enabling PPP and Async Interface Commands

Cisco.com

```
Router(config-if)# encapsulation ppp
```

- Defines encapsulation type

```
Router(config-if)# async mode dedicated
```

- Places the line in dedicated PPP mode

OR

```
Router(config-if)# async mode interactive
```

- Places the interface in interactive mode (allows an EXEC process)

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3-4

To provide some flexibility to the dial-in user to start either a PPP session or an EXEC session, use the **async mode interactive** command:

```
Router(config-if)# async mode interactive
```

The **async mode interactive** command configures the router so that it will allow the remote host to choose either a PPP session or an EXEC session.

Enabling this feature requires two steps:

Step 1 You must configure the interface with the **async mode interactive** command.

Step 2 You must configure the corresponding terminal line with the **autoselect** command.

The **during-login** optional parameter of the **autoselect** command causes the username and password prompt to display in the remote host terminal window without the user having to press the Return key.

After a host has established an EXEC session, the remote user can switch to a PPP session at any time by issuing the **ppp** command from privileged EXEC mode router prompt.

Note With synchronous connections, there is no differentiation between an EXEC session and a PPP session. Normally, the user would use the synchronous PPP connection the same as an asynchronous PPP session. A user who needed to start an EXEC session on the router would use Telnet to access the router CLI.

Asynchronous Interface Commands for Addressing

This topic describes how to configure Layer 3 addressing on an asynchronous interface.

Asynchronous Interface Commands for Addressing

Cisco.com

```
Router(config-if)#interface async 1
Router(config-if)#ip address ip-address mask
```

- Assigns an IP address to a network interface

```
Router(config-if)#ip unnumbered type number
```

- Configures the asynchronous interface to be unnumbered

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—3-6

Most dialup PPP sessions are established for the purpose of sending and receiving TCP/IP packets. Asynchronous PPP connections allow remote users to dial up and access the corporate IP network or the Internet.

However, to participate in a TCP/IP network, the router interface must have an IP address. The remote nodes must also be assigned an IP address.

To assign an IP address to an access server asynchronous interface, use the standard **ip address** command. The following example configures the IP address of interface async 1:

```
Router(config)# interface async 1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

Access servers can have literally hundreds of asynchronous interfaces. It is also unlikely that all interfaces will be in use at the same time. For this reason, the IP unnumbered feature may be used to help conserve IP addresses. Multiple asynchronous interfaces on the same router can share the same IP address, including an address assigned by the **ip unnumbered** command.

When a serial or asynchronous interface is configured with the **ip unnumbered** command, it does not have an IP address. Packets generated by that interface “borrow” the address of another interface and use that as the source address. You can use the IP unnumbered feature with point-to-point configurations only. The syntax for the **ip unnumbered** command is:

```
Router(config-if)# ip unnumbered type number
```

With this command, the type and number of the interface to borrow the IP address from (ethernet 0, loopback 0, and so on) must be specified. A loopback interface is the ideal line to use as the reference to the **ip unnumbered** command, because it is a virtual interface that never goes down.

The following commands illustrate how to configure an asynchronous interface for IP unnumbered using a loopback interface:

```
Router(config)# interface loopback 0  
Router(config-if)# ip address 10.1.1.1 255.255.255.0  
Router(config-if)# exit  
Router(config)# interface async 1  
Router(config-if)# ip unnumbered loopback 0
```

Asynchronous Interface Commands for Addressing (Cont.)

Cisco.com

```
Router(config-if)# peer default ip address  
                    {address | pool pool-name | dhcp}
```

- Assigns an IP address to a remote node

```
Router(config-if)# async dynamic address
```

- Allows a remote user to specify the IP address

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—3-7

After the router interface is assigned a valid IP address, remote dial-in users must also be assigned a valid IP address. Fortunately, PPP allows for the automatic assignment of IP addresses using a specific address, a pool of addresses, or Dynamic Host Configuration Protocol (DHCP). Alternatively, the access server can be configured to allow the remote host to choose an address.

To assign a default (predefined) IP address to the remote dial-in host, use the **peer default ip address** command. Additionally, the **pool** and **dhcp** arguments allow address allocation from a local pool of addresses or a DHCP server. This example shows how to configure an asynchronous interface to assign a specific IP address to the dial-in host:

```
Router(config)# interface async 1  
Router(config-if)# peer default ip address 10.1.1.2
```

In contrast, the next example displays how to configure a group of asynchronous interfaces (rotary group) to assign IP addresses from a locally defined pool:

```
Router(config)# ip local pool DIAL-IN 10.1.1.2 10.1.1.254  
Router(config)# interface group-async 1  
Router(config-if)# peer default ip address pool DIAL-IN
```

Note The **pool** and **dhcp** options to the **peer default ip address** command require a global command to create the pool of addresses. For example, **ip local pool pool-name starting-address end-address**.

Note A dialer rotary group eases configuration by allowing one logical interface configuration to apply to multiple physical interfaces. Dialer rotary groups are not covered in this course.

Dynamic addressing allows a user to specify the address at the EXEC level when making the connection. If you specify dynamic addressing, the router must be configured with the **async mode interactive** mode. The user will enter the address at the EXEC level.

For example, after the remote user enters the **ppp** EXEC command, the access server will prompt the user for an IP address or logical host name.

To enable this dynamic addressing feature, use the **async dynamic address** command in interface configuration mode:

```
Router(config-if)# async dynamic address
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Cisco IOS software commands can be used to configure serial interfaces using PPP encapsulation for leased-line connections.
- Asynchronous connections can be used as either an in-band PPP session or an out-of-band EXEC session.
- The autoselect command permits the access server to allow an appropriate process to start automatically when a starting character is received.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-8

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which of the following commands will enable PPP encapsulation on a serial interface of a Cisco router?
- A) `router(config)# encapsulation ppp`
 - B) `router(config-if)# encapsulation ppp`
 - C) `router(config-line)# encapsulation ppp`
 - D) `router# encapsulation ppp`
- Q2) Which of the following command modes is used to ensure that the dial-in user runs PPP on the specified line?
- A) `router(config-if)# async mode dedicated`
 - B) `router(config-if)# sync mode dedicated`
 - C) `router(config-if)# dedicated mode sync`
 - D) `router(config-if)# ppp mode dedicated`
- Q3) Which of the following router command modes allows remote users to log into the router and issue commands as if the user were connected to the console port?
- A) `router(config-line)# interface async 1`
 - B) `router(config-if)# encapsulation ppp`
 - C) `router(config-if)# async mode interactive`
 - D) `router(config-if)# interface async 1`
- Q4) When you are configuring PPP, which command permits the access server router to allow an appropriate process to start automatically as soon as a starting character is received?
- A) `autoselect`
 - B) `autoconfig`
 - C) `selectauto`
 - D) `configauto`

Quiz Answer Key

Q1) B

Relates to: PPP: Enabling

Q2) A

Relates to: PPP Session and EXEC Session

Q3) C

Relates to: PPP and Asynchronous Interface: Enabling Commands

Q4) A

Relates to: Autoselect

Configuring LCP Options: Authentication with PAP and CHAP

Overview

To enhance network security, two password protocols are available with PPP. This topic covers the concepts and configuration commands for optional PAP and CHAP authentication with PPP.

Relevance

You can select PAP or CHAP when configuring PPP authentication. In general, CHAP is the preferred protocol. You should know how to enable these two protocols for added network security.

Objectives

Upon completing this lesson, you will be able to:

- Describe the PPP authentication process
- Enable PAP authentication with PPP
- Enable CHAP authentication with PPP
- Enable both CHAP and PAP authentication with PPP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

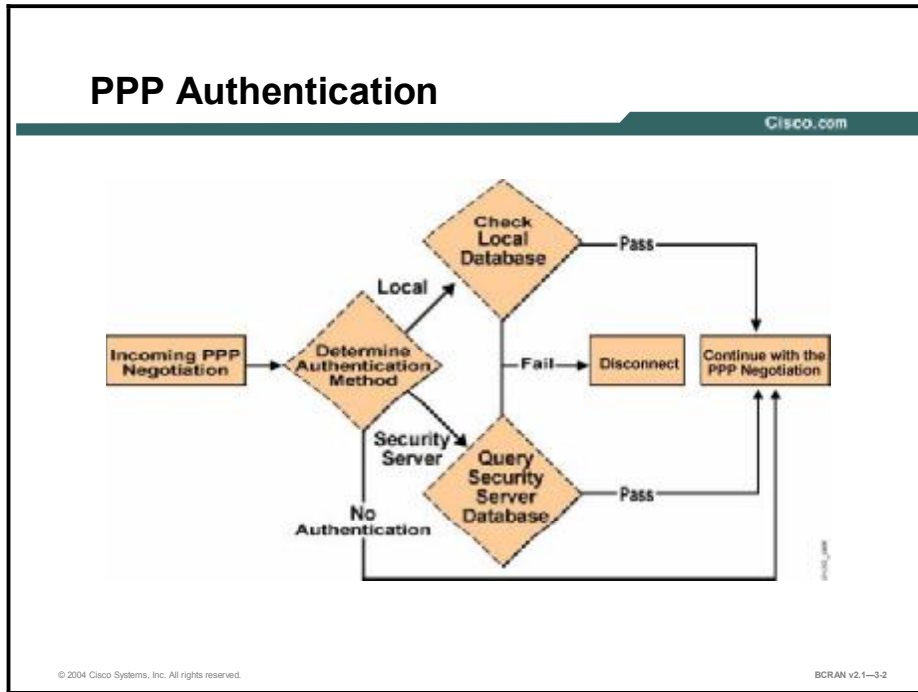
Outline

This lesson includes these topics:

- Overview
- PPP Authentication
- PPP Using PAP Authentication
- PAP Configuration Example
- PPP Using CHAP Authentication
- CHAP Configuration Example
- CHAP and PAP Configuration Authentication
- Summary
- Quiz

PPP Authentication

This topic describes the PPP authentication process.

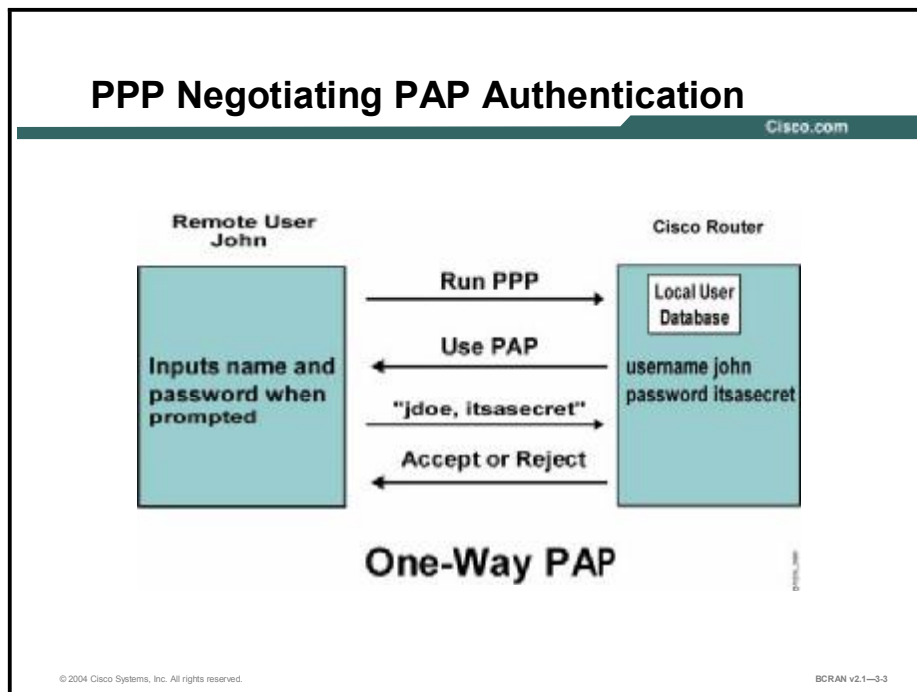


This flowchart in the figure displays the PPP authentication process with PAP or CHAP security as follows:

1. When a user enters the **ppp** command, the system determines the type of authentication configured. If no authentication is configured, the PPP process starts immediately.
2. If the system determines the authentication method to be used, it does one of the following:
 - It checks the local database (established with the **username** and **password** commands) to determine if the given username and password pair matches the pair in the local database (CHAP or PAP).
 - It sends an authentication request to the security server (TACACS+ or RADIUS).
3. The system checks the authentication response sent back from the security server or local database. If the response is positive, the PPP process is started. If it is negative, the user is rejected immediately.

PPP Using PAP Authentication

This topic describes the PAP authentication process. PAP authentication sends passwords in plaintext.



If you have decided to use an authentication protocol, it will likely be PAP or CHAP. PAP is a one-way authentication between a host and a router or a two-way authentication between routers. With PAP, this process provides an insecure authentication method.

When using PAP, the remote host is in control of the frequency and timing of login requests. This situation is undesirable because the router or access server must respond to all login requests, even the repeated attempts of a hacker to guess a username and password combination. (This is known as a brute force attack.) PAP also sends passwords as cleartext over the media, which means that a strategically placed packet sniffer could capture and easily decode the password.

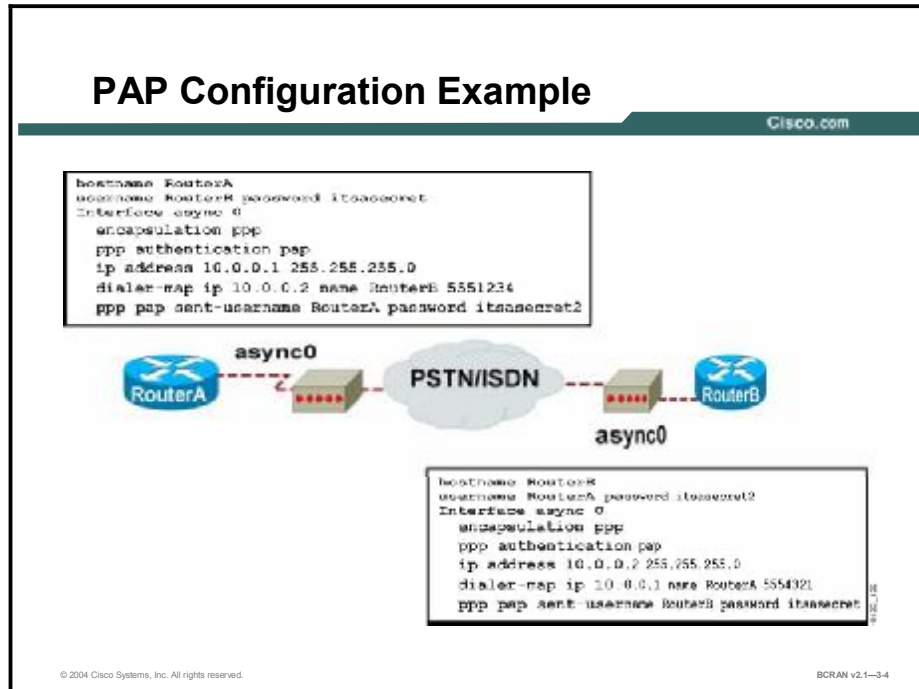
For more secure access control, use CHAP instead of PAP as the authentication method. You should use PAP only when you find that hosts running legacy software may not support CHAP. In this case, PAP is your only authentication option.

Always configure asynchronous lines to require authentication. PPP gives you the option of requiring that callers authenticate using one of two authentication protocols, PAP or CHAP. However, if you are using PPP over a point-to-point leased line, authentication is unnecessary and should not be configured.

Note Most Internet service providers (ISPs) use PAP and CHAP because of the relative management ease and the reduced number of support calls.

PAP Configuration Example

This topic describes how to configure PAP authentication on a Cisco router.



In the figure shown, two routers, RouterA and RouterB, are connected across a network.

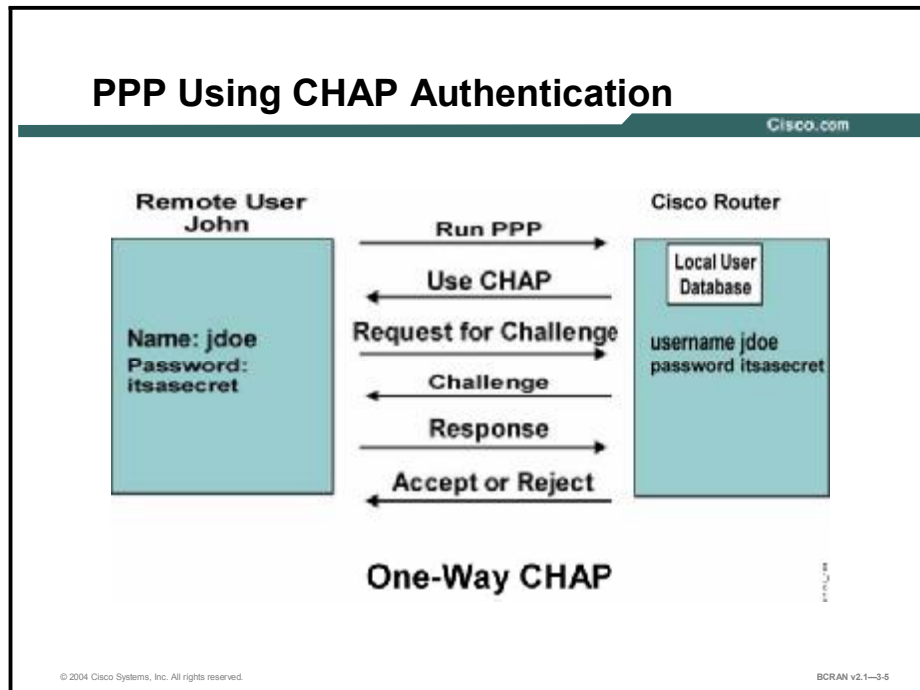
Perform the following steps to configure PAP authentication:

- Step 1** On each of the interfaces, specify **encapsulation ppp**.
- Step 2** Enable the use of PAP authentication with the **ppp authentication pap** command.
- Step 3** Configure the router with a local username and password database, using the global configuration command **username username password password**, or point it to a network host that has that information (such as a TACACS+ server). The username and password must match the username and password in the remote router **ppp pap sent-username** command.
- Step 4** Configure the router with the **ppp pap sent-username** command, which must match the **username username password password** statement on the remote host or router. Note that in the RouterA configuration, the **ppp pap sent-username** command is used to specify the username and password information to send in the event that it dials RouterB and is asked to authenticate. RouterB is also configured to send a username and password for PAP, if challenged. The name included with the username and dialer map commands is case sensitive. If the remote host name is RouterA and you create a username entry for rta instead, authentication will fail.
- Step 5** Configure IP addresses on the interfaces.
- Step 6** To ensure that both systems can communicate properly, configure the **dialer-map** command lines for each router. If each router is configured with a **dialer-map** command, each system will know what to do with authentication issues because the

systems will have prior knowledge of each other. The **dialer-map** command also contains the telephone number to dial to reach the specified router.

PPP Using CHAP Authentication

This topic describes the CHAP authentication process. CHAP authentication does not send passwords in plaintext.

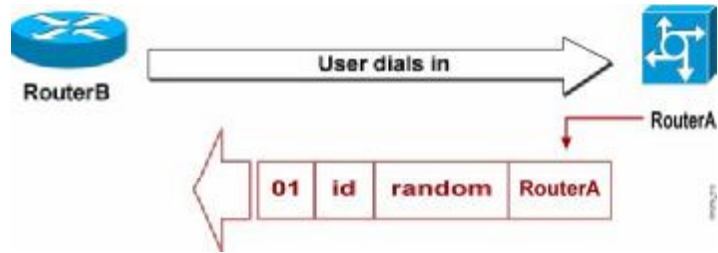


When using CHAP, the router sends a challenge message to the remote node after the PPP link is established. The remote node responds with a value calculated by using a one-way hash function, typically message digest algorithm 5 (MD5). The router checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is immediately terminated. Thus, the actual username and password are not sent over the media.

CHAP provides protection against a playback attack through the use of a variable challenge value that is unique and unpredictable. The use of repeated challenges every 2 minutes during any CHAP session is intended to limit the time of exposure to any single attack. The router (or authentication server, such as TACACS+) controls the frequency and timing of the challenges. A major advantage of the constantly changing challenge string is that the line cannot be sniffed and played back later to gain unauthorized access to the network.

CHAP in Action—Challenge

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

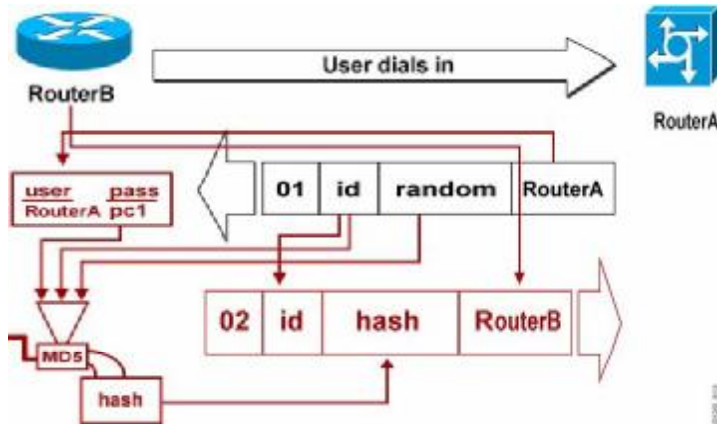
BCRAN v2.1—3.6

This figure illustrates the following steps in the CHAP authentication process between the two routers:

1. The call arrives on an interface configured for the **ppp authentication chap** command. Therefore, a CHAP challenge from RouterA to the calling router RouterB is required on this call.
2. A CHAP challenge packet is built with the following characteristics:
 - “01” = challenge packet type identifier
 - “id” = sequential number that identifies the challenge
 - “random” = a reasonably random number
 - “RouterA” = the authentication name of the challenger
3. The “id” and “random” values are kept on the access server.
4. The challenge packet is sent to the caller.
5. A list of outstanding challenges is maintained.

CHAP in Action—Response

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-3.7

This figure illustrates the receipt and MD5 processing of the challenge packet from the server.

The calling router processes the CHAP challenge packet in the following manner:

1. The “id” value and “random” value are fed into the MD5 hash generator.
2. The name “RouterA” is used to look up the password.
3. The password is fed into the MD5 hash generator.

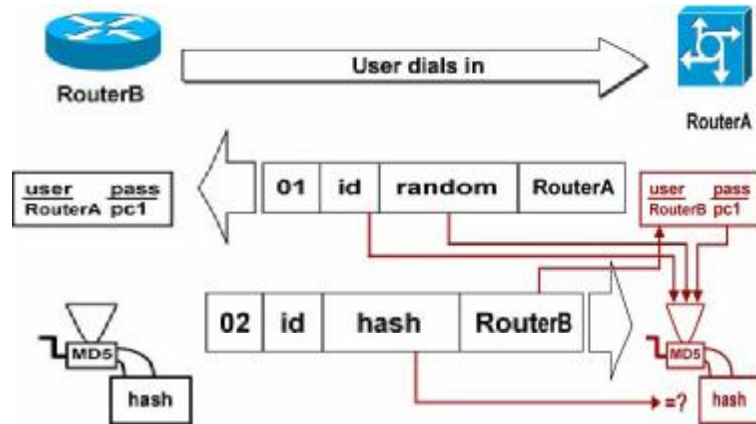
The one-way hash result is then used to form a response packet containing the following:

- “02” = CHAP response packet type identifier
- “id” = number copied from the challenge packet
- “hash” = the output from the MD5 hash generator (the hashed information from the challenge packet)
- “RouterB” = the authentication name of this caller

The result is a one-way MD5-hashed CHAP challenge that will be sent back in the CHAP response.

CHAP in Action—Verification

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—3.8

This figure shows the response packet processing that occurs on the challenger.

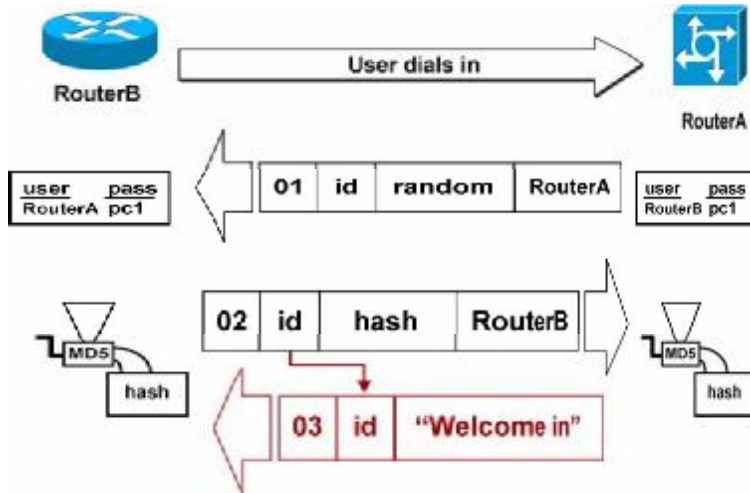
The CHAP response packet is processed in the following manner:

1. The “id” value is used to find the original challenge packet.
2. The “id” value is fed into the MD5 hash generator.
3. The original challenge “random” value is fed into the MD5 hash generator.
4. The name “RouterB” is used to look up the password (this name can be used to identify this session) from the local database, TACACS server, or RADIUS server.
5. The password is fed into the MD5 hash generator.
6. The hash value received in the response packet is then compared to the calculated MD5 hash value.

CHAP authentication succeeds if the calculated and the received hash values are equal.

CHAP in Action—Result

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-3-9

The figure illustrates the success message being sent to the calling router.

If authentication is successful, a CHAP success packet is built from the following components:

- "03" = CHAP success message type
- "id" = number copied from the response packet
- "Welcome in" is simply a text message of some kind, meant to be a user-readable explanation

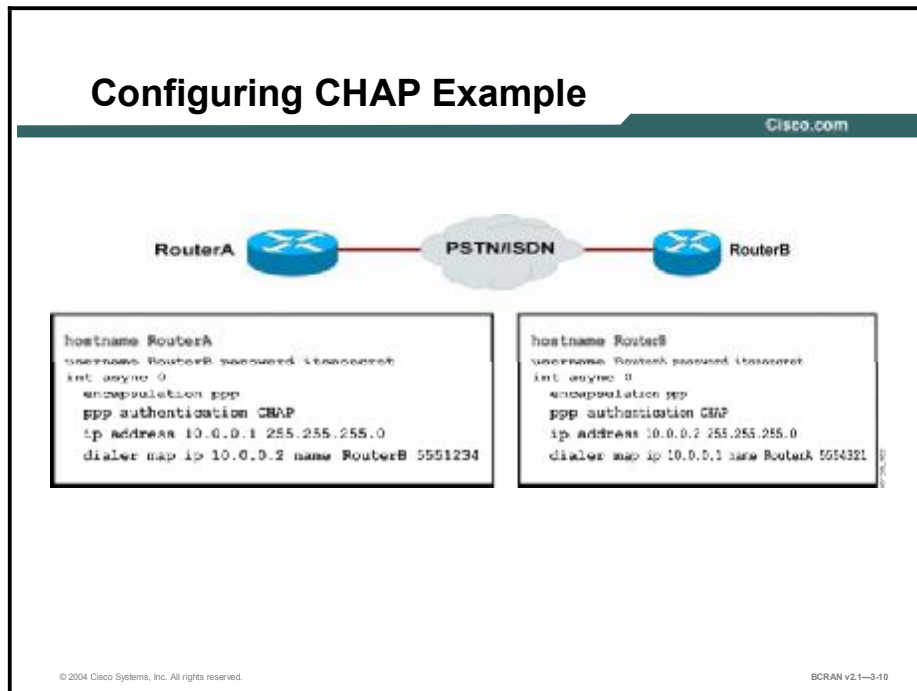
If authentication fails, a CHAP failure packet is built from the following components:

- "04" = CHAP failure message type
- "id" = number copied from the response packet
- "Authentication failure" or some such text message, meant to be a user-readable explanation

The success or failure packet is then sent to the caller.

CHAP Configuration Example

This topic describes how to configure CHAP authentication on a Cisco router.



Configuring CHAP is straightforward. As with the PAP example, RouterA and RouterB are connected across a network. Use the following steps as a guide to configuring CHAP authentication:

- Step 1** On each of the interfaces, specify the **encapsulation ppp** command.
- Step 2** Enable the use of CHAP authentication with the **ppp authentication chap** command.
- Step 3** You must also configure the usernames and passwords. Use the command **username username password password**, where **username** is the hostname of the peer.

The passwords must be identical at both ends.

The router name and password are case sensitive.

```
Router(config)# username username password password
```

- Step 4** Configure the router with a local username/password database, using the global configuration command **username username password password**, or point it to a network host that has that information (such as a TACACS+ server). By default, the router uses its hostname to identify itself to the peer. Therefore, the username must match the remote host hostname.

However, if you want the router to send a different username and password, you have the option of specifying this username and password with the commands:

```
Router(config-if)# ppp chap hostname name
```

```
Router(config-if)# ppp chap password password
```

- Step 5** Configure IP addresses on the interfaces.

CHAP and PAP Configuration Authentication

This topic describes how to configure both CHAP and PAP authentication on a Cisco router.

Configuring CHAP and PAP Authentication

Cisco.com

```
Router(config-if)# ppp authentication pap chap
```

- Enables both CHAP and PAP, and performs PAP authentication before CHAP

or

```
Router(config-if)# ppp authentication chap pap
```

- Enables both CHAP and PAP, and performs CHAP authentication before PAP

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—3-11

Both PAP and CHAP authentication can be configured on an interface. The first method specified is requested during link negotiation. If the peer suggests using the second method or simply refuses the first method, then the second method will be tried. This command can be useful because some remote devices support only CHAP and others only PAP.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **PAP authentication sends password in plaintext.**
- **CHAP authentication sends passwords in encrypted text.**
- **Both PAP and CHAP authentication can be configured on an interface.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-12

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) During the PPP authentication process, and after the system checks the authentication response sent back from the security server or local database, what happens if the response is positive?
- A) The user is rejected immediately.
 - B) Nothing occurs.
 - C) The PPP process is started.
 - D) The user is prompted for a credit card authorization code.
- Q2) Which authentication protocol would be used if you have decided to use an authentication protocol on your router?
- A) POP
 - B) CHAP
 - C) TFTP
 - D) ICMP
- Q3) Which command is used to enable the use of PAP authentication on a Cisco router?
- A) **pap authentication ppp**
 - B) **chap authentication ppp**
 - C) **ppp authentication chap**
 - D) **ppp authentication pap**
- Q4) Which Cisco router authentication protocol provides protection against a playback attack through the use of a variable challenge value that is unique and unpredictable?
- A) PAP
 - B) TFTP
 - C) CHAP
 - D) ICMP
- Q5) Which two information items in the local database are essential in configuring the CHAP authentication protocol?
- A) username and user password
 - B) username and user phone number
 - C) username and user birthday
 - D) username and user hire date

- Q6) Which of the following commands enables both PAP and CHAP authentication on an interface, but performs CHAP authentication before PAP authentication?
- A) `router(config-if)# ppp authentication pap chap`
 - B) `router(config-if)# pap authentication chap ppp`
 - C) `router(config-if)# ppp authentication chap pap`
 - D) `router(config-if)# chap authentication pap ppp`

Quiz Answer Key

- Q1) C
Relates to: PPP Authentication
- Q2) B
Relates to: PPP Using PAP Authentication
- Q3) D
Relates to: PAP Configuration Example
- Q4) C
Relates to: PPP Using CHAP Authentication
- Q5) A
Relates to: CHAP Configuration Example
- Q6) C
Relates to: CHAP and PAP Configuration Authentication

Configuring LCP Options: Callback and Compression

Overview

When you can create PPP connections, you may want to take advantage of other PPP LCP options. These options include PPP callback and several types of compression. This lesson explains how to configure a PPP callback server and a PPP callback client, and how to enable various types of compression.

Relevance

The callback feature can be useful to control access and toll costs between hosts because only the two authenticated hosts will participate in the WAN connection. Compression is valuable for maximizing limited capacity on a WAN link.

Objectives

Upon completing this lesson, you will be able to:

- Describe how to implement and configure PPP callback
- Configure a PPP callback server using Cisco IOS commands
- Configure a PPP callback client using Cisco IOS commands
- List and describe the various compression schemes supported by Cisco routers
- Configure compression using Cisco IOS commands
- Identify that compression is occurring use **show** commands

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

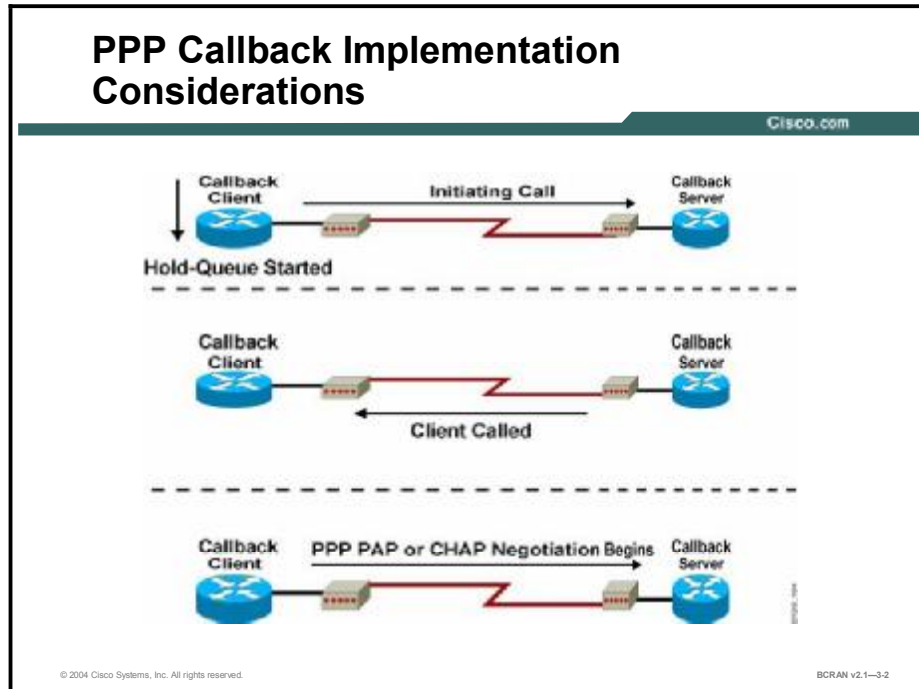
Outline

This lesson includes these topics:

- Overview
- PPP Callback Overview
- Asynchronous Callback Operation Flowchart
- PPP Callback Operation
- Asynchronous Callback Line and Interface Commands
- PPP Callback Client Configuration
- PPP Callback Server Configuration
- Compression and PPP
- Compression Configuration
- Compression Verification
- Summary
- Quiz

PPP Callback Overview

This topic describes the PPP callback configuration.



PPP callback is an LCP option used over dialup links. PPP callback provides a client/server relationship between the endpoints of a point-to-point connection. PPP callback allows a dialup client to request that a dialup server call back. The callback feature can be used to control access and toll costs between hosts.

When PPP callback is configured on two routers, the calling router (the callback client) passes authentication information to the remote router (the callback server), which uses the host name and dial string authentication information to determine whether or not to place a return call. If the authentication is successful, the callback server disconnects, and then places a return call. The remote username of the return call is used to associate it with the initial call so that the packets can be transmitted.

Both routers on a point-to-point link must be configured for PPP callback. One router must function as a callback client; the other router must be configured as a callback server. The callback client must be configured to initiate PPP callback requests. The callback server must be configured to accept PPP callback requests and place return calls.

When the client router dials the initial call, the router hold-queue timer is started. Calls to this destination will not be made again until the hold-queue timer expires. The timer is stopped if PPP LCP negotiation is successful or if the call fails.

Note the following regarding rotary groups including ISDN:

- If the enable time is too long and another user dials into the last interface before the enable timer expires, the return call will never be made.
- If an interesting packet arrives at the server during the enable time, the dialer may use the last interface for the interesting packet and the return call will never be made.

When planning to implement PPP callback, consider the following:

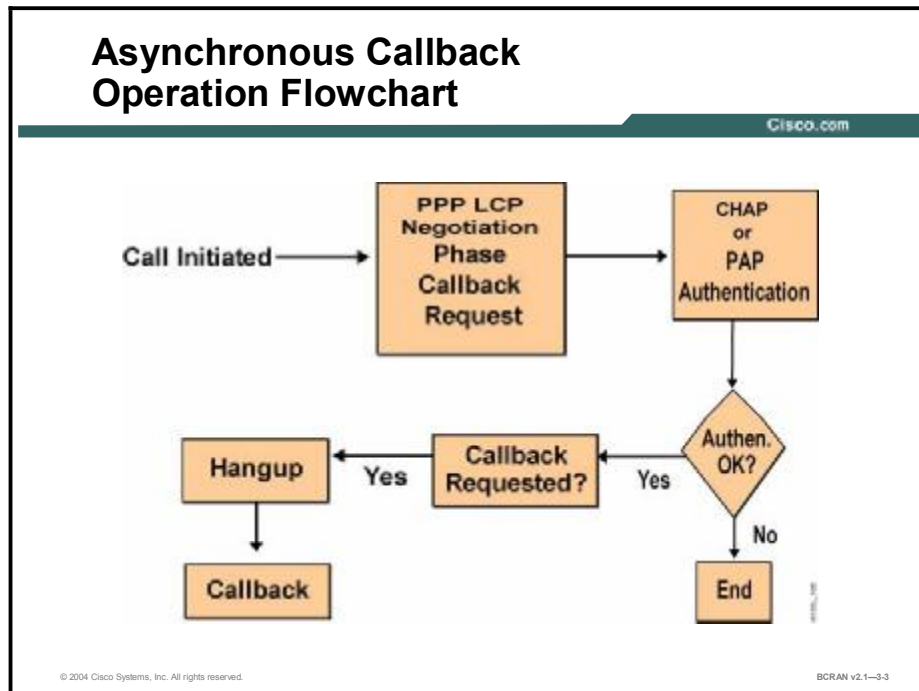
- Authentication is required for callback to be successful.
- The **dialer enable-timeout** command specifies the time in seconds that the Cisco IOS software waits before the next call can occur on the specific interface. This value must be greater than the serial pulse interval for the interface that is set using the **pulse-time** command. Acceptable values are positive, nonzero integers.
- The **dialer hold-queue timeout** command determines how long to wait before the client can make another call to the same destination. The server must make the return call before the client hold-queue timer expires to prevent the client from trying again and possibly preventing the return call from being connected.

The hold timer on the callback client should be approximately four times longer than the server hold-queue timer.

Note The **dialer redial** command could also be used to customize the number of redial attempts and the interval between redial attempts.

Asynchronous Callback Operation Flowchart

This topic describes the general steps that occur during a typical PPP callback exchange.



The asynchronous callback feature supports EXEC, PPP, and ARA Protocol sessions. The main motivation for callback is telephone bill consolidation and dialup cost savings. Although asynchronous callback is not positioned as a security feature, it enforces security by making callbacks only to telephone numbers assigned in the authentication database. The incoming calls go through the normal login process and must pass authentication before callback can occur.

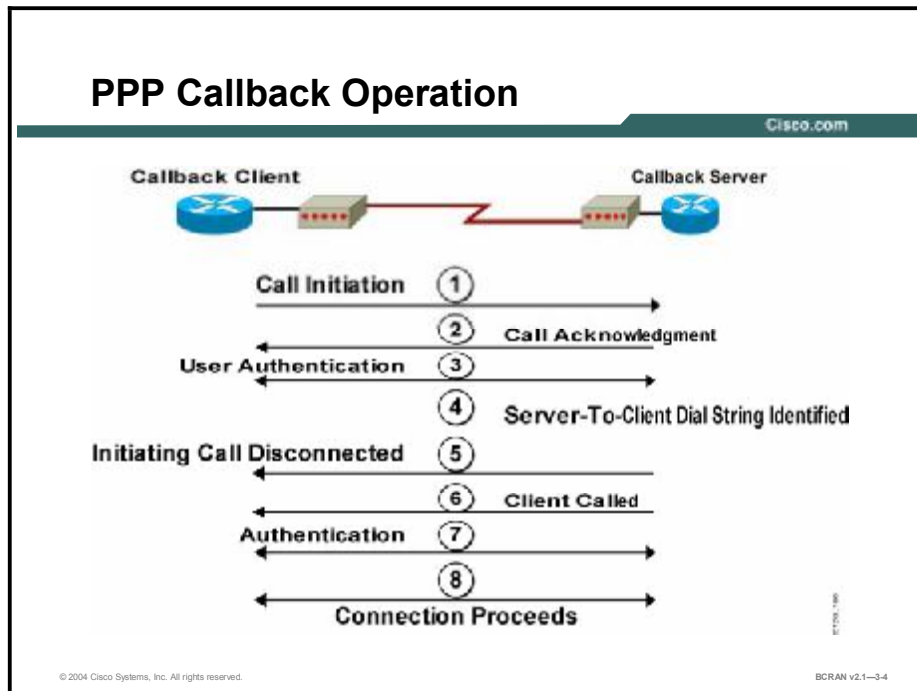
The callback feature employs a two-pass process:

- On the first pass the callback engine determines which target line to use for callback to the remote user and then hangs up on the incoming line. Then the callback engine dials back to the remote user through the target line using the dial string provided.
- On the second pass the callback engine proceeds normally as if there is no callback.

Note To make callback work properly, you must make sure that callback is configured for each autoselect protocol (PPP, SLIP, or ARA Protocol) that is defined for any given remote user. Otherwise, the remote dial-in autoselect process may work, but no callback will occur.

PPP Callback Operation

This topic describes the steps that occur during a typical PPP callback exchange.



PPP callback operation consists of the following steps:

- Step 1** The callback client initiates the call. The client requests callback using the callback option during the PPP LCP negotiation phase.
- Step 2** The callback server acknowledges the callback request and checks its configuration to verify that callback is enabled.
- Step 3** The callback client and server authenticate using either CHAP or PAP authentication. The username identifies the dial string for the return call.
- Step 4** After successful initial authentication, the callback server router identifies the callback dial string. The callback server compares the username of the authentication to the host name in a dialer map table. The dial string can be identified by a mapping table or by the Callback Option Message field during PPP LCP negotiations. The Callback Option Message field is defined in RFC 1570.
 - If the commands **dialer callback-secure**, **ppp callback accept**, and **ppp authenticate pap** or **ppp authenticate chap** are enabled on an interface, all calls answered on that interface are disconnected after authentication, and the callback server proceeds with Steps 5 through 8.
 - If the **dialer callback-secure** command is not enabled, the callback server will maintain the initial call if the authenticated username is not configured for callback.
- Step 5** The callback server rejects the initiating call. Therefore, there is no cost to the calling party.

- Step 6** The callback server uses the dial string to initiate the callback. If the return call fails, no additional calls are attempted. Callback is not negotiated on the return call.
- Step 7** If the return call succeeds, authentication occurs.
- Step 8** The connection is established, and data is exchanged.

Asynchronous Callback Line and Interface Commands

This topic describes the commands that are used for enabling asynchronous PPP callback on the callback server.

Asynchronous Callback Line/Interface Commands

Cisco.com

```
Router(config-if)# ppp callback accept
```

```
Router(config-if)# ppp callback initiate
```

```
Router(config)# line line-number
Router(config-line)# callback forced-wait seconds
Router(config-line)# script callback script-name
```

- On the callback server

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-5

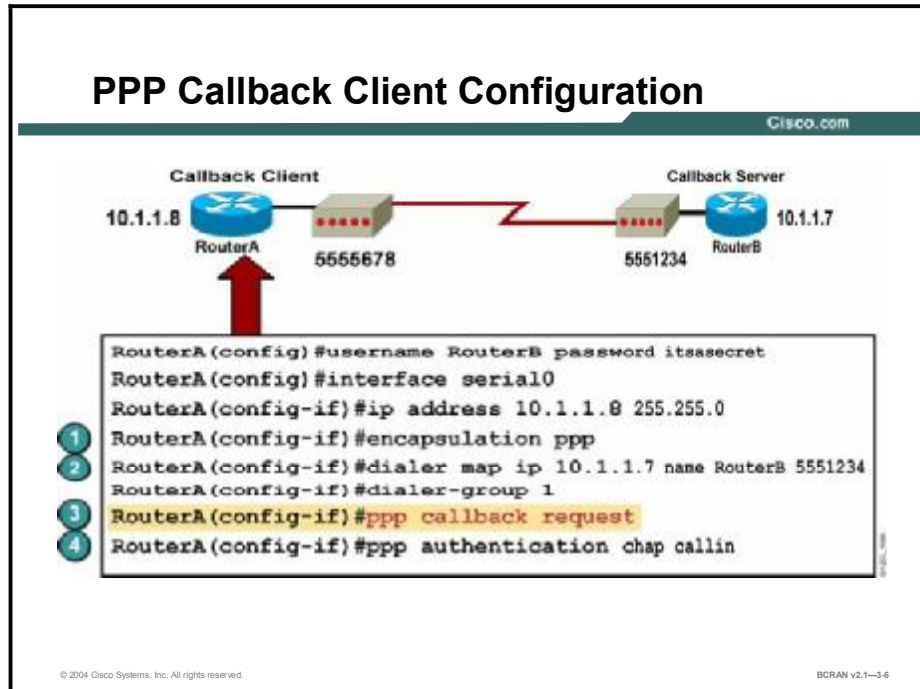
The asynchronous line configurations or asynchronous interface commands for PPP callback are shown in the table.

PPP Callback Commands

Command	Description
ppp callback accept	This interface command allows the specified interface to accept a callback request initiated from a remote node (per RFC 1570).
ppp callback initiate	This interface command allows the router to initiate a callback to a remote node when the remote node is capable of putting itself in an answer mode for callback.
callback forced-wait seconds	This line command allows an additional wait (in seconds) before the callback chat script is applied to the outgoing target line. This option accommodates modems that require a longer “resting” period before any input can be accepted again.
script callback script-name	This line command specifies a chat script to issue AT commands to the modem during a callback attempt made to the target asynchronous line. This command is used for EXEC and PPP callbacks.

PPP Callback Client Configuration

This topic describes the commands that enable PPP callback on the callback client.



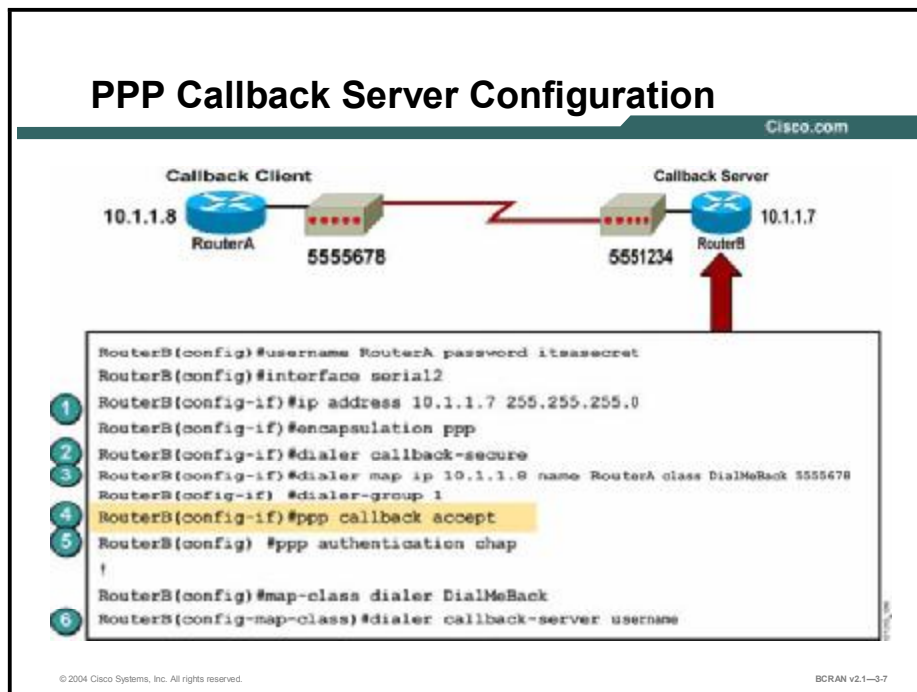
To configure client PPP callback so that all calls over this interface will request callback, perform the following tasks:

- Step 1** Configure PPP on the serial or ISDN interface.
- Step 2** Set up a dialer map with the **dialer map ip** and **dialer-group** commands. Be sure that the **dialer map** command has a **name** field with the correct name of the server. In this example, the server is named RouterB.
- Step 3** Configure the router interface as the callback client using the **ppp callback request** command.
- Step 4** Set the authentication to CHAP using the **ppp authentication chap** command.

Note You can use the optional **dialer hold-queue timeout** or **dialer redial** commands to specify the number of seconds that the callback client waits for a return call from the callback server.

PPP Callback Server Configuration

This topic describes the commands that are used to configure PPP callback on the callback server.



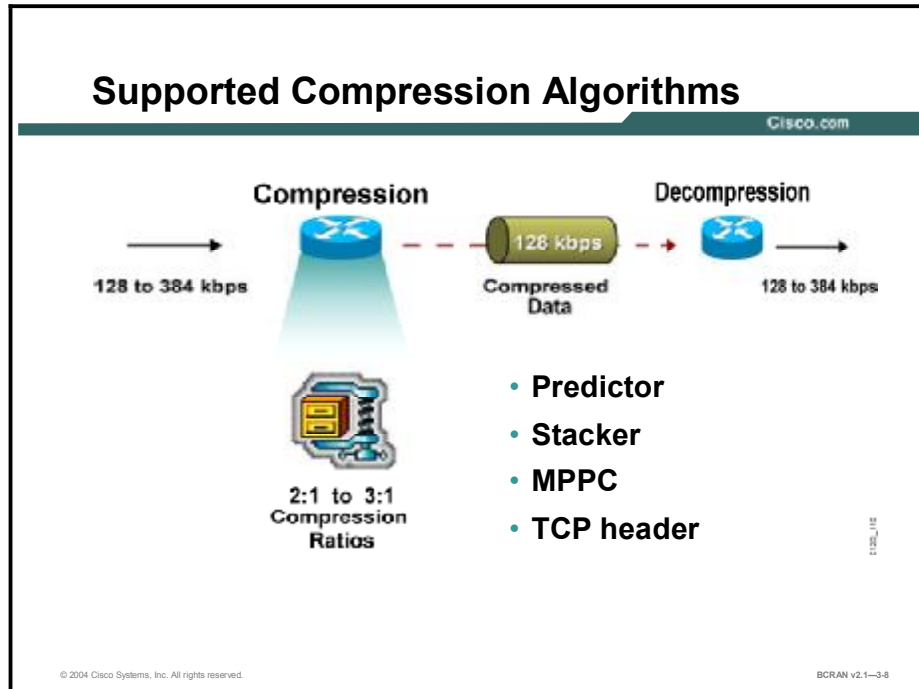
To configure PPP callback for a server, perform the following steps:

- Step 1** Configure IP on the dial-in line.
- Step 2** Use the **dialer callback-secure** command to disconnect calls that are not properly configured for callback. If the username specified in the **dialer map** command is not authorized for callback, the call will be disconnected. If the **dialer callback-secure** command is not configured, it will allow both callback and noncallback clients.
- Step 3** Configure the dialer map including a map class “DialMeBack” to establish PPP callback.
- Step 4** Use the **ppp callback accept** command to enable callback.
- Step 5** Define the PPP authentication method with the **ppp authentication chap** command.
- Step 6** Configure the **dialer callback-server username** command in a dialer map class to identify the name used in the dialer map as a valid callback client.

When the callback client router dials in and is authenticated, the call will be disconnected. For example, in the figure, a return call will be made to 555-5678 as configured by the **dialer map** command. The **dialer map** command identifies the map class to be used for this connection.

Compression and PPP

This topic describes the various compression schemes that are available on Cisco routers.



Cisco routers can also maximize performance using data compression, enabling higher data throughput across the link, especially for low-speed links.

Cisco compression schemes are as follows:

- **Predictor:** Determines if the data is already compressed. If the data is compressed, the data is sent. No time is wasted trying to compress data that is already compressed.
- **Stacker:** A Lempel-Ziv (LZ)-based compression algorithm looks at the data and sends each data type only once. The data type includes information about where the type occurs within the data stream. The receiving side uses this information to reassemble the data stream.
- **MPPC:** MPPC Protocol (RFC 2118) allows Cisco routers to exchange compressed data with Microsoft clients. MPPC uses an LZ-based compression algorithm.
- **TCP header compression:** This type of compression, also known as Van Jacobson compression, is used to compress only the TCP headers.

Compression is an option that is negotiated by LCP. Therefore, if the remote party that is being called is not configured for compression, no compression will take place.

The highest compression ratio is usually reached with highly compressible text files. Compressed files such as Joint Photographic Experts Group (JPEG) graphics or Motion Picture Experts Group (MPEG) files, or files that were compressed with software such as PKZIP or StuffIt, will be compressed only 1:1 or less.

If you frequently transfer already-compressed data, such as graphics and video, you must consider global compression. Trying to further compress already-compressed data can take longer than transferring the data without any compression at all. Ideally, you can attain 2:1 or 3:1 compression for information that has not already been compressed. Expect an average of 1.6:1 compression for mixed compressed and uncompressed source data.

Typically, you should configure compression only on low-speed links because the router compresses data using software, which requires router CPU time and memory. Some algorithms are more memory intensive, while others are more CPU intensive. For example:

- More CPU intensive: Stacker, MPPC
- More memory intensive: Predictor

Memory-intensive algorithms require an extra memory allowance. CPU-intensive algorithms require more CPU cycles. In either case, the ability of the router to route packets is impaired by the drain on its resources.

You should take memory and CPU usage into consideration when you are implementing compression on a specific router. Some routers with slow CPUs or inadequate memory can be overloaded when configured to compress traffic. If you are using a Cisco 2500 Series or faster processor router, either of these methods should be acceptable if you have sufficient memory in the router. Use caution with smaller systems that have less memory and slower CPUs, and ensure that you are not overloading the router.

Cisco recommends that you disable compression if the CPU load exceeds 65 percent. To display the CPU load, use the **show process cpu** command.

Predictor compression is recommended when a bottleneck is caused by a high load on the router. Stacker compression is recommended when the bottleneck is caused by bandwidth limitations on a line.

Compression Configuration

This topic discusses the commands that enable compression on a Cisco router.

Compression Configuration

Cisco.com

```
Router(config)# int serial2
Router(config-if)# compress {predictor | stac | mppc}
```

Interface Compression Algorithms

```
Router(config)# int async 2
Router(config-int)# ip tcp header-compression
```

```
Router(config)# int async 2
Router(config-int)# ip tcp header-compression passive
```

- TCP Header

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-3-9

Configuring for compression is simple. From the interface, issue the **compress predictor**, **compress stac**, **compress mppc**, or **ip tcp header-compression** command on both sides of the link.

TCP header compression is an option negotiated by LCP. The TCP header compression technique is described in RFC 1144.

TCP header compression is supported on serial lines that use HDLC, PPP, or SLIP encapsulation. You must enable TCP header compression on both ends of the connections for it to work. Only TCP headers are compressed. User Datagram Protocol (UDP) headers are not affected. Header compression is useful on networks with a large percentage of small packets, such as those supporting many Telnet connections.

Configure TCP header compression by using the **ip tcp header-compression** command. The optional **ip tcp header-compression passive** command specifies that TCP header compression is not required but will be used if the router receives compressed headers from its link partner.

Note Cisco IOS software includes the PPP commands **ppp compression predictor** and **ppp compression stacker**. Using these commands has exactly the same effect as using the **compress predictor** and **compress stac** commands, respectively. For example, if you enter the **ppp compression stacker** command, it will appear as **compress stac** in the configuration file.

Compression Verification

This topic describes the commands that are used to verify compression activity.

Using the show compress Command

Cisco.com

```
Router1# show compress
Serial2
uncompressed bytes xmt/rcv 81951/85500
 1 min avg ratio xmt/rcv 0.789/0.837
 5 min avg ratio xmt/rcv 0.789/0.837
10 min avg ratio xmt/rcv 0.789/0.837
no bufs xmt 0 no bufs rcv 0
restarts 0

Additional Stacker Stats:
Transmit bytes: Uncompressed = 28049 Compressed = 65745
Received bytes: Compressed = 74738 Uncompressed =0
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1--3-10

Verify compression by using the **show compress** command in privileged EXEC mode to view compression statistics. This example shows report statistics for an interface that is configured with Stacker compression. The report includes the number of compressed bytes that are received and transmitted by the interface.

Uncompressed Bytes

This line provides an uncompressed byte count of compressed data. It does not include packets that cannot be compressed.

```
uncompressed bytes xmt/rcv 81951/85500
```

Throughput Ratio

The next section of output is a ratio of the data throughput gained or lost in the compression routine. Any number less than one (1) indicates that the compression is actually slowing down the data throughput. It does not reflect the data compressibility.

```
 1 min avg ratio xmt/rcv 0.789/0.837
 5 min avg ratio xmt/rcv 0.789/0.837
10 min avg ratio xmt/rcv 0.789/0.837
```

Buffer Allocation

This line indicates the number of times the compression routine was not able to allocate a buffer to compress or decompress a packet:

```
no bufs xmt 0 no bufs rcv 0
```

Bytes Transmitted

The uncompressed value is the amount of data that could not be compressed and that the router sent in an uncompressed format. The compressed value is the byte count of the data after compression. The sum of these two values represents the actual number of bytes that are transmitted on the interface, minus the Layer 2 encapsulation overhead.

```
Transmit bytes: Uncompressed = 28049 Compressed= 65745
```

Bytes Received

The compressed value is the byte count of the compressed data received. The uncompressed value is the amount of data received in uncompressed format. The sum of these two values represents the actual byte count received on the interface, minus the Layer 2 encapsulation overhead.

```
Received bytes: Compressed = 74738 Uncompressed= 0
```

Interpreting the *show compress* Command Output

From this output, the following calculations can be made:

- Total amount of data to be transmitted before applying the compression routine: $81,951 + 28,049 = 110,000$
- Total amount of data to be transmitted after compression: $28,049 + 65,745 = 93,794$
- Overall data compression: $110,000 / 93,794 = 1.17$
- Compression ratio of the compressed packets: $81,951 / 28,049 = 2.92$

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The callback feature can be used to control access and toll costs between hosts.**
- **PPP callback is an LCP option used over dialup links.**
- **The asynchronous callback feature supports EXEC and PPP.**
- **Cisco routers can also maximize performance using data compression, which enables higher data throughput across the link.**
- **To verify compression, use the show compress command in privileged EXEC mode.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-11

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which LCP option feature does a Cisco router use over dialup links?
- A) PAP callback
 - B) NCP callback
 - C) PPP callback
 - D) LCP callback
- Q2) Which of the following session types is supported by the asynchronous callback feature?
- A) EXEC, PPP, and ARA Protocol
 - B) TTT, IPC, and OPX
 - C) ASC, CB, and FS
 - D) AUX, CON, and TTP
- Q3) Which party initiates the call in the PPP callback process?
- A) callback server
 - B) callback client
 - C) caller ID
 - D) three-way calling service
- Q4) Which interface command allows the router to initiate a callback to a remote node when the remote node is capable of putting itself in an answer mode for callback?
- A) **callback forced-wait seconds**
 - B) **ppp callback initiate**
 - C) **ppp callback accept**
 - D) **script callback script-name**
- Q5) Which command configures the router interface as the PPP callback client?
- A) **ppp authentication pap**
 - B) **ppp dialer map id**
 - C) **ppp callback request**
 - D) **ppp authentication chap**

- Q6) Which command is used to disconnect calls that are not properly configured for PPP callback?
- A) **dialer map**
 - B) **dialer callback-secure**
 - C) **dialer group**
 - D) **dialer hold**
- Q7) Which of the Cisco compression algorithms determines whether the data is already compressed before sending the compressed data?
- A) MPPC
 - B) Predictor
 - C) Stacker
 - D) TCP header compression
- Q8) When TCP header compression is enabled on both sides of the router, which headers are compressed?
- A) UDP headers
 - B) TCP headers
 - C) PPC headers
 - D) STA headers
- Q9) Which command is used in privileged EXEC mode to view compression statistics to verify compression?
- A) **show stacker**
 - B) **show predictor**
 - C) **show MPPC**
 - D) **show compress**

Quiz Answer Key

- Q1) C
Relates to: PPP Callback Overview
- Q2) A
Relates to: Asynchronous Callback Operation Flowchart
- Q3) B
Relates to: PPP Callback Operation
- Q4) B
Relates to: Asynchronous Callback Line and Interface Commands
- Q5) C
Relates to: PPP Callback Client Configuration
- Q6) B
Relates to: PPP Callback Server Configuration
- Q7) B
Relates to: Compression and PPP
- Q8) B
Relates to: Compression Configuration
- Q9) D
Relates to: Compression Verification

Configuring LCP Options: Multilink PPP

Overview

Multilink PPP (MLP) allows two or more connections to be bundled into a single virtual connection. These bundles can be established through both circuit-switched and leased-line topologies. This topic describes the use and operation of MLP.

Relevance

You should know how to configure MLP for situations when additional bandwidth is desired, such as during periods of high utilization.

Objectives

Upon completing this lesson, you will be able to:

- Describe MLP operation and concepts
- Configure MLP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

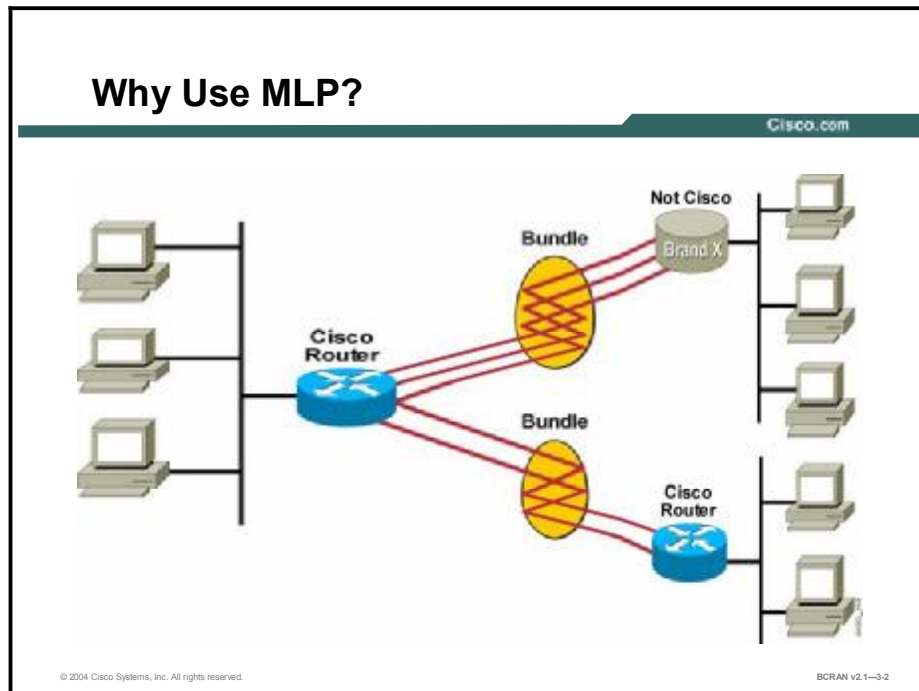
Outline

This lesson includes these topics:

- Overview
- Multilink PPP Overview
- Multilink PPP Operation and Configuration
- Multilink PPP Example
- Summary
- Quiz

Multilink PPP Overview

This topic describes MLP over parallel circuits.



MLP is an LCP option that permits a system to signal that it is capable of combining multiple links into a bundle. MLP can improve throughput and reduce latency between systems by splitting Layer 3 packets and sending the fragments over parallel circuits. It is important to remember that MLP works by splitting packets into fragments, not by load-balancing complete packets to a destination.

Prior to the adoption of MLP (described first in RFC 1717), there was no standardized way to use both of the ISDN B channels of a BRI and also ensure proper sequencing. MLP is interoperable between Cisco routers running Cisco IOS software and most routers that comply with the most recent MLP standard, RFC 1990.

Typically, you should use MLP with applications, in which bandwidth requirements are dynamic, such as remote LAN access applications for SOHO environments. When user traffic exceeds a predefined threshold, an additional physical link (such as a B channel) can be brought up to handle the burst of traffic.

MLP solves several problems related to load balancing across multiple WAN links, including the following:

- Multivendor interoperability, as specified by RFC 1990, which replaces RFC 1717
- Packet fragmentation, improving the latency of each packet (supports RFC 1990 fragmentation and packet-sequencing specifications)
- Packet-sequence and load calculation


This feature negotiates the Maximum Receive Reconstructed Unit (MRRU) option during the PPP LCP negotiation to indicate to its peer that it can combine multiple physical links into a bundle.

Multilink PPP Operation and Configuration

This topic demonstrates how to configure an MLP connection on two parallel circuits.

MLP Operation and Configuration

Cisco.com



```
Router(config-if)#ppp multilink
```

- Enables MLP on an interface

```
Router(config-if)#dialer load-threshold load  
[outbound | inbound | either]
```

- Defines the threshold to bring up another link

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3.3

The **ppp multilink** interface configuration command enables MLP on an interface. The interface must use PPP encapsulation. The maximum number of links in a bundle is the number of interfaces in the dialer or ISDN interface. To limit the number of links in a multilink bundle, include the **ppp multilink links maximum** *links* command on the MLP interface.

The **dialer load-threshold** command enables a dialer rotary group to bring up links and add the links to a multilink bundle. The load threshold is expressed as a ratio of $x/255$, with a value of 128, meaning 50 percent bandwidth utilization. This command allows threshold determination for the following:

- Outbound traffic only (default)
- Inbound traffic only
- The maximum of either inbound or outbound traffic

It is necessary to configure only one end of a link for load threshold.

To ensure proper load calculation, be sure to set the correct interface bandwidth using the **bandwidth** command.

Note Standard dial-on-demand routing (DDR) configuration should be in place before you configure MLP.

Multilink PPP Example

This topic discusses the steps that are necessary in configuring an MLP connection.

MLP Example

Cisco.com

```
RouterA(config)#interface BRI0
RouterA(config-if)#ip address 192.168.12.3.255.255.255.240
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# dialer map ip 192.168.12.1 name ROUTER1 5554321
RouterA(config-if)# dialer-group 1
RouterA(config-if)# ppp authentication chap
RouterA(config-if)#ppp multilink
RouterA(config-if)#dialer load-threshold 1 either
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3-4

Only two commands must be added to this interface configuration to make MLP possible. The router at the other end of the call must be similarly configured. These two commands are:

- The **ppp multilink** command
- The **dialer load-threshold *load* [outbound | inbound | either]** command

The **ppp multilink** command activates the interface for MLP operation and allows negotiation of the protocol at connect time, thus establishing a single-channel MLP bundle. However, this command is not sufficient to take advantage of the fragmentation, load-balancing, or bandwidth-on-demand features of the protocol.

The **dialer load-threshold *load*** command sets the point at which additional B channels will be added to the MLP bundle. When the total load of all up B channels is greater than the load threshold, the dialer interface (in this case, the BRI or PRI) adds an extra channel to the multilink bundle. In a similar way, if the total load for all the up B channels, minus one ($n - 1$) is at or below the threshold, channels will be taken down.

The **load** argument is the average load for the interface. It is a value from 1 (unloaded) to 255 (fully loaded).

The **outbound** argument sets the load calculation to be made on outbound traffic only. The **inbound** argument sets the load calculation to be made on inbound traffic only. The **either** argument sets the load as the larger of the outbound and inbound loads.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **MLP allows several connections to be bundled into a single virtual connection.**
- **MLP is controlled by adding a 2- or 4-byte sequencing header in the PPP frame that indicates sequencing for the fragments.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3-5

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Why use MLP?
- A) MLP can improve throughput and reduce latency between systems by splitting Layer 3 packets and sending the fragments over parallel circuits.
 - B) MLP can reduce throughput and improve latency between systems by splitting Layer 3 packets and sending the fragments over parallel circuits.
 - C) MLP can improve throughput and increase latency between systems by splitting Layer 3 packets and sending the fragments over parallel circuits.
 - D) MLP can reduce throughput and reduce latency between systems by splitting Layer 3 packets and sending the fragments over parallel circuits.
- Q2) Which command enables a dialer rotary group to bring up additional links to form a multilink bundle?
- A) **ppp multilink**
 - B) **dialer threshold**
 - C) **dialer load-threshold**
 - D) **bandwidth**
- Q3) Two commands must be added to the interface configuration to make MLP possible. The router at the other end of the call must be similarly configured. What are these two commands?
- A) **ppp multilink** and **dialer group**
 - B) **ppp multilink** and **dialer load-threshold load [outbound | inbound | either]**
 - C) **ppp multilink** and **dialer map**
 - D) **ppp multilink** and **dialer encapsulation**

Quiz Answer Key

Q1) A

Relates to: Multilink PPP Overview

Q2) C

Relates to: Multilink PPP Operation and Configuration

Q3) B

Relates to: Multilink PPP Example

Verifying and Debugging PPP

Overview

After you have configured PPP, you may need to troubleshoot an incorrect configuration for intended data travel on the PPP link. This topic describes how to verify and debug a PPP connection.

Relevance

Verification and debugging commands help troubleshoot nonworking PPP connections.

Objectives

Upon completing this lesson, you will be able to:

- Verify proper PPP configurations using **show** commands
- Verify proper dialer configurations using **show** commands
- Identify the anomalies in PPP configurations using **debug** commands

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- PPP Verification
- **show dialer** Command Example
- PPP Debugging
- Multilink Verification
- Summary
- Quiz

PPP Verification

This topic identifies the commands that verify PPP and link control protocol (LCP) options on a Cisco router.

show interface Command Example

Cisco.com

```
Router#show interface bri0 1
BR10: S-Channel 1 is up, line protocol is up
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive not set
lcp      = OPEN      multilink = OPEN
ipcp     = OPEN
Last input 0:05:51, output 0:05:52, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops) ; Total output drops: 0
Output queue: 0/64/0 (size/threshold/drops)
Conversations 0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
15 packets input, 804 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
14 packets output, 806 bytes, 0 underruns
0 output errors, 0 collisions, 19 interface resets, 0 restarts
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3-2

The **show interface** command is the best way to verify that a PPP connection has been established. Command output indicates this by showing the status IP in IPCP as OPEN.

The **show interface bri** command also displays multilink status. The multilink field for the individual B channel shows the LCP multilink status as OPEN if the multilink is active. If it is enabled, but not active, the status is CLOSED.

show dialer Command Example

This topic demonstrates the **show dialer** command to verify proper PPP operation.

show dialer Command Example

Cisco.com

```
router# show dialer
BRIO/0 - dialer type = ISDN

Dial String    Successes    Failures    Last DNIS    Last status
5551235        0            0           never        -
5551234        21           0           00:00:31    successful
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRIO/0:1 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is multilink member
Dial reason: ip (s=192.168.1.2, d=192.168.0.1)
Connected to 5551234 (SanJose1)

BRIO/0:2 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is multilink member
Dial reason: Multilink bundle overload
Connected to 551234 (SanJose1)
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-3.3

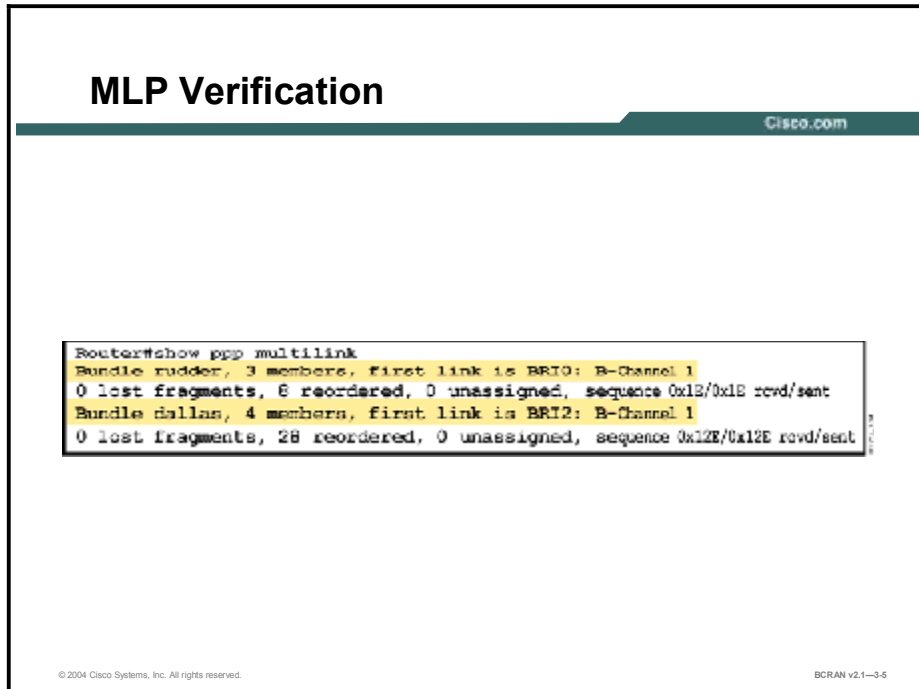
Use the **show dialer**, or the **show user**, and **show line** commands to determine if PAP or CHAP authentication was passed. The **show dialer** command can be used for ISDN connections.

If **show dialer** displays the name of the remote router, PAP or CHAP authentication has passed. You can check the **show dialer** command output on both routers to verify that the name of the other router is displayed. If it is, then you know that PAP or CHAP authentication worked. The **show dialer** command output will also indicate if a line is a member of an MLP bundle.

Use the **show user** command to view the progress of asynchronous dialup connections. Authentication has passed if a name is displayed with the line number in the **show user** output. Use the line number in a **show line** command for details about the asynchronous connection.

Multilink Verification

This topic identifies the command to verify MLP.



The screenshot shows a document titled "MLP Verification" with the Cisco.com logo in the top right corner. The main content is a terminal window displaying the output of the command "Router#show ppp multilink". The output lists two bundles: "Bundle rudder" with 3 members and "Bundle dallas" with 4 members. Each bundle entry includes statistics on lost fragments, reordered fragments, unassigned fragments, and sequence numbers. The document footer contains the copyright notice "© 2004 Cisco Systems, Inc. All rights reserved." and the identifier "BCRAN v2.1-3.6".

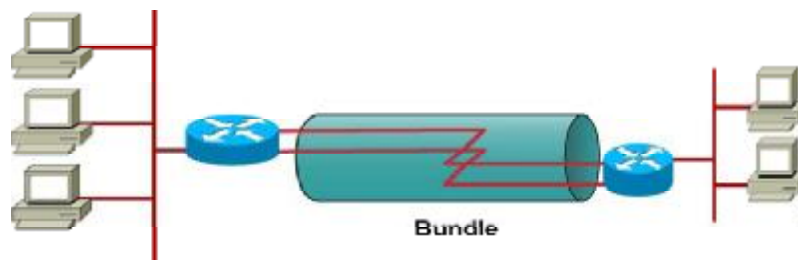
```
Router#show ppp multilink
Bundle rudder, 3 members, first link is BR10: B-Channel 1
0 lost fragments, 6 reordered, 0 unassigned, sequence 0x1B/0x1E rcvd/sent
Bundle dallas, 4 members, first link is BR12: B-Channel 1
0 lost fragments, 28 reordered, 0 unassigned, sequence 0x12E/0x12E rcvd/sent
```

The **show ppp multilink** command displays bundle information on a rotary group in the packet multiplexing section, including the number of members in a bundle and the bundle to which a link belongs.

The figure displays an example output when two active bundles are on a system.

MLP Troubleshooting

Cisco.com



- CHAP/PAP/caller ID on answering router?
- Dialer load threshold on one router?

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-3-6

Use the following problems and solutions to troubleshoot your MLP configuration:

- **Problem 1:** MLP is open, but no data is passing through.
Solution: Check dialer map statements and verify that routing is on.
- **Problem 2:** The last link of a bundle dials but never connects.
Solution: Check **debug isdn q931**, **debug modem**, or **debug chat** command output for asynchronous application operation. You can also use the **debug ppp multilink events** command for help. MLP might not be enabled.
- **Problem 3:** Data throughput is low.
Solution: Verify that fair queuing is not enabled.

The **debug ppp multilink** command displays packet sequence numbers. The command is useful only as a last resort because it will not help troubleshoot *why* connections are not being bundled.

The **debug ppp negotiation** command displays the Maximum Receive Reconstructed Unit (MRRU) option negotiation.

The **debug ppp authentication** command is useful for displaying the steps in the PPP authentication process.

The **debug isdn events** command also displays information useful for monitoring and troubleshooting MLP.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The show interface command is the best way to verify that PPP connection has been established.**
- **The show dialer command is the easiest way to determine if PAP or CHAP authentication was passed.**
- **The debug ppp negotiation command is an excellent tool for troubleshooting the PPP LCP activities.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—3.7

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 3-1: Configuring and Verifying PPP Operations

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which command is the best way to verify that PPP connection has been established?
- A) **show interface**
 - A) **show dialer**
 - B) **show stacker**
 - C) **show predictor**
- Q2) Which command is the easiest way to determine if the PAP or CHAP authentication was passed?
- A) **show dialer**
 - B) **show interface**
 - C) **show pap**
 - D) **show authentication**
- Q3) Which command is an excellent tool for troubleshooting the PPP LCP activities, such as authentication compression and MLP?
- A) **debug ppp negotiation**
 - B) **debug ppp negotiation tcp**
 - C) **debug remote negotiation**
 - D) **debug the negotiation**

Quiz Answer Key

Q1) A

Relates to: PPP Verification

Q2) A

Relates to: **show dialer** Command Example

Q3) A

Relates to: PPP Debugging

Module 4

Accessing Broadband

Overview

This module reviews the use of broadband for remote access to a central site using Network Address Translation (NAT). The four types of broadband covered are digital subscriber line (DSL), cable technology, wireless, and satellite links.

Objectives

Upon completing this module, you will be able to:

- Describe various broadband options
- Configure NAT so you can reuse a limited number of available registered IP addresses for your private network
- Describe RF concepts and the physical infrastructure of a cable link
- Distinguish key attributes for different types of DSL
- Perform a simulated install procedure
- Configure a Cisco 827 router for NAT with PPPoA
- Verify proper operation of DSL and NAT with available Cisco verification commands

Outline

The module contains these lessons:

- Identifying Broadband Features
- Addressing Broadband with NAT
- Describing Cable Technology
- Defining DSL Technology
- Configuring the CPE as the PPPoE Client
- Configuring DSL with PPPoA
- Troubleshooting DSL

Identifying Broadband Features

Overview

This lesson describes the needs that drive development of broadband and the challenges to its widespread deployment.

Relevance

Broadband can allow remote office staff and small office, home office (SOHO) users to connect to the central office (CO) LAN at high speeds for remote access.

Objectives

Upon completing this lesson, you will be able to:

- Describe broadband options as a viable choice for remote access to a central site
- Describe cable options for remote access
- Describe DSL options for remote access
- Describe satellite options for remote access
- Describe wireless options for remote access

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Broadband Uses
- Cable Options
- DSL Options
- Satellite Options
- Wireless Options
- Summary
- Quiz

Broadband Uses

This topic describes broadband options as a viable choice for remote access to a central site.

Why Broadband?

Cisco.com

- High-speed access
- Rich voice and video services
- Always **on**

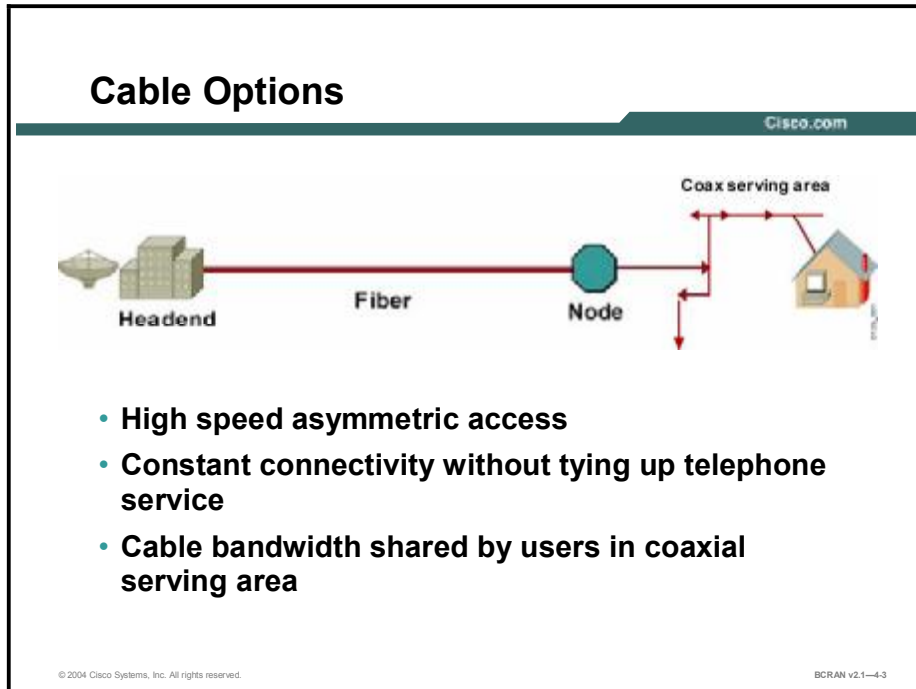
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.2

The Internet is moving from dialup modems and slow connections to a world of high-speed broadband using a variety of technologies. Broadband access can allow remote office staff and SOHO staff to connect to the CO LAN at high speeds (generally defined as any sustained speed above 128 kbps). Broadband access improves employee productivity and provides a foundation for rich new voice and video services. Unlike standard dialup connections, broadband is always *on*.

Broadband options include DSL, fast downstream data connections from direct broadcast satellite (DBS), fixed wireless providers, and high-speed cable modems.

Cable Options

This topic describes cable options for remote access.

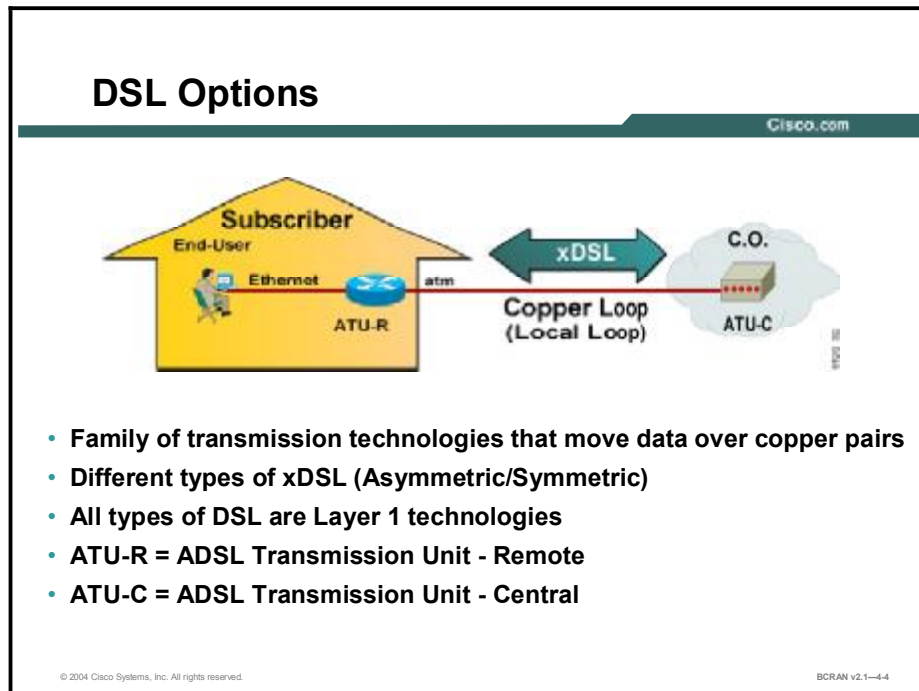


Currently, the most common remote access broadband service is a cable modem. Cable modem users connect to the Internet through a digital cable TV connection. One benefit of cable is its high speed. Cable modems also offer the benefit of constant connectivity. Because there is no need to dial in to the Internet, a user does not have to worry about receiving busy signals. Additionally, going online does not tie up a telephone line. Many cable operators offer telephone services over cable, such as Voice over IP (VoIP) over Cable and Voice over Cable.

The primary disadvantage of cable is that the bandwidth is shared among all of the data users in a given area. Connection speed could drop during busy periods if the cable operator has not placed proper bandwidth quality of service (QoS) mechanisms in place. If there is not enough bandwidth available, then customers might not get the minimum committed information rate (CIR) that they have purchased. However, in practice, end users tend to experience a much higher data rate than the level they have purchased.

DSL Options

This topic describes DSL options for remote access.



DSL is a group of technologies that use the unused bandwidth on a regular copper telephone line to deliver fast digital data transmission. DSL connections are as easy to obtain as dial access. Like leased lines, DSL connections can be always *on* if the DSL modem of the customer connects to a CO DSL termination. Occasionally, the DSL modem may need to place a telephone call if the provider has oversubscribed the service.

There are two disadvantages to DSL:

1. DSL has a maximum distance requirement from the PSTN CO of 18,000 feet.
2. Not all PSTN central offices have been built-out to support DSL. As a result, you may live in a neighborhood that is not serviced by a DSL-capable CO while a neighborhood down the street may have access to DSL service.


Satellite Options

This topic describes satellite options for remote access.

Satellite Options

Cisco.com

- First came the original (bigger) C-band backyard satellite dish in the 1980s
- Followed by direct broadcast satellite (DBS) in the 1990s
- DBS uses smaller-size dishes to receive the satellite signals
- The satellite orbits the earth 22,300 miles above the equator



© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.5

The main issue that satellite access resolves is getting high-bandwidth remote access to places without a high-bandwidth infrastructure. The only way to receive broadband communications in many rural or low-population areas is via a two-way satellite.

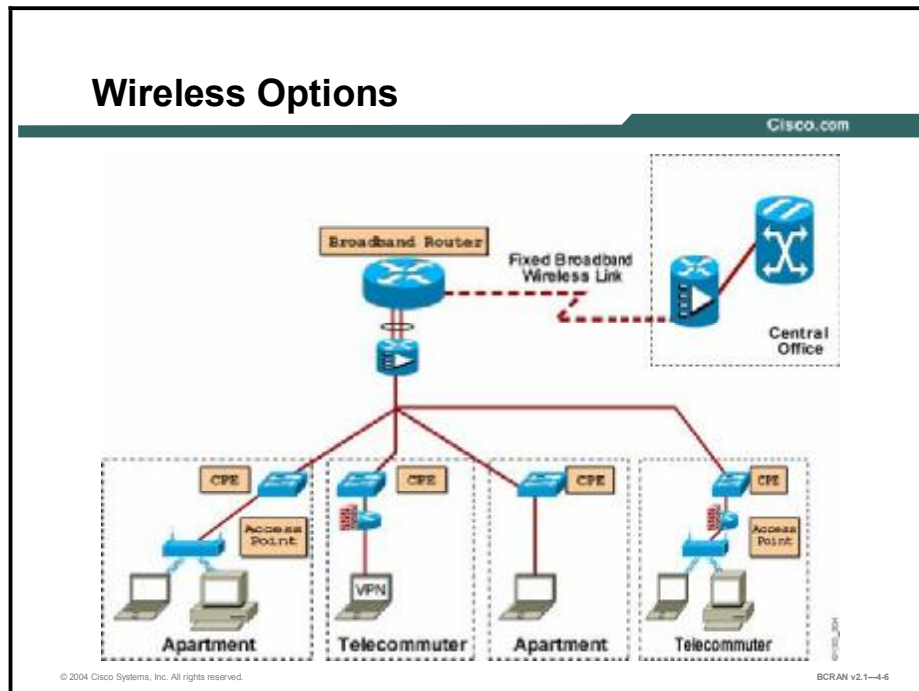
Satellite services deliver downstream data in bursts up to 400 kbps, with upstream speeds as much as 125 kbps. A computer connected to the satellite network does not require time-consuming dialup protocols to log in. However, because of the asymmetric nature of satellite communication, certain applications such as VoIP do not perform very well over satellite. Also, heavy activity on the network can affect satellite speeds.

The typical satellite system requires a small, 1.2-meter or less satellite dish, two standard coaxial cables to connect the satellite dish to a satellite modem, and a satellite modem that connects to a PC through an Ethernet or Universal Serial Bus (USB) port. The latest satellite systems allow subscribers to send and receive information using a satellite dish and still receive television programming.

Satellite networks include geostationary orbit (GSO) satellites and nongeostationary orbit (NGSO) satellites. The latter includes low-earth orbit (LEO) satellites. Latency is higher for GSO satellites than for LEO satellites because the GSO is much higher. Most broadband satellite options use a satellite in orbit approximately 22,300 miles above the equator.

Wireless Options

This topic describes wireless options for remote access.



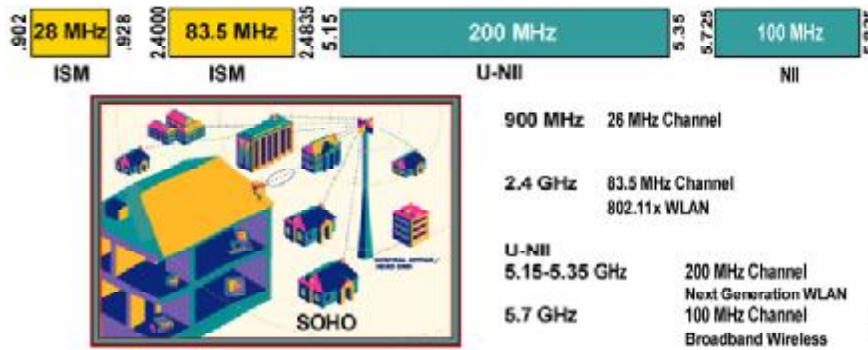
Wireless technology provides line-of-sight bridging at 2-Mbps throughput at distances of up to 25 miles (40.2 km) in U.S. Federal Communications Commission (FCC)-regulated countries or 6.5 miles (10.5 km) in Europe. This technology can provide up to 11-Mbps connectivity from one site to another or from the main site to many remote sites. You need only a bridge and an antenna for each site, which can connect to either a wired or wireless network within those sites. Wireless technology also enables multiple buildings to share a single high-speed connection to the Internet without cabling or dedicated lines. However, you must have line of sight.

Fixed-wireless systems have a long history. Point-to-point microwave connections have long been used for voice and data communications. As technology has continued to advance, higher frequencies have been employed. Thus, smaller antennas can be used, resulting in lower costs and easier-to-deploy systems for private use. The reduction in cost has resulted in a whole generation of carriers that are planning to use wireless access as their last mile of communication.

Wireless Options (Cont.)

Cisco.com

- Various unlicensed frequency bands
- Mobile—low data rate
- Fixed—high data rate
- Spread spectrum
- Residential, SOHO, and small/medium business
- Multi-sectored node sites
- Up to 6 miles in multipoint, 15 miles in point-to-point



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4.7

The fixed wireless broadband market consists of four segments: Local Multipoint Distribution Service (LMDS), Multichannel Multipoint Distribution Service (MMDS), license-free fixed wireless services in the Industrial, Scientific, and Medical (ISM) bands, and the Unlicensed National Information Infrastructure (U-NII) bands.

LMDS, with a 3-mile range and slightly higher throughput than T3 fiber lines, is best suited to large and medium-size enterprises in urban areas. MMDS, with about a 35-mile range and throughput comparable to DSL and cable, is targeted at small businesses and residential customers, particularly those in multitenant dwellings. License-free services, with a 3-to-25-mile range and throughput from 128 kbps to 53 Mbps, vary according to the type of equipment used and number of subscribers.

Summary

This topic summarizes the key points described in this lesson.

Summary

Cisco.com

- **A cable modem can provide up to 90 times the speed of a dial-up connection.**
- **DSL uses the unused bandwidth on a telephone line to deliver fast digital data transmission.**
- **Satellite delivers downstream data in bursts up to 400 kbps, with upstream speeds of up to 125 kbps.**
- **Wireless provides bridging at 2 Mbps throughput at distances of up to 25 miles.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4-8

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers follow in the Quiz Answer Key.

- Q1) Broadband is generally defined as any sustained speed above ____.
- A) 28,800 bps
 - B) 56,000 bps
 - C) 96,000 bps
 - D) 128,000 bps
- Q2) A cable modem could provide up to ____ times the transmission speed (9 Mbps) for remote access in the upstream compared to other technologies.
- A) 40
 - B) 70
 - C) 150
 - D) 128
- Q3) Like leased lines, DSL connections are ____.
- A) inexpensive
 - B) always *on*
 - C) easy to install
 - D) all of the above
- Q4) Most broadband satellite options use a satellite in orbit approximately ____ above the equator.
- A) 22,300 miles
 - B) 23,300 miles
 - C) 32,300 miles
 - D) 28,300 miles
- Q5) Wireless technology provides line-of-sight bridging at ____ throughput at distances of up to 25 miles, but you must have line of sight.
- A) 1-Mbps
 - B) 2-Mbps
 - C) 3-Mbps
 - D) 4-Mbps

Q6) LMDS has a slightly higher throughput than _____ fiber lines.

- A) T1
- B) T3
- C) ISDN
- D) cable

Quiz Answer Key

- Q1) D
Relates to: Broadband Uses
- Q2) C
Relates to: Cable Options
- Q3) B
Relates to: DSL Options
- Q4) A
Relates to: Satellite Options
- Q5) B
Relates to: Wireless Options
- Q6) B
Relates to: Wireless Options

Addressing Broadband with NAT

Overview

This lesson provides an overview of NAT for remote access networks and describes why NAT should be implemented in a broadband environment.

Relevance

The two most compelling problems facing the Internet include IP address depletion and scaling in routing. There are many solutions being developed to solve these problems, but as they are being more fully adopted, a short-term solution is provided by NAT.

Objectives

Upon completing this lesson, you will be able to:

- Describe the process of NAT and explain why you enable it
- Explain the Cisco use of NAT terminology
- Describe the process of translating inside source addresses
- Describe the process of overloading inside global addresses
- Configure NAT to provide dynamic translation
- Configure NAT to provide global address overloading
- Verify correct operation of NAT using the **show** commands
- Identify specific operations in NAT using the **debug** commands
- Remove specific or all NAT entries using the **clear** commands

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

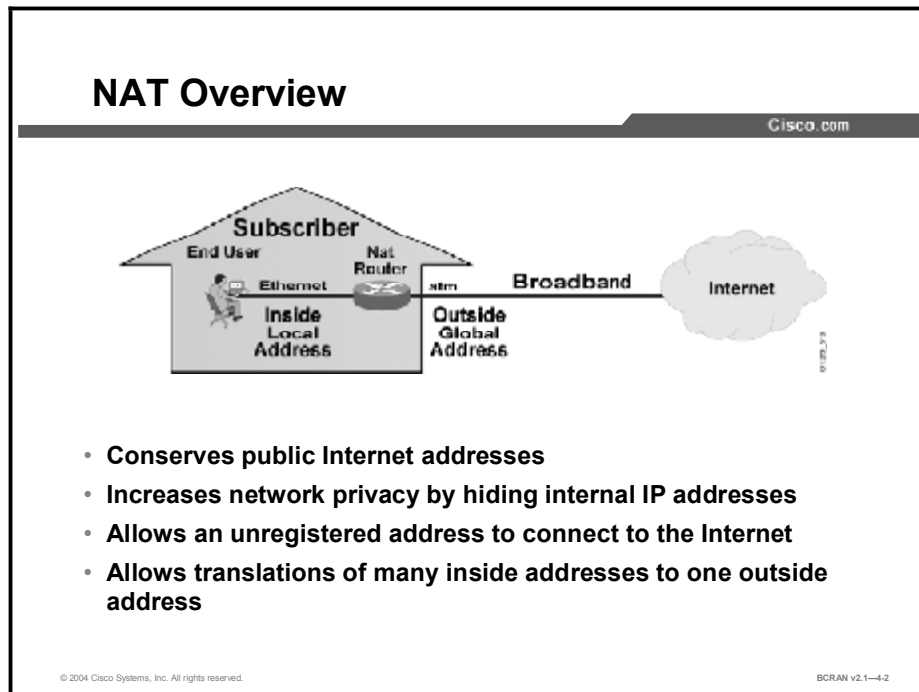
Outline

This lesson includes these topics:

- Overview
- NAT Overview
- NAT Concepts and Terminology
- NAT Operation
- Inside Source Address Translation
- Inside Global Address Overload
- Dynamic NAT Configuration
- Inside Global Address Overload Configuration
- NAT Verification and Troubleshooting
- NAT Troubleshooting
- NAT Entry Clearing
- Summary
- Quiz

NAT Overview

This topic describes why NAT is used.



IP address depletion is a key problem facing the public network. To maximize the use of registered IP addresses, Cisco IOS software implements NAT. This feature, which is the Cisco implementation of RFC 1631, provides a way to use the same IP addresses in multiple internal subnetworks, thereby reducing the need for registered IP addresses.

NAT allows privately addressed networks to connect to public networks such as the Internet. The privately addressed “inside” network sends a packet through the NAT router, and the addresses are converted to legal, registered IP addresses, enabling the packets to be passed to the public network.

NAT can be used when an internal address scheme must be altered due to a change in service providers. It can also be used when merging two intranets, such as when two companies merge. NAT can change addresses incrementally, without changes to hosts or routers other than those bordering stub domains, thereby eliminating duplicate address ranges without readdressing host computers.

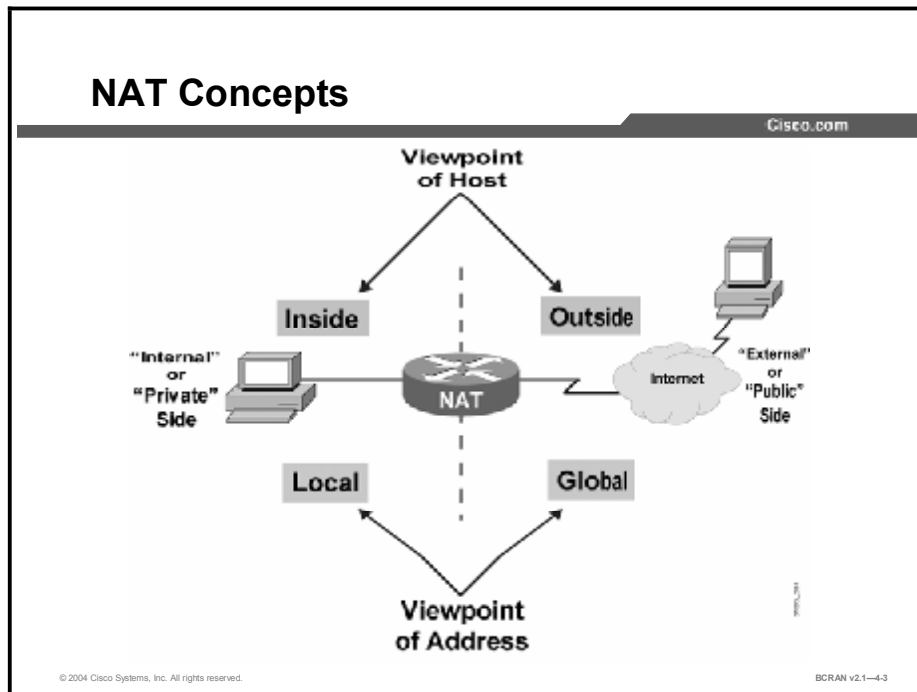
The translation performed using NAT can be either static or dynamic:

- Static translation occurs when addresses in a lookup table are manually configured. A specific inside address maps into a prespecified outside address. The inside and outside addresses are statically mapped one-for-one.
- Dynamic mapping occurs when the NAT border router is configured to understand which inside addresses must be translated and which pool of addresses may be used for the outside addresses. There can be multiple pools of outside addresses.

Multiple internal hosts can also share a single outside IP address, which conserves address space. Address sharing is accomplished by port multiplexing, or changing the source port on the outbound packet so that replies can be directed back to the appropriate host. This option is commonly referred to as Port Address Translation (PAT), or overloading.

NAT Concepts and Terminology

This topic describes NAT concepts and terminology.



As discussed, NAT technology enables private IP networks that use nonregistered IP addresses to connect to the public network such as the Internet. NAT is usually configured on border routers between a stub domain (inside network) and a public network (outside network). To properly understand the concepts and configuration of NAT, you must understand the terms that Cisco uses to describe NAT components.

Using the NAT device as the reference point, all IP addresses can be classified as either inside or outside and as either local or global:

- **Inside or Outside:** Specifies the physical location of an IP host in relation to the NAT device
- **Local or Global:** Specifies the location of the user, or the user point of view, in relation to the NAT device

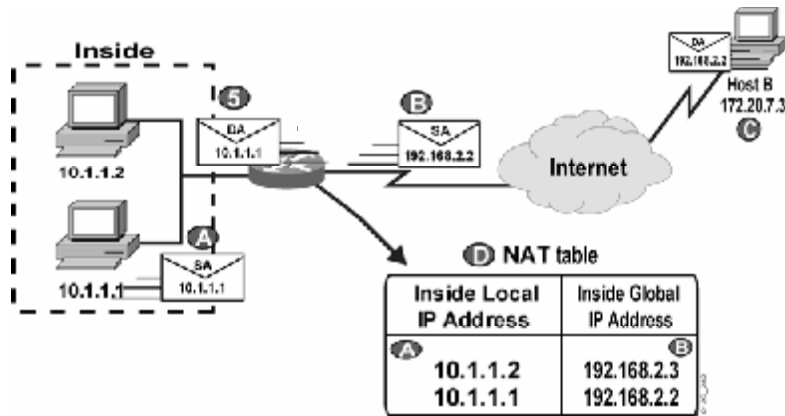
For example, an *inside global* address is the address of an IP host located on the *inside* network from the perspective of a user located on the *global* network; it is the address that a global user would use to communicate with a host on the inside network.

Inside and *local* reference the same side of a NAT device; this side is commonly referred to as the internal or private network. *Outside* and *global* also reference the same side of a NAT device; this other side is commonly referred to as the external or public network. The key difference is that inside/outside refers to host location whereas local/global refers to the user perspective.

Note The designations of inside/outside and local/global are relative to where NAT occurs. The NAT process can occur anywhere and at multiple points between two hosts.

NAT Terminology

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4-4

NAT translates the internal local addresses into globally unique IP addresses before sending packets to the outside network. NAT takes advantage of the fact that relatively few hosts in a stub domain communicate outside of the domain at any given time. Therefore, only a subset of the IP addresses in a stub domain must be translated into globally unique IP addresses for outside communication. The table details various terms that are used to define NAT functions.

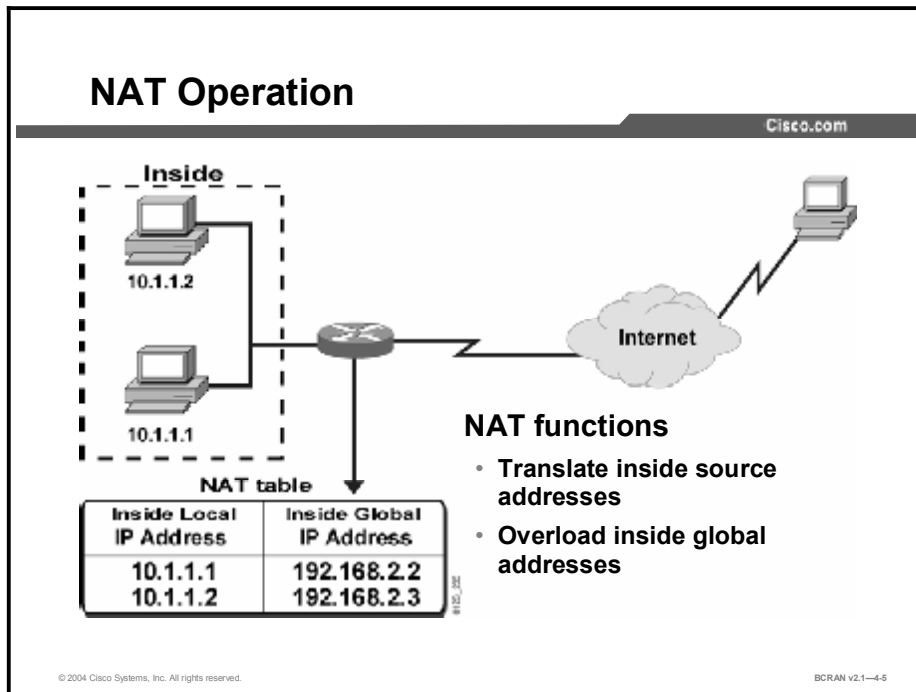
NAT terminology

Term	Definition
Inside local IP address (A, in figure)	The IP address assigned to a host on the inside network. The address can be globally unique but obsolete, allocated from RFC 1918 (Address Allocation for Private Internet Space), or randomly picked.
Inside global IP address (B, in figure)	A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world. The address is allocated from a globally unique address space, typically provided by the ISP.
Outside global IP address (C, in figure)	The IP address that was assigned to a host on the outside network by its owner. The address is allocated from a globally routable address space.
Outside local IP address	The IP address of an outside host as it appears to the inside network. The address can be allocated from address space routable on the inside, for example, from RFC 1918.
Simple translation (D, in figure)	A translation entry that maps one IP address to another.
Extended translation	A translation entry that maps one IP address and port pair to another address and port pair.

Note The NAT examples in this course use an alternative private address range to represent legal registered IP addresses. This is a policy decision to avoid the unauthorized use of public addresses.

NAT Operation

This topic identifies the various NAT functions.

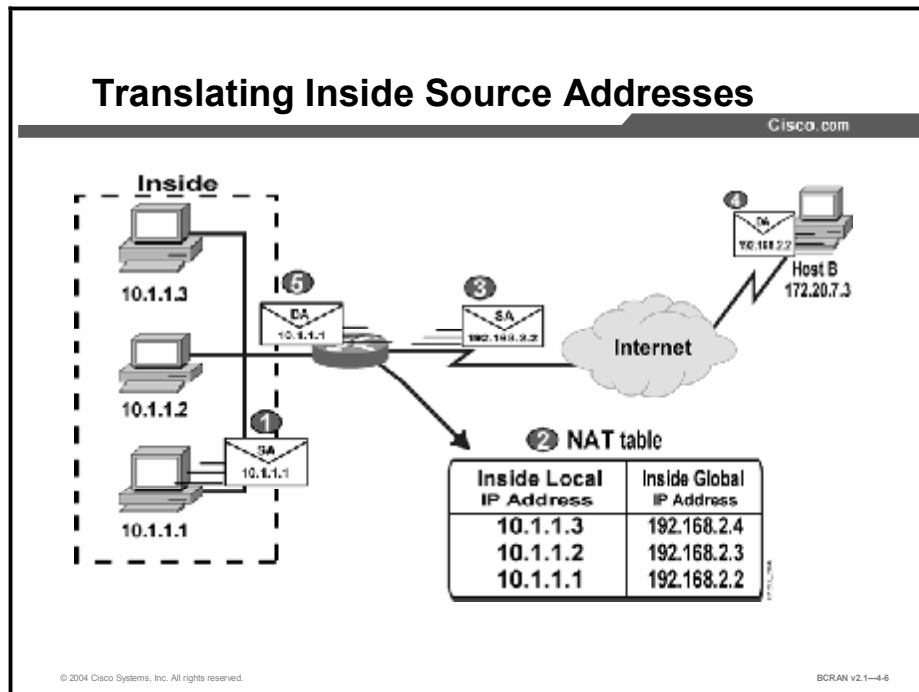


NAT can be used to perform these functions to support a broadband subscriber:

- **Translating inside source addresses:** Establishes a mapping between inside local and inside global addresses.
- **Overloading inside global addresses:** You can conserve addresses in the inside global address pool by allowing source ports in TCP connections or UDP conversations to be translated. When different inside local addresses map to the same inside global address, the TCP or UDP port numbers of each inside host are used to distinguish between the hosts.

Inside Source Address Translation

This topic describes the process of translating inside source addresses.



The figure illustrates NAT operation when it is used to translate source addresses from inside a network to destinations outside the network. These steps include:

- Step 1** User at host 10.1.1.1 opens a connection to outside Host B.
- Step 2** The first packet that the border router receives from host 10.1.1.1 causes the router to check its NAT table, because the packet is going from an inside interface to an outside interface.

Note If a translation is found because it has been statically configured, the router continues to Step 3. If no translation is found and dynamic translation is configured, the router determines that address 10.1.1.1 must be translated to an address available from an address pool. The router dynamically allocates a new address and sets up a translation of the inside local address 10.1.1.1 to a legal inside global address from the dynamic address pool. This type of translation entry is referred to as a *simple entry*.

- Step 3** The border router replaces the inside local IP address of 10.1.1.1 with the selected inside global address, 192.168.2.2, and forwards the packet.
- Step 4** Host B receives the packet and responds to that node using the inside global IP address 192.168.2.2.
- Step 5** When the border router receives the packet with the inside global IP address, the router performs a NAT table lookup using the inside global address as the reference. The router then translates the address back to 10.1.1.1, the inside local address, and forwards the packet to 10.1.1.1. Host 10.1.1.1 receives the packet and continues the conversation.

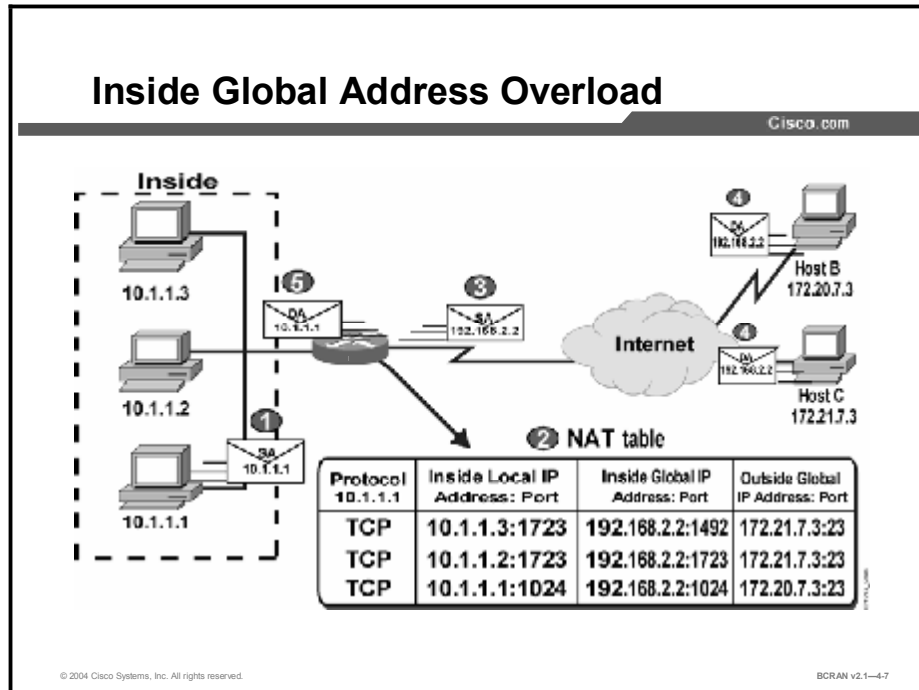
For each packet, the router performs Steps 2 through 5.

Note With static translations, you can initiate connections from either inside or outside. This is because the translation will *always* be in the translation table. With dynamic translations, however, connections *must* be initiated inside-to-outside or outside-to-inside, depending on your configuration.

When configuring inside-to-outside dynamic NAT using the **ip nat inside source list** command, connections *must* be initiated from inside. Likewise, when using **ip nat outside source list** for outside-to-inside dynamic translations, connections *must* be initiated from the outside.

Inside Global Address Overload

This topic describes the process of overloading inside global addresses, also known as PAT.



The figure illustrates NAT operation when a single inside global address is used to represent multiple inside local addresses simultaneously. In this example, an extended translation entry table is used, in which the combination of address and port makes each global IP address unique. The use of ports to make an address unique is called PAT, a subset of NAT. This operation consists of these steps:

Step 1 The first packet the router receives from 10.1.1.1 causes the router to check its NAT table because the packet is going from inside to outside.

Step 2 User at host 10.1.1.1 opens a connection to Host B.

Note If no translation is found, the router determines whether address 10.1.1.1 should be translated based on the configuration. The router allocates a new address and sets up a translation of the inside local address 10.1.1.1 to a legal global address if configured to do so. If overloading is enabled and another translation is active, the router will reuse the global address from that translation and save the unique port information to be able to distinguish it from the other translation entry. This type of entry is called an *extended entry*.

Step 3 The router replaces the inside local IP address of 10.1.1.1 with the selected inside global address, 192.168.2.2, and forwards the packet.

Step 4 Outside Host B receives the packet and responds to that node using the inside global IP address 192.168.2.2 and TCP port 1024.

Step 5 When the router receives the packet with the inside global IP address, the router performs a NAT table lookup using the inside global address and port number, and the outside address and port number as the references. The router then translates the address back to the inside local address of 10.1.1.1 and forwards the packet to 10.1.1.1. Host 10.1.1.1 receives the packet and continues the conversation.

For each packet, the router performs Steps 2 through 5.

Dynamic NAT Configuration

This topic describes a sample configuration of dynamic NAT

Dynamic NAT Configuration

Cisco.com

```
ip nat pool dyn-nat 192.168.2.1 192.168.2.254
netmask 255.255.255.0
ip nat inside source list 1 pool dyn-nat
!
interface Ethernet0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0
ip address 172.16.2.1 255.255.255.0
ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
```

Map inside hosts on the 10.1.1.0/24 network to a pool of globally unique addresses in the 192.168.2.0/24 network.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.8

To enable dynamic inside source IP address translation, perform these steps:

- Step 1** Configure IP routing and appropriate IP addresses on the router.
- Step 2** Define a standard IP access list for the inside network using the **access-list** *access-list-number* {**permit** | **deny**} *source source-wildcard* command.

Note NAT does not always have to occur with directly connected networks. The access list can match any inside local addresses or networks that are present on the inside internetwork.

- Step 3** Define an IP NAT pool of global addresses using the **ip nat pool** *pool-name start-ip end-ip* {**netmask netmask** | **prefix-length prefix-length**} [**type rotary**] command.
ip nat pool pool-name start-ip end-ip {**netmask netmask** | **prefix-length prefix-length**} [**type rotary**] Command

Command	Description
<i>pool-name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the global address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the global address pool.
netmask <i>netmask</i>	Network mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. Specify the netmask of the network to which the address pool belongs.
prefix-length <i>prefix-length</i>	Number that indicates how many bits of the netmask are 1s. Specify the netmask of the network to which the pool addresses belong.
type rotary	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.

Step 4 Map the access list to the IP NAT pool using the **ip nat inside source list** *access-list-number* **pool** *pool-name* command.

Step 5 Enable NAT on at least one inside and one outside interface with the **ip nat {inside | outside}** command. Only packets traveling between inside and outside interfaces can be translated. For example, if a packet is received on an inside interface but is not destined for an outside interface, it will not be translated.

Note The steps for enabling dynamic outside source IP address translation are similar to those listed above, except that the **ip nat outside source list** *access-list-number* **pool** *pool-name* command is used instead. This command maps the access list for outside global addresses to the IP NAT pool of available outside local addresses.

Inside Global Address Overload Configuration

This topic describes how to configure global address overloading.

Inside Global Address Overload Configuration

Cisco.com

```
ip nat pool ovrl-d-nat 192.168.2.1 192.168.2.2
netmask 255.255.255.0
ip nat inside source list 1 pool ovrl-d-nat overload
!
interface Ethernet0/0
ip address 10.1.1.10 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 172.16.2.1 255.255.255.0
ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

Translate all inside hosts on network 10.1.1.0/24 to address 192.168.2.1 or 192.168.2.2

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.9

To configure inside global address overloading, perform these steps:

- Step 1** Configure IP routing and appropriate IP addresses on the router.
- Step 2** Configure dynamic address translation for inside source addresses.
- Step 3** When you define the mapping between the access list and the IP NAT pool using the **ip nat inside source list** *access-list-number* **pool** *pool-name* command, add the **overload** keyword to the command.
- Step 4** Enable NAT on the appropriate interfaces using the **ip nat {inside | outside}** command.

NAT Verification and Troubleshooting

This topic describes the commands that are used to verify and troubleshoot NAT.

Verifying NAT Translations

Cisco.com

Basic IP address translation

```
router#show ip nat trans
Pro  Inside global  Inside local  Outside local  Outside global
---  192.2.2.1       10.1.1.1     ---          ---
---  192.2.2.2       10.1.1.2     ---          ---
```

IP address translation with overloading

```
router#sh ip nat trans
Pro  Inside global  Inside local  Outside local  Outside global
tcp  192.168.2.1:11003  10.1.1.1:11003  172.16.2.2:23  172.16.2.2:23
tcp  192.168.2.1:1067  10.1.1.1:1067  172.16.2.3:23  172.16.2.3:23
```

Unique TCP port numbers are used to distinguish between hosts.

→ A translation for a Telnet connection is still active.
Two different inside hosts appear on the outside with a single IP address.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4-10

The commands in the table here can be used to verify NAT operation.

Commands to Verify NAT Operation

Command	Description
<code>show ip nat translations [verbose]</code>	Shows active translations
<code>show ip nat statistics</code>	Shows translation statistics

Verifying NAT Statistics

Cisco.com

```
router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 extended) Outside interfaces:
Serial10
Inside interfaces:
Ethernet0
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
--Inside source access-list 1 pool dyn-nat refcount 2
pool dyn-nat: netmask 255.255.255.0
start 192.169.2.1 end 192.169.2.250
type generic, total addresses 250, allocated 2 (1%),
misses 0
```

Number and type of active translations

NAT-enabled interfaces

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4.11

The **show ip nat statistics** command displays the number and type of active translations in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out. The number of expired translations is also provided. Other information displayed by this command includes:

- Interfaces that are NAT-enabled using the **ip nat {inside | outside}** command.
- Hits and misses: Number of times a translation table lookup is performed and an entry is either found (hit) or an entry is not found and a new entry must be created (miss).
- Dynamic translation configuration and statistics. These are described in the table here.

Output Field	Description
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, dyn-nat).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start / end	Starting / ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

NAT Troubleshooting

This topic describes how to troubleshoot NAT.

NAT Troubleshooting

Cisco.com

```
router#debug ip nat
IP NAT debugging is on
router#
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [0]
NAT: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [0]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [1]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [2]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [3]
NAT*: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [1]
NAT: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [1]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [4]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [5]
NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [6]
NAT*: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [2]
```

An example address translation inside-to-outside

A reply to the packet sent

An example TCP conversation, outside-to-inside

* Indicates translation was in the fast path

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4-12

If you must use a trace on a NAT operation, use the **debug ip nat [list | detailed]** command in this table.

debug ip nat [list | detailed] Command

Command	Description
debug ip nat [list detailed]	Displays a line of output for each packet that gets translated

As shown in the figure, the debug output includes these key points:

- The asterisk next to NAT indicates that the translation is occurring in the fast path. The first packet in a conversation will always go through the slow path (being process-switched). The remaining packets will go through the fast path if a cache entry exists.
- s=10.1.1.1 is the source address and is being translated to 192.168.2.1.
- d=172.16.2.2 is the destination address.
- The value in brackets is the IP identification number. This information may be useful for debugging because, for example, it can enable you to correlate with other packet traces from sniffers.

NAT Troubleshooting (Cont.)

Cisco.com

```
router#debug ip nat detailed
IF NAT detailed debugging is on
router#
06:20:06: NAT: i: tcp (10.1.1.1, 1045) -> (172.16.2.2, 23) [432]
06:20:06: NAT: s=10.1.1.1->192.168.2.1, d=172.16.2.2 [432]
06:20:06: NAT: o: tcp (172.16.2.2, 23) -> (192.168.2.1, 1045) [0]
06:20:06: NAT: s=172.16.2.2, d=192.168.2.1->10.1.1.1 [0]
06:20:06: NAT*: i: tcp (10.1.1.1, 1045) -> (172.16.2.2, 23) [588]
06:20:06: NAT*: s=10.1.1.1-> 192.168.2.1, d=172.16.2.2 [50688]
06:20:06: NAT*: o: tcp (172.16.2.2, 23) -> (192.168.2.1, 1045) [1]
06:20:06: NAT*: s=172.16.2.2, d= 192.168.2.1 ->10.1.1.1 [1]
06:20:06: NAT*: i: tcp (10.1.1.1, 1045) -> (172.16.2.2, 23) [944]
06:20:06: NAT*: s=10.1.1.1-> 192.168.2.1, d=172.16.2.2 [944]
06:20:06: NAT*: o: tcp (172.16.2.2, 23) -> (192.168.2.1, 1045) [2]
```

Inside interface, protocol TCP, source port 1045, destination port 23
Outside interface, protocol TCP, source port 23, destination port 1045

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4-13

The **debug ip nat [detailed]** command generates a description of each packet that is being considered for translation. This command also outputs information about certain errors or exceptional conditions, such as the failure to allocate a global address. In addition to the information provided by the basic **debug ip nat** command, the **detailed** option reports the protocol and the source and destination port numbers for inbound and outbound translations.

As shown in the figure, the debug output includes these key points:

- “i:” indicates a packet arriving on the inside interface requiring address translation.
- “o:” indicates a packet arriving on the outside interface requiring address translation.
- “tcp” refers to the protocol of the packet.
- The value following the IP address represents the port number.

NAT Entry Clearing

This topic describes how to clear NAT entries.

Clearing NAT Entries

Cisco.com

```

router#sh ip nat trans
Pro  Inside global      Inside local      Outside local     Outside global
tcp  192.168.2.1:11003   10.1.1.1:11003   172.16.2.2:23    172.16.2.2:23
tcp  192.168.2.1:1067   10.1.1.1:1067    172.16.2.3:23    172.16.2.3:23
router#clear ip nat trans *
router#show ip nat trans

```

→ All entries are cleared.

```

router#sh ip nat trans
Pro  Inside global      Inside local      Outside local     Outside global
udp  192.168.2.2:1220   10.1.1.2:1120    171.69.2.132:53   171.69.2.132:53
tcp  192.168.2.1:11003   10.1.1.1:11003   172.16.2.2:23    172.16.2.2:23
tcp  192.168.2.1:1067   10.1.1.1:1067    172.16.2.3:23    172.16.2.3:23
router#clear ip nat trans udp inside 192.168.2.2 10.1.1.2 1220
171.69.2.132 53 171.69.2.132 53
router#sh ip nat trans
Pro  Inside global      Inside local      Outside local     Outside global
tcp  192.168.2.1:11003   10.1.1.1:11003   172.16.2.2:23    172.16.2.2:23
tcp  192.168.2.1:1067   10.1.1.1:1067    172.16.2.3:23    172.16.2.3:23

```

→ 192.168.2.2 is cleared.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4-14

If you must clear a dynamic translation entry, use the commands in the table here.

Commands for Clearing NAT Entries

Command	Description
clear ip nat translation *	Clears all translation entries
clear ip nat translation inside <i>global-ip local-ip [outside local-ip global-ip]</i>	Clears a simple translation entry containing an inside translation, or both an inside and outside translation
clear ip nat translation outside <i>local-ip global-ip</i>	Clears a simple translation entry containing an outside translation
clear ip nat translation protocol <i>{inside global-ip global-port local-ip local-port outside local-ip local-port global-ip global-port}</i>	Clears an extended entry (in its various forms)

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **NAT technology enables private IP networks that use nonregistered IP addresses to connect to a public network.**
- **NAT can be used for translating inside source addresses.**
- **NAT can be used for overloading inside global addresses.**
- **Configure Dynamic NAT configuration and enable overloading of global addresses.**
- **Use show commands to verify correct operation of NAT.**
- **Use debug commands to identify specific operations in NAT.**
- **Use clear commands to remove specific or all NAT entries.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—4-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) How does NAT help solve the limited IP address problem?
- A) NAT allows the use of restricted IP addresses on the public Internet.
 - B) NAT translates 32-bit IP addresses to 48-bit IP addresses.
 - C) NAT has you renumber all your existing addresses to restricted IP addresses.
 - D) NAT translates inside private addresses to legal outside addresses.
- Q2) Which is a legitimate public IP address that represents one or more inside local IP addresses to the outside world?
- A) inside local IP address
 - B) inside global IP address
 - C) outside global IP address
 - D) outside local IP address
- Q3) What is the process of using unique TCP and UDP port numbers to distinguish translations for traffic sourced from the same IP address?
- A) overloading inside global addresses
 - B) translating inside source addresses
 - C) handling overlapping networks
 - D) translating inside global addresses
- Q4) When translating inside source addresses, the inside local IP address is translated to the _____.
- A) inside IP address of the NAT router
 - B) outside global IP address of the source host device
 - C) inside global IP address of the source host device
 - D) outside global IP address of the destination host device
- Q5) Here is the output of a **show ip nat translations** command:

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	192.168.2.1:11003	10.1.1.1:11003	172.16.2.2:23	172.16.2.2:23
tcp	192.168.2.1:1067	10.1.1.2:1067	172.16.2.3:23	172.16.2.3:23

Which type of NAT function do these lines indicate is occurring?

- A) dynamic translation of outside local addresses
- B) static translation of inside local addresses
- C) overloading inside global addresses
- D) this is an error display; no NAT function is occurring

- Q6) When translating inside source IP addresses, you use the **ip nat pool** command to provide a pool of _____.
- A) static inside global IP addresses
 - B) static outside local IP addresses
 - C) dynamic inside local IP addresses
 - D) dynamic inside global IP addresses
- Q7) Which best describes the overloading of inside global addresses using NAT?
- A) translating multiple inside addresses to a single global IP address
 - B) translating multiple inside addresses to multiple outside IP addresses
 - C) combining two networks that have the same IP addresses
 - D) translating a single inside address to multiple outside IP addresses
- Q8) Which command can you use to verify NAT is operating?
- A) **show ip nat status**
 - B) **show ip nat pool**
 - C) **show ip nat translations**
 - D) **show ip route**
- Q9) What does the **detailed** option for the **debug ip nat** command display?
- A) packet switched from cache entry
 - B) inside-to-outside NAT IP address and port translations
 - C) inside-to-outside NAT IP address translations
 - D) NAT translations timers
- Q10) Which command clears an extended IP NAT translation?
- A) **clear ip nat translation**
 - B) **clear ip nat translation inside**
 - C) **clear ip nat translation outside**
 - D) **clear ip nat translation *protocol* inside**

Quiz Answer Key

- Q1) D
Relates to: NAT Overview
- Q2) B
Relates to: NAT Concepts and Terminology
- Q3) A
Relates to: NAT Operation
- Q4) C
Relates to: Inside Source Address Translation
- Q5) C
Relates to: Inside Global Address Overload
- Q6) D
Relates to: Dynamic NAT Configuration
- Q7) A
Relates to: Inside Global Address Overload Configuration
- Q8) C
Relates to: NAT Verification and Troubleshooting
- Q9) A
Relates to: NAT Troubleshooting
- Q10) D
Relates to: NAT Entry Clearing

Describing Cable Technology

Overview

This lesson covers cable technology concepts and the physical infrastructure of a cable link.

Relevance

Cable technology can provide a reliable high-speed alternative for remote access to a central site.

Objectives

Upon completing this lesson, you will be able to:

- Describe a traditional hybrid fiber-coaxial architecture
- Describe how data services can be delivered over a cable network
- Describe how data signals are transmitted over RF channels
- Describe current trends in digital cable systems

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

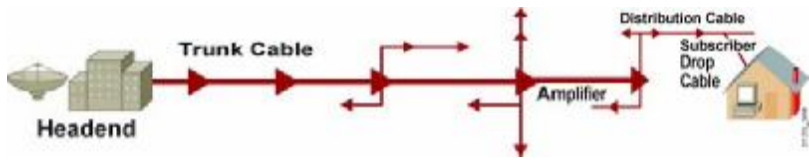
- Overview
- Cable Features
- Data over Cable
- Cable System Functionality
- Cable System Components
- Hybrid Fiber-Coaxial Architecture
- Digital Signals over RF Channels
- Cable Technology Terms
- Cable Technology: Putting It All Together
- Process for Provisioning a Cable Modem
- Configuration of a Router with a Cable Modem
- Summary
- Quiz

Cable Features

This topic describes the features of cable technology.

What Is Cable?

Cisco.com



The diagram illustrates the cable network architecture. It starts with a **Headend** on the left, which connects to **Trunk Cable**. The Trunk Cable leads to an **Amplifier**, which has multiple output lines. From the Amplifier, the signal goes to **Distribution Cable**, which then branches into **Subscriber Drop Cable** leading to a house icon.

- **Cable refers to use of coaxial cable for signal transmission.**
- **CATV: originally meant “community antenna television.”**
- **Cost-effective “broadcast” architecture cascaded to users.**
- **Can offer voice and data as well as analog and digital video.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-2

CATV, commonly called cable TV, was invented to solve the problem of poor TV reception. To ensure that consumers could obtain cable service with the same TV sets that they use to receive over-the-air broadcast TV signals, cable operators recreate a portion of the over-the-air radio frequency (RF) spectrum within a sealed coaxial cable line.

Since the introduction of high-speed data and telephony and other such services, it has become more common for the larger cable operators to have telephone switches *and* the cable modem termination system (CMTS). These cable operators also maintain other equipment in the same facility, taking care of both telephony and data services, in addition to analog and digital video services.

Small and medium-size businesses can gain the following benefits from high-speed cable Internet access:

- Virtual Private Network (VPN) connectivity to corporate intranets
- SOHO capabilities for work-at-home employees
- Interactive television
- PSTN-quality voice and fax calls over the managed IP networks

Businesses large and small have employees who work from their homes. To stay in touch, employees need secure high-speed remote access to the corporate intranet and access to the Internet for e-mail communication with customers and suppliers.


Data over Cable

This topic describes how data services can be delivered over a cable network using fiber cable technology.

Why Fiber?

Cisco.com

- **Small size**
- **Lightweight**
- **Easy to handle**
- **Immune to external interference**



© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4-3

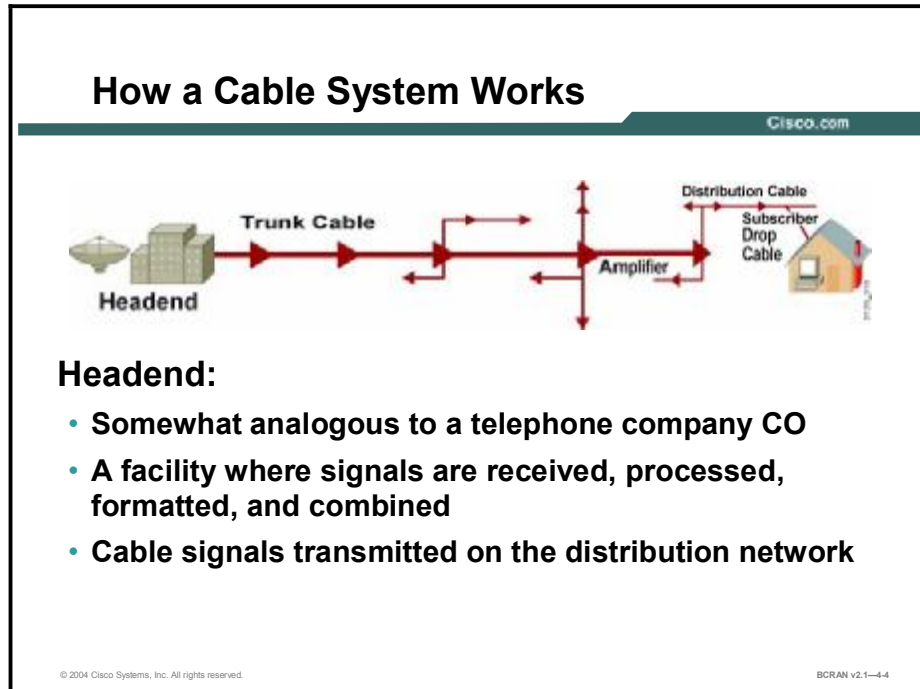
Fiber is used to replace cable amplifiers throughout the cable plant. Amplifiers are placed approximately every 2000 feet to ensure that all RF signals will be delivered to the home of the user with enough power and clarity to receive all channels within the spectrum (50 to 860 MHz) for analog TV, digital TV, and digital data cable modem services.

In a 20-mile plant, approximately 52 amplifiers would be used to reach the last house 20 miles away. Fiber allows the cable operator to run longer distances, with less noise, and to remove amplifiers from the link.

The downstream traffic emanates from the headend and is injected into a trunk cable, at signal strength above 50 dB. Feeder cables emanate from the trunk cables. Passive devices called splitters divide the traffic at branching points to provide geographical coverage.

Cable System Functionality

This topic describes how data services can be delivered over a cable network.



The headend and its connected coaxial cables and subscribers constitute a cable system. In most cases, a cable system is a local operation in a given community that includes:

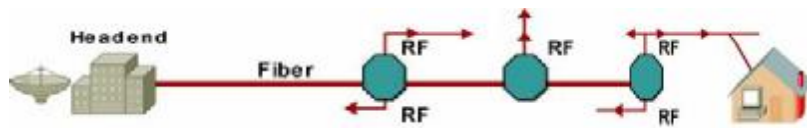
- A business office
- A variety of technical facilities, including the cable network itself
- A warehouse where materials and spare parts are kept
- A storage lot where vehicles are parked and some materials are stored

The headend is where the cable operator puts the various channels on the frequencies that are compatible with the cable network.

Larger cable systems will be much more complex and may serve several communities in a geographical area. Big companies that operate multiple systems are called multiple service operators (MSOs).

How a Cable System Works (Cont.)

Cisco.com



Distribution network

- In a hybrid fiber-coaxial (HFC) architecture, optical fiber replaces trunk portion of the distribution network.
- Small service areas, each with from as few as 100 to as many as 2,000 homes passed.
- Fiber connects between the headend (or hub) and an optical node, where light is converted to RF.
- From the node, RF signals are distributed throughout the serving area via coaxial cable.

© 2004 Cisco Systems, Inc. All rights reserved.

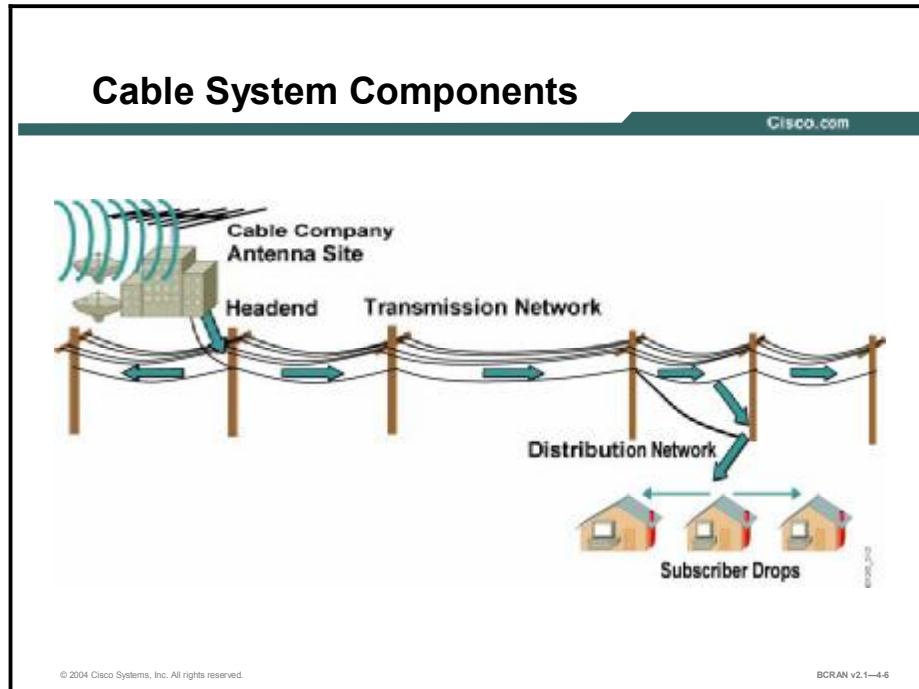
BCRAN v2.1-4.6

The distribution network is made up of fiber and coaxial cabling, which carry television signals toward the subscriber. The last part, and also one of the most infamous parts of the cable network, is the subscriber drop. The subscriber drop includes the following:

- Everything from the connection to the feeder out of the utility pole
- Set-top box
- Grounding and attachment hardware
- Cable
- All the bits and pieces that make that final connection work

Cable System Components

This topic describes the components of a cable system delivering data services.



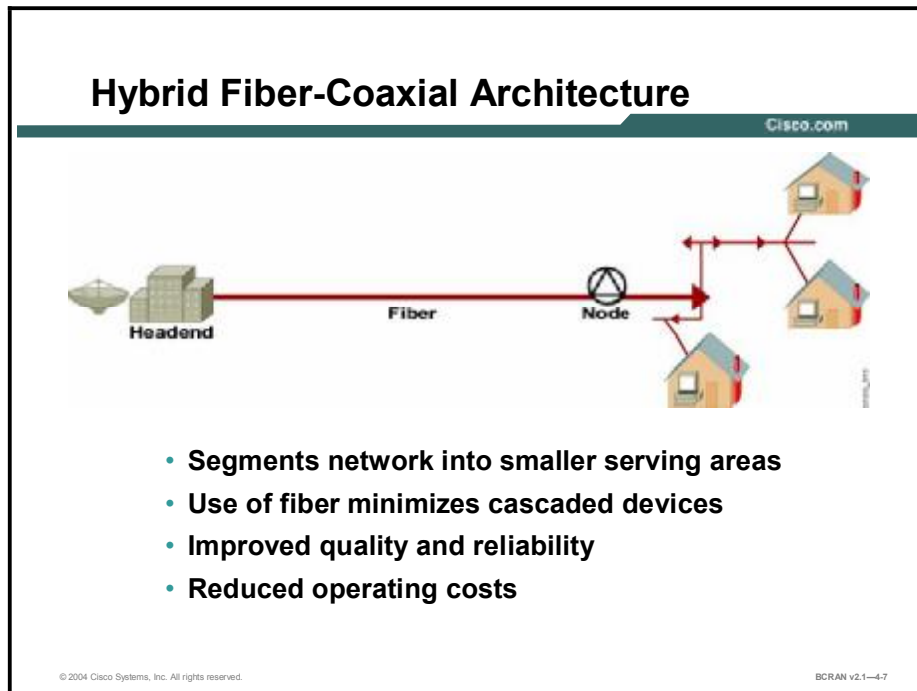
The major components of a cable system include:

- **Antenna site:** The location of main receiving antennas for broadcast and satellite reception.
- **Headend:** Somewhat analogous to a CO of a telephone company. A facility where signals are received, processed, formatted, and combined for transmission on the distribution network.
- **Transportation network:** Used where necessary to link a remote antenna site to a headend or a remote headend to the distribution network. Also used to link microwave, fiber, or coaxial supertrunk.
- **Distribution network:** In a classic tree-and-branch cable system, trunk and feeder cables constitute the distribution network. The trunk is the backbone. The trunk distributes signals throughout the community that is being served and typically uses 0.750-inch (19 mm) diameter coaxial cable. The feeder branches off the trunk and passes all of the homes in the service area, typically using 0.500-inch (13 mm) diameter coaxial cable.
- **Subscriber drop:** Connection between the feeder portion of distribution network and the subscriber terminal (TV set, VCR, and so forth). Includes coaxial (typically 59-series or 6-series coaxial cable), hardware, passive devices, and set-top box.

This topology minimizes the amount of wiring that is required and is a natural topology for broadcasting. The fundamental technical problem encountered by cable TV engineers is that broadcast analog signal strength attenuates (weakens) as it moves through conducting material. Outside noise, weather, and temperature changes affect signal strength through coaxial cable. To combat these problems, cable operators use fiber-optic cable in place of coaxial cable trunks.

Hybrid Fiber-Coaxial Architecture

This topic describes current trends in digital cable systems.



To offer high-speed Internet services, a cable operator creates a data network that operates over the HFC system. To deliver data services over a cable network, one 6-MHz television channel (in the 50-to-750 MHz range) is typically allocated for downstream traffic to homes, and another 6-MHz channel (in the 5-to-42 MHz band) is used to carry upstream signals.

A headend CMTS communicates through these channels with cable modems that are located in subscriber homes to create a virtual LAN connection.

This upstream and downstream bandwidth is shared by the active data subscribers that are connected to a given cable network segment, typically 500 to 2,000 homes on a modern HFC network. The tree-and-branch network architecture for HFC can be a fiber backbone, cable area network, superdistribution, Fiber to the Feeder, or a ring.

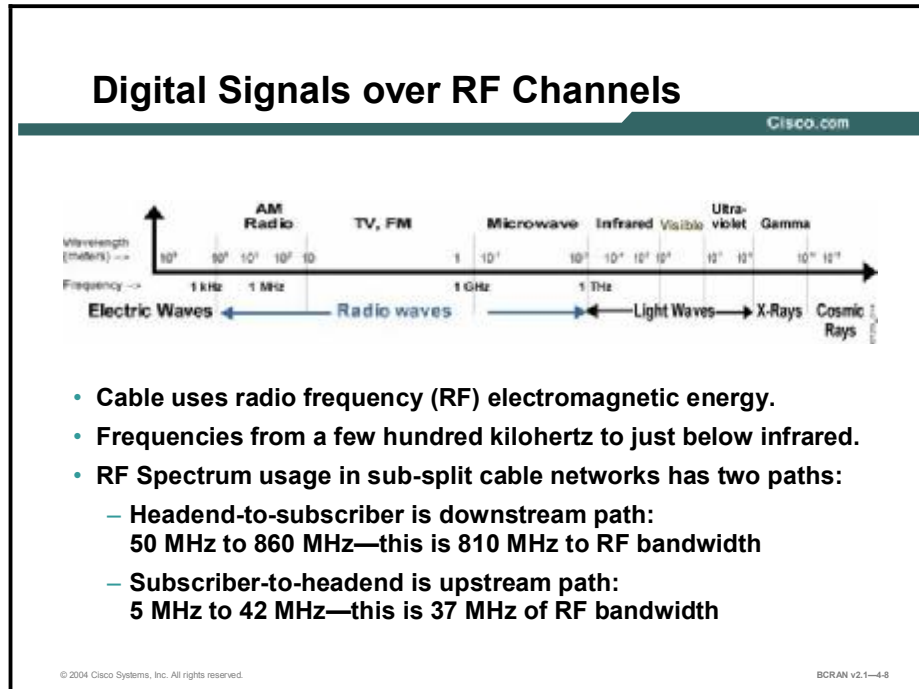
An individual cable modem subscriber may experience access speeds from 500 kbps to 2.5 Mbps, depending on the network architecture and traffic load.

If high usage does begin to cause congestion, cable operators have the flexibility to add more bandwidth for data services. A cable operator can simply allocate an additional 6-MHz video channel for high-speed data, doubling the downstream bandwidth that is available to users.

Another option for adding bandwidth is to subdivide the physical cable network by running fiber-optic lines deeper into the neighborhoods. This practice reduces the number of homes that are served by each network segment and increases the amount of bandwidth that is available to customers.

Digital Signals over RF Channels

This topic describes the current RF used in digital cable systems.



- Cable uses radio frequency (RF) electromagnetic energy.
- Frequencies from a few hundred kilohertz to just below infrared.
- RF Spectrum usage in sub-split cable networks has two paths:
 - Headend-to-subscriber is downstream path:
50 MHz to 860 MHz—this is 810 MHz of RF bandwidth
 - Subscriber-to-headend is upstream path:
5 MHz to 42 MHz—this is 37 MHz of RF bandwidth

When you tune your FM radio across the spectrum to find different radio stations, you are tuning that radio to different electromagnetic frequencies across the spectrum. Cable works the same way.

The cable TV industry uses the portion of the electromagnetic spectrum between approximately 5 MHz and 1 GHz. This band is in a portion of the electromagnetic spectrum known as radio waves and is commonly as RF.

Cable carries TV channels or data carriers at different frequencies. The equipment in the subscriber home is able to tune to those frequencies and allow the customer to view the channel, either on the TV or through a cable modem, and route that information to a computer.

Cable networks can transmit signals in both directions simultaneously on the same cable. Outgoing frequencies to the customer are in the 50-to-860 MHz range, while the incoming frequencies are in the 5-to-42 MHz range.

The downstream path is divided into 6 MHz (or 7 MHz or 8 MHz channels) as defined by a frequency plan.

The cable TV spectrum has been defined by the cable industry as:

- Very high frequency (VHF) low band (TV channels 2 through 6)
- VHF midband (TV channels 98, 99, and 14 through 22)
- VHF high band (TV channels 7 through 13)
- VHF superband (TV channels 23 through 36)
- VHF hyperband (TV channels 37 and higher)

The upstream or the reverse path is the frequency that is used to transmit signals from the customer back to the cable company. The reverse path operates in the 5-to-42 MHz span.

The upstream path has no frequency plan. It is up to the cable operator to monitor the frequency band of the upstream and place the data signals into clean areas where there is no interference from noise and other signals. Usually, the area between 5 and 15 MHz is noisy and is unusable.

Digital Signals over RF Channels (Cont.)

Cisco.com

Data-over-Cable Service Interface Specification (DOCSIS):

- **RF interface specification of minimum recommended technical performance requirements for data**
- **Cable modem termination system (CMTS) and cable modem (CM) vendors must pass certification**
- **CableLabs tests and grants (or withholds) DOCSIS “Certified” or “Qualified” status**
- **Cable operators purchase certified/qualified equipment to ensure interoperability with vendors**
 - **Reference:**
 - www.cablemodem.com/specifications
- **A variation is Euro-DOCSIS standards that use 7 MHz and 8 MHz for cable plants**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4-9

Data-over-Cable Service Interface Specifications (DOCSIS) defines specific bandwidths for data signals (200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz) that the cable operator can use.

The cable TV industry assigns the available spectrum to serve two purposes. Under the National Television Standards Committee (NTSC) standard, the North American TV standard, each country can determine its own splits and frequency assignments. DOCSIS specifications are based on NTSC TV channel plans. Euro-DOCSIS specifications are written for Phase Alternating Line (PAL) based deployments.

There are three DOCSIS standards currently used:

- DOCSIS 1.0 was the first standard.
- DOCSIS 1.1 was the standard needed to deploy VoIP packet cable with end-to-end quality.
- DOCSIS 2.0, a standard in progress, will be able to provide 30 Mbps in the upstream path.

For more information, refer to the following:

- www.cablemodem.com/specifications/specifications10.html
- www.cablemodem.com/specifications/specifications11.html
- www.cablemodem.com/specifications/specifications20.html

There is a separate set of standards for Euro-DOCSIS. This standards variation defines the physical layers as they fit into 7-MHz and 8-MHz plants around the world. Euro-DOCSIS standards specify 108 to 810 MHz for the downstream. These Euro-DOCSIS standards are:

- SP-RFI-C01-01119 for DOCSIS 1.0, now ANSI/SCTE 22-1 2002
- SP-RFIV1.1-I08-020301 for DOCSIS 1.1, now ANSI/SCTE 23-1 2002

Cable Technology Terms

This topic summarizes basic terms, standards organizations, and RF signaling terms.

Identifying Cable Technology Terms

Cisco.com

Basic Cable Terms

- **Broadband**
- **CATV: Originally community antenna television**
- **Coaxial cable**
- **Headend**
- **Downstream (DS)**
- **Upstream (US)**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—4-10

The following key terms are commonly used to describe cable technology basics:

- **Broadband:** Refers to the ability to frequency-division multiplex (FDM) many signals in a wide RF bandwidth over an HFC network and the ability to handle vast amounts of information.
- **Coaxial cable:** The principal physical medium with which cable TV systems are built. Coaxial cable is used to transport RF signals. Coaxial cable signal loss (attenuation) is a function of the diameter of the cable, dielectric construction, ambient temperature, and operating frequency (f).
- **Headend:** The location where the cable company aggregates, combines, mixes, and modulates all signals to send them downstream. Upstream signals usually are received in the headend.
- **Downstream:** RF signal flow from headend toward subscribers. Also called forward path.
- **Upstream:** RF signal flow from the subscribers to the headend. Also called the return or reverse path.

Identifying Cable Technology Terms (Cont.)

Cisco.com

- **NTSC: National Television System Committee**
- **PAL: Phase Alternating Line**
- **SECAM: Sequential Couleur avec Mémoire**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—4-11

The following are commonly used standards:

- **National Television System Committee (NTSC):** This North American TV technical standard is named after the organization that created it in 1941. Uses a 6-MHz modulated signal.
- **Phase Alternating Line (PAL):** This TV system is used in most of Europe, Asia, Africa, Australia, Brazil, and Argentina. The color difference signals an alternate phase at the horizontal line rate. Uses a 6-MHz, 7-MHz, or 8-MHz modulated signal, depending on PAL version.
- **Sequential Couleur avec Mémoire (SECAM):** This TV system is used in France and other eastern European countries. Uses an 8-MHz modulated signal.

Identifying Cable Technology Terms (Cont.)

Cisco.com

- **Carrier or RF carrier**
- **Spectrum reuse**
- **FDM: Frequency-division multiplexing**
- **QPSK—Quadrature phase shift keying**
- **QAM—Quadrature amplitude modulation**
- **Carrier-to-noise: C/N (also CNR)**
- **Signal-to-noise: S/N (also SNR)**
- **Ingress noise**
- **FEC: Forward error correction**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—4-12

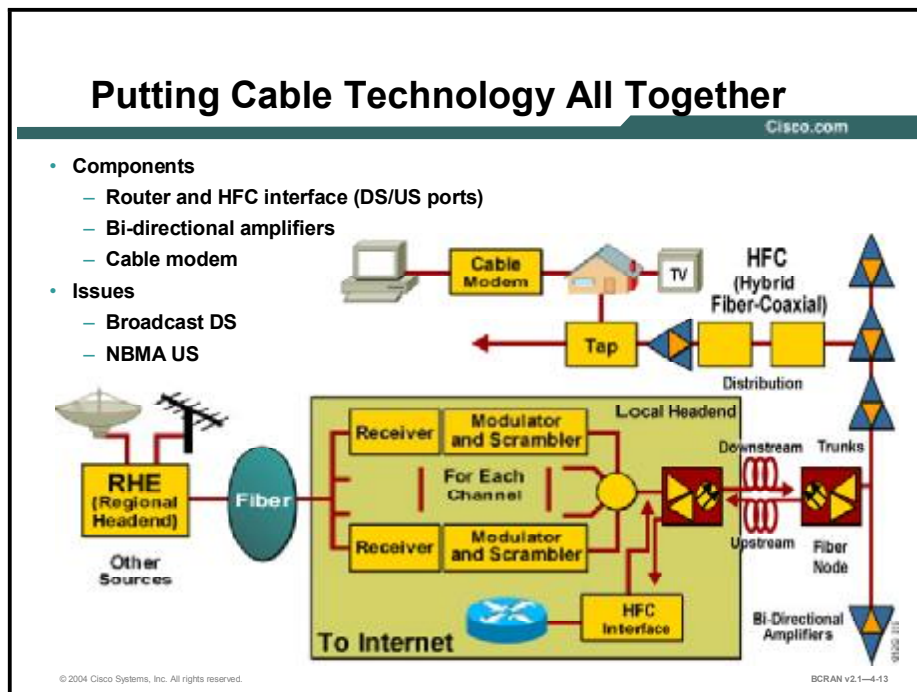
The following are important cable technology terms about RF signal handling:

- **Carrier:** Also RF carrier. An electromagnetic signal on which another, lower-frequency signal (usually baseband, such as analog audio, analog video, or digital data) is modulated to transport the lower-frequency signal to another location.
- **Spectrum reuse:** The most fundamental concept of cable TV is spectrum reuse. Historically, the over-the-air spectrum has been assigned to many uses: two-way radio, broadcasting, cellular phones, and pagers. Much of the spectrum is therefore not available for the carriage of just TV. The result is an inadequate supply of spectrum to serve viewer needs. Cable operators can reuse spectrum that is “sealed” in the coaxial cables of their networks.
- **Frequency-division multiplexing (FDM):** An RF transmission method in which a number of transmitters share a transmission medium. Each transmitter occupies a different frequency.
- **Quadrature phase shift keying (QPSK):** A digital modulation method in which the phase of the RF carrier is varied to transmit data. There are 2 bits per symbol.
- **Quadrature amplitude modulation (QAM):** A digital modulation method in which the phase and amplitude of an RF carrier are varied to transmit data. Typical QAM types are 16-QAM (4 bits per symbol), 64-QAM (6 bits per symbol), and 256-QAM (8 bits per symbol).
- **Carrier-to-noise (C/N):** Also carrier-to-noise ratio (CNR). The difference in amplitude between the desired RF carrier and the noise in a defined bandwidth.
- **Signal-to-noise (S/N):** Also signal-to-noise ratio (SNR). Similar to C/N but relates to a baseband signal.
- **Ingress noise:** Over-the-air (OTA) signals that are coupled into the nominally-closed coaxial cable distribution system, generally via damaged cable, other network components, or poorly shielded TVs and VCRs. Difficult to track down and intermittent in nature.

- **Forward error correction (FEC):** In data transmission, a process by which data is added that is derived from the payload by an assigned algorithm. It allows the receiver to determine if certain classes of errors have occurred in transmission and, in some cases, allows other classes of errors to be corrected.

Cable Technology: Putting It All Together

This topic describes the use of the various cable components and the issues surrounding the technologies that are described in this module.



In the figure shown, the various cable technologies are combined to show how they work together. In the downstream path, entertainment signals come in on the left through satellite dishes, antennas, and analog and digital video servers.

The signals are combined onto a coaxial cable in the headend, and then are presented to a fiber transmitter. The fiber transmitter converts the signals into light and sends to a fiber node somewhere in town.

Farther down the distribution network, the light is converted back to an RF signal and distributed through an amplifier network by the use of taps and drops.

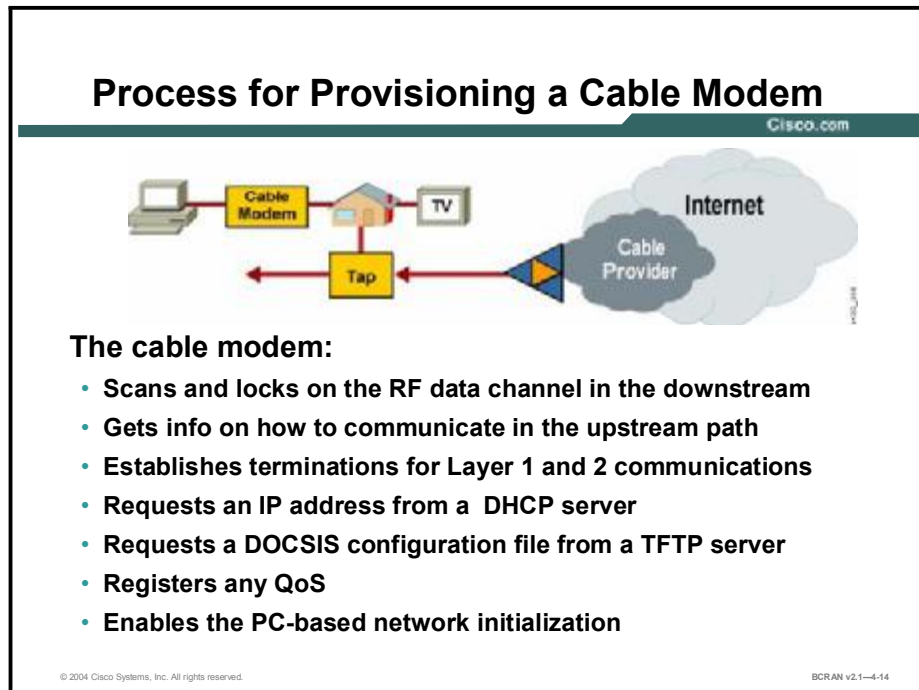
The cable modem receives RF signals, tunes the RF signal, demodulates the data signal back into digital data, and then presents it to the PC.

In the upstream path, the cable modem takes the response from the PC, modulates it to an RF signal, and transmits it at a specific frequency and power level. The transmission specifics are determined by the CMTS back into the drop, tap, distribution network, fiber, and eventually to the CMTS.

The CMTS tunes the RF signal, demodulates the data signal back to digital, and routes it to the Internet.

Process for Provisioning a Cable Modem

This topic describes the steps that provision a cable modem to work in a SOHO of a subscriber that uses TCP/IP.



There are several steps for provisioning a cable modem to operate with a host system for Internet services to provide Cisco Architecture for Voice, Video and Integrated Data (Cisco AVVID) content.

Cable modems are designed and coded to perform these specific DOCSIS-defined steps in the initialization and registration sequence:

- Step 1** The cable modem powering up must scan and lock on the RF data channel in the downstream path.
- Step 2** The modem must read specific maintenance messages in the downstream path that inform it how, where, and when to communicate in the upstream path.
- Step 3** The modem communicates with the CMTS to establish Layer 1 and 2 communications.
- Step 4** The cable modem then requests an IP address and core configuration information from a Dynamic Host Configuration Protocol (DHCP) server. DHCP servers must support RFC 2131 to provide IP addresses to the cable modem.
- Step 5** The modem requests a DOCSIS configuration file from a TFTP server. DOCSIS configuration files are ASCII files created by special DOCSIS editors. To handle the request of the modem, the TFTP server must support RFC 1350.
- Step 6** The cable modem registers with the CMTS, negotiating and ensuring any QoS.
- Step 7** After the cable modem initiation has completed, the PC downstream from the cable modem can request its own IP address from a DHCP server.

Configuration of a Router with a Cable Modem

This topic provides a sample configuration of a Cisco 806 router with an external cable modem.

```
hostname KENSROUTER
!
logging rate-limit console 10 except errors
enable secret andrewisgood
!
ip subnet-zero
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
    import all
    network 10.10.10.0 255.255.255.0
    default-router 10.10.10.1
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
!
!
interface Ethernet0
    ip address 10.10.10.1 255.255.255.0
    ip nat inside
    no cdp enable
    hold-queue 32 in
    no shut
!
interface Ethernet1
    ip address dhcp
    ip nat outside
    no cdp enable
    no shut
!
ip nat inside source list 102 interface Ethernet1 overload
ip classless
!
access-list 102 permit ip 10.10.10.0 0.0.0.255 any
!
line con 0
    exec-timeout 120 0
```

```
stopbits 1
line vty 0 4
  exec-timeout 0 0
  password kenisgood
  login
!
scheduler max-task-time 5000
end
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cable networks can offer voice and integrated data as well as analog and digital video.**
- **Cisco high-speed cable Internet equipment use the HFC system.**
- **On a cable network:**
 - **One 810-MHz channel carries downstream traffic from the headend to subscribers.**
 - **Another 37-MHz channel carries upstream signals from the subscriber toward the headend.**
- **DOCSIS is the cable service interface standard for data carried across RF interfaces.**
- **The DOCSIS CMTS communicates through channels with cable modems located in subscriber homes.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—4-15

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers follow in the Quiz Answer Key.

- Q1) CATV, commonly called cable TV, was invented to solve what consumer problem?
- A) no data communications
 - B) cost-effectiveness
 - C) poor TV reception
 - D) not enough channels
- Q2) The downstream video traffic emanates from the headend and is injected into a trunk cable at signal strength above _____.
- A) 25 dB
 - B) 50 dB
 - C) 75 dB
 - D) 100 dB
- Q3) The _____ is the beginning of the cable distribution network.
- A) headend
 - B) MSO
 - C) cable system
 - D) CSP
- Q4) The subscriber drop includes _____.
- A) the set-top box
 - B) the TV set
 - C) every thing up to the utility pole feeder
 - D) the backyard pedestal
- Q5) Which of the following does not affect signal strength through coaxial cable?
- A) weather
 - B) outside noise
 - C) temperature changes
 - D) topology
- Q6) An individual cable modem subscriber may experience access speeds from_____.
- A) 128 kbps to 2.5 Mbps
 - B) 250 kbps to 2.5 Mbps
 - C) 500 kbps to 2.5 Mbps
 - D) 800 kbps to 2.5 Mbps

- Q7) The upstream frequencies coming from the customer are in the range of _____.
- A) 5 to 42 kHz
 - B) 5 to 42 MHz
 - C) 5 to 42 GHz
 - D) all of the above
- Q8) _____ defines specific bandwidths for data signals (200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz) that the cable operator can use.
- A) Euro-DOCSIS
 - B) DOCSIS
 - C) NTSC
 - D) PAL
- Q9) The location where the cable company aggregates, combines, mixes, and modulates all signals to send them downstream is called _____.
- A) headend
 - B) DOCSIS
 - C) NTSC
 - D) PAL
- Q10) _____ is the TV system used in most of Europe.
- A) Euro-DOCSIS
 - B) DOCSIS
 - C) NTSC
 - D) PAL
- Q11) In what path are signals demodulated back to digital?
- A) upstream
 - B) downstream
 - C) CMTS
 - D) RF
- Q12) Where does a PC receive an IP address in a CMTS?
- A) from headend
 - B) from DHCP server
 - C) from TFTP server
 - D) from DOCSIS

Quiz Answer Key

- Q1) C
Relates to: Cable Features
- Q2) B
Relates to: Data over Cable
- Q3) A
Relates to: Data over Cable
- Q4) A
Relates to: Cable System Functionality
- Q5) D
Relates to: Cable System Components
- Q6) C
Relates to: Hybrid Fiber-Coaxial Architecture
- Q7) B
Relates to: Digital Signals over RF Channels
- Q8) B
Relates to: Digital Signals over RF Channels
- Q9) A
Relates to: Cable Technology Terms
- Q10) D
Relates to: Cable Technology Terms
- Q11) B
Relates to: Cable Technology: Putting It All Together
- Q12) B
Relates to: Process for Provisioning a Cable Modem

Defining DSL Technology

Overview

This lesson distinguishes among the variations of DSL and explains the various encapsulation methods, including Point-to-Point Protocol over ATM (PPPoA), Point-to-Point Protocol over Ethernet (PPPoE), and RFC 1483 Bridged.

Relevance

DSL technology can provide a reliable high-speed alternative for remote access to a central site.

Objectives

Upon completing this lesson, you will be able to perform the following tasks:

- Describe DSL fundamentals
- Describe the various types of DSL
- Describe the distance limitations of DSL
- Describe the fundamentals of ADSL
- Describe how ADSL and POTS coexist
- Describe encapsulation types for ADSL
- Describe bridging functionality
- Describe PPPoE functionality
- Describe PPPoA functionality

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- DSL Features
- DSL Types
- DSL Limitations
- ADSL
- ADSL and POTS Coexistence
- ADSL Channels and Encoding
- Data over ADSL: Bridging
- Data over ADSL: PPPoE
- Data over ADSL: PPPoA
- Summary
- Quiz

DSL Features

This topic describes the features of DSL.

What Is DSL?

Cisco.com

DSL is a family of access technologies that utilize high transmission frequencies (up to 1MHz) to deliver high bandwidth over conventional copper wiring at limited distances.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.2

DSL, although considered an end-to-end solution, really occurs only in the local loop between the customer premises equipment (CPE) and the digital subscriber line access multiplexer (DSLAM). A DSLAM is the device in the CO that is used to terminate many Layer 1 DSL connections. Like dial, cable, wireless, and T1, DSL by itself is a Layer 1 transmission technology, not a complete end-to-end solution.

DSL uses the high-frequency range of up to approximately 1 MHz. For example, asymmetric digital subscriber line (ADSL) uses the frequency range of approximately 20 kHz to 1 MHz. ADSL does not overlap the plain old telephone service (POTS) voice frequency range. Therefore, POTS and ADSL service can coexist over the same wire. Other DSL variants, such as single-line digital subscriber line (SDSL), use a frequency range that overlaps the POTS voice frequency range. Therefore, POTS and SDSL services cannot coexist over the same wire.

DSL Types

This topic describes the various types of DSL.

DSL Variants Examples

Cisco.com

- **Asymmetric DSL (ADSL)**
 - **Key feature: Slow travel upstream (from subscriber to CO), fast travel downstream (from CO to subscriber)**
- **Single-Line DSL (SDSL)**
 - **Key feature: Upstream and downstream speeds are the same**
- **G.SHDSL**
 - **Key feature: G.SHDSL is a new standard that was developed by the International Telecommunications Union (ITU) that addresses the worldwide SDSL market.**
- **Integrated Services Digital Network DSL (IDSL)**
 - **Key feature: No call setup**
- **Very-High-Data-Rate DSL (VDSL)**
 - **Key feature: Very high speed with shorter reach**
- **High-Data-Rate DSL (HDSL)**
 - **Key feature: Used to replace T1 or E1 service**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.3

DSL variants include the following:

- **ADSL:** With ADSL, the connection speed for downloading data is faster than the connection speed for uploading data. This type of DSL service is geared more toward a residential application, where the typical end user is not concerned with being able to send large amounts of data to the Internet. ADSL is perfect for common residential high-speed requirements, such as downloading music or movies, playing online games, surfing the Internet, or receiving large e-mail messages. ADSL provides slow upstream speed for uploading (sending) low-data-rate requests and fast downstream speed for downloading bursts of rich graphics and multimedia content
- **SDSL:** With SDSL, the connection speed for downloading data is exactly the same as the connection speed for uploading data. This type of DSL service is ideal for a commercial application where the end user must send large amounts of data over the Internet. SDSL is perfect for applications such as sending large e-mail messages with attachments to customers, uploading information to a company or corporate server, or updating web pages.
- **G.SHDSL:** A new standard, G.SHDSL, is a symmetric high-data-rate digital subscriber line, was developed by the International Telecommunication Union (ITU) that addresses the worldwide SDSL market. G.SHDSL is multirate, multiservice, extended reach, and repeatable. Supporting data rates from 192 kbps to 2.3 Mbps, G.SHDSL delivers approximately 30 percent greater reach than currently deployed DSL technologies and is expected to rapidly replace the proprietary SDSL implementations of today.

- **ISDN DSL (IDSL):** IDSL is a cross between ISDN and DSL. Like ISDN, it uses a single wire pair to transmit full-duplex data up to 144 kbps. IDSL also uses a 2B1Q line code to enable transparent operation through the ISDN U interface. IDSL is essentially a leased-line ISDN BRI, or an ISDN BRI that is not switched and does not contain signaling (a data [D] channel). The line can be configured for a speed of 64 kbps, 128 kbps, or 144 kbps. IDSL carries only data, but is ideal for remote users because the signals can be repeated, as with ISDN, and because it is billed at a flat rate, thus avoiding per-call fees.

- **Very-high-data-rate digital subscriber line (VDSL):** VDSL delivers 13 to 52 Mbps downstream and 1.5 to 2.3 Mbps upstream over a single-twisted copper pair. The operating range of VDSL is limited to 1,000 to 4,500 feet (304.8 to 1,372 meters). The Cisco Long Reach Ethernet (LRE) solution is based on Ethernet over VDSL.

- **High-data-rate digital subscriber line (HDSL):** HDSL is commonly used as a T1 or E1 replacement. Because HDSL provides T1 or E1 speed, telephone companies have been using HDSL to provision local access to T1 or E1 services whenever possible. The operating range of HDSL is limited to 12,000 feet (3658.5 meters), so signal repeaters are installed to extend the reach.

DSL Limitations

This topic describes the distance limitations of DSL.

DSL Distance Limitations			
DSL Technology	Max. Data Rate Down/Uplink (bps)	Max. Reach feet (km)	Key Attributes
VDSL	51-56Mbps / 1.6-2.3Mbps 13Mbps / 1.6-2.3Mbps	1,000 (0.3) 4,500 (1.5)	Very fast - Short reach No Standard
ADSL	8Mbps / 1Mbps 1.5Mbps / 640kbps	18,000 (5.5)	Coexists with POTS Technology of choice for residential
IDSL	144kbps / 144kbps	18,000 (5.5)+ (wirerepeaters)	Uses existing ISDN CPE Relatively slow
SDSL	1168kbps / 1168kbps	12,000 (3.65)	Symmetric No standard
G.SHDSL	192kbps-2.3Mbps / 192kbps-2.3Mbps	28,000 (8.52)	ITU Standard

© 2004 Cisco Systems, Inc. All rights reserved. BCAN v2.1-4.4

- The tradeoff between different DSL variants is reach vs. speed.
- Maximum Reach numbers are best-case assuming “clean” copper.

The trade-off among various DSL types is reach versus speed. The longer the local loop, the lower the maximum speed the DSL connection can support.

For example, VDSL supports the highest speed but it has the shortest distance limitation.

For ADSL, the maximum distance is typically about 18,000 feet (5,460 meters). To support the maximum ADSL download speed of 8 Mbps, the CPE must be very close to the CO, within several thousand feet.

The maximum speed listed in the figure assumes that there are minimal local loop impairments. Here are some of the many local loop impairments that will influence the maximum speed of the DSL connections and the ability to obtain DSL service in an area:

- **Loading coils in the local loop:** Loading coils will cut off (block) the DSL frequency. Loading coils are used to improve POTS quality on long local loops. They are effectively low-frequency band pass filters. Loading coils must be removed from the local loop to support DSL.
- **Distance from CO to the DSL CPE:** The longer the distance, the lower the speed.
- **Gauge of wire used in the local loop:** Thicker wire supports higher speeds.
- **Wire gauge change:** Changes in wire gauge cause an impedance mismatch that can reduce speed.
- **Bridge taps:** Bridge taps in the local loop cause reflections that can reduce speed.
- **Crosstalk:** Crosstalk between different wires in the same bundle can cause interference that can reduce speed.
- **AM radio:** AM radio interference can also reduce speed.

ADSL

This topic describes ADSL fundamental concepts.

ADSL

Cisco.com

- **ADSL is designed to coexist with POTS, unlike most other DSL types.**
- **ADSL provides slow upstream speed for uploading (sending) low-data-rate requests.**
- **ADSL provides fast downstream speed for downloading bursts of rich graphics and multimedia content.**
- **ADSL features three basic modulation techniques:**
 - **Carrierless Amplitude and Phase (CAP) modulation**
 - **Discrete MultiTone (DMT)**
 - **Consumer/Mass-Market DMT (G.lite)**

NOTE: The type of modulation must match the provider.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-6

ADSL features three basic modulation techniques:

- Carrierless Amplitude and Phase (CAP) modulation
- Discrete Multitone (DMT) modulation
- Consumer/mass-market DMT (G.lite). This technique is the most popular.

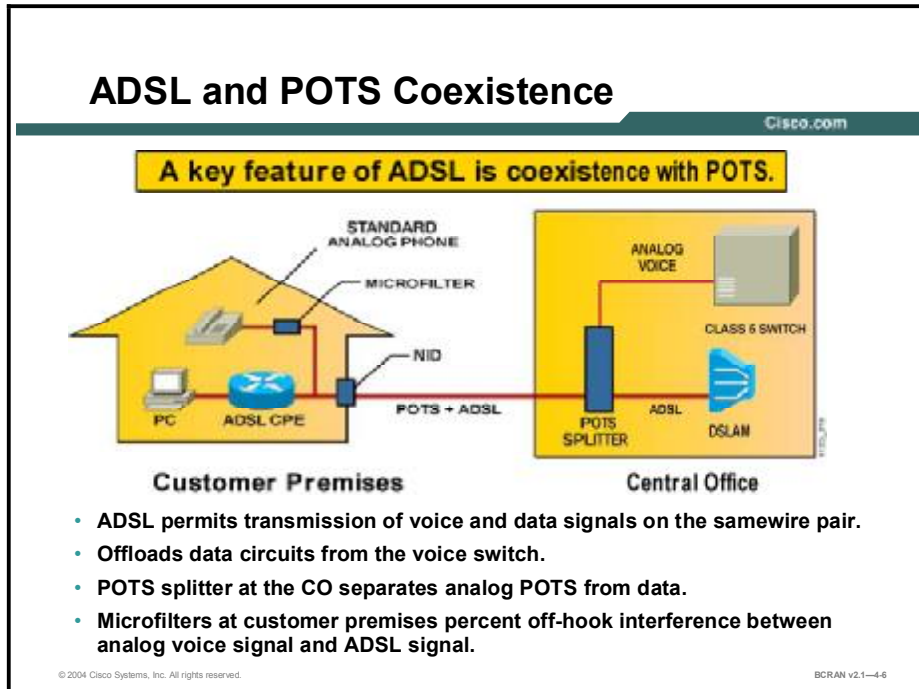
DMT is a line code that is implemented in ITU 992.1 (G.dmt), ITU 992.2 (G.lite), and ANSI T1.413 Issue 2. DMT divides the 1-MHz spectrum offered by a telephone line into multiple 4-kHz subchannels. Each subchannel is optimized based on the local loop characteristics.

In contrast, CAP relies on a single channel for upstream and another single channel for downstream.

An installer must check with the service provider to determine which modulation technique is being used. The modulation method used must correspond with the ADSL CPE and the ADSL modems on the DSLAM.

ADSL and POTS Coexistence

This topic describes how ADSL and POTS coexist.



ADSL is designed to coexist with POTS voice service because ADSL does not overlap the POTS frequency range. ADSL and POTS can be carried over the same wire (local loop) to the CO.

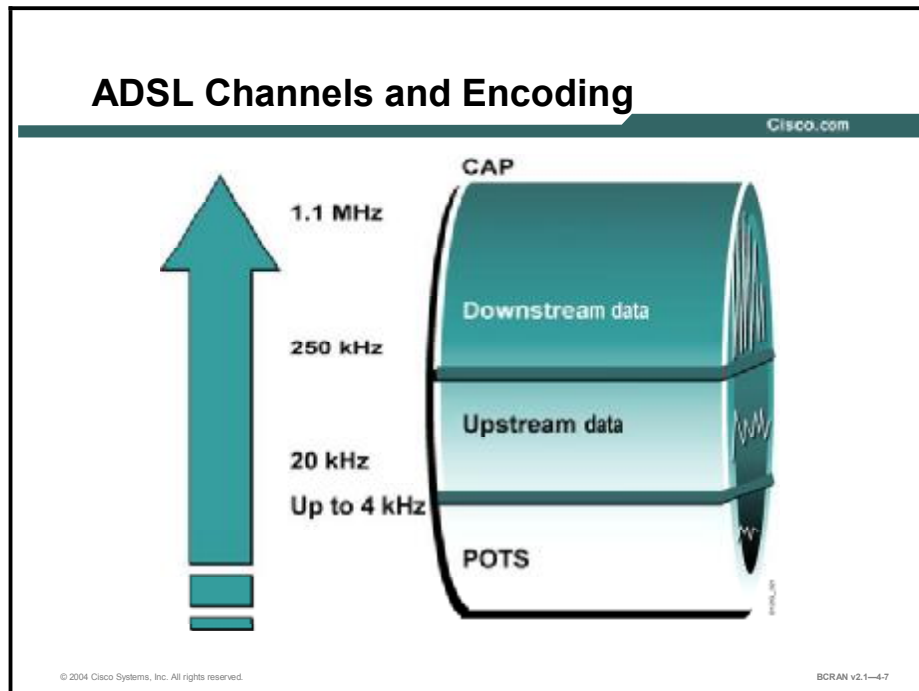
A POTS splitter at the CO splits up the POTS (voice) and ADSL (data) traffic. The POTS traffic goes to the voice switch in the CO, and the ADSL traffic goes to the DSLAM in the CO. The POTS splitter is a passive device. In the event of a power failure, the voice traffic will still be carried to the voice switch in the CO.

ADSL offloads the data (modem) traffic from the voice switch and keeps analog POTS separate from data. Separating voice and data traffic provides fail-safe 911 emergency-call services for POTS operation in the United States.

At the customer premises, a POTS splitter can be installed at the network interface device (NID) by the service provider technician. However, this process will require a trunk roll (having a technician go out to the customer site to install the POTS splitter) to set up the ADSL service. Instead of installing a POTS splitter at the NID, most installations today use microfilters. Microfilters can be installed by the customer and prevent off-hook interference between the analog voice signal and ADSL signal. A microfilter is a passive low-pass filter with two ends. One end connects to the telephone, and the other end connects to the telephone wall jack.

ADSL Channels and Encoding

This topic describes the encapsulation types for ADSL.

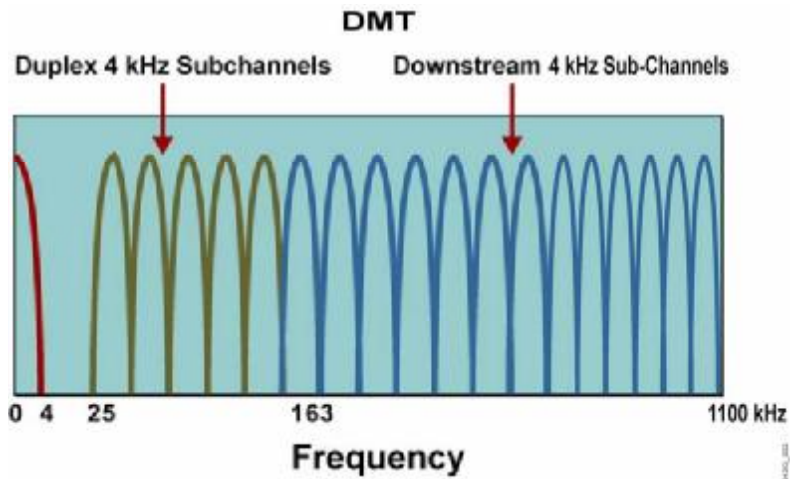


There are two competing and incompatible standards for ADSL. The official American National Standards Institute (ANSI) and ITU standard for ADSL is DMT. Most of the ADSL equipment installed today uses DMT. An earlier and more easily implemented modulation method was the CAP system, which was used on many of the early installations of ADSL. Unlike DMT, CAP is proprietary.

CAP operates by dividing the signals on the telephone line into three distinct bands. Voice conversations are carried in the 0-to-4 kHz band, because they are in all POTS circuits. The upstream channel is carried in a band between 25 and 160 kHz. The downstream channel begins at 240 kHz and goes up to a point that varies, depending on a number of conditions (line length, line noise, or number of users in a particular telephone company switch) but has a maximum of about 1.5 MHz. This system, with the three channels widely separated, minimizes the possibility of interference between the channels on one line or between the signals on different lines.

ADSL Basics—CAP vs DMT Modulation

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

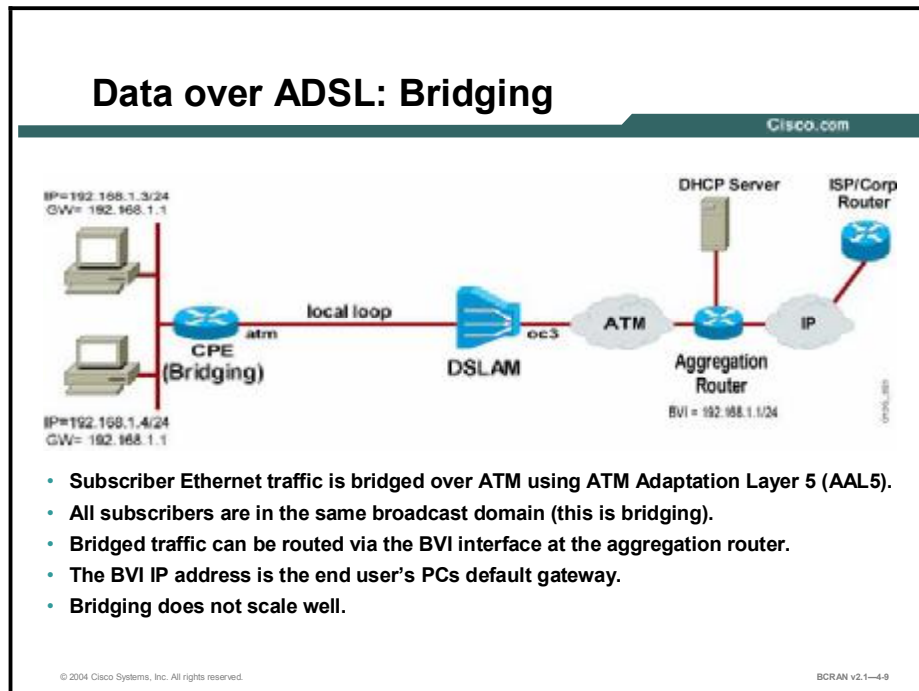
BCRAN v2.1—4.8

DMT also divides signals into separate channels, but does not use two fairly broad channels for upstream and downstream data. Instead, DMT divides the data into 250 separate channels, each 4 kHz. Each channel is monitored and, if the quality is too impaired, the signal is shifted to another channel. This system constantly shifts signals among different channels, searching for the best channels for transmission and reception. Because DMT uses 250 channels, it is more complex to implement than CAP, but it gives more flexibility on lines of differing quality.

G.lite is a less complex version of the DMT standard. Also known as half-rate DMT, G.lite uses only half as many subchannels as DMT and supports a lower maximum downstream speed of 1.5 Mbps and a maximum upstream speed of 640 kbps.

Data over ADSL: Bridging

This topic describes bridging functionality.



DSL is a high-speed Layer 1 transmission technology that works over copper wires. ATM is used as the data-link layer protocol over DSL.

A DSLAM is basically an ATM switch containing DSL interface cards. The DSL Layer 1 connection from the CPE is terminated at the DSLAM. The DSLAM terminates the ADSL connections, then switches the traffic over an ATM network to an aggregation router. For example, the Cisco 6160 DSLAM has an OC-3 ATM uplink and can terminate up to 256 DSL subscriber lines.

There are three major approaches to encapsulating an IP packet over an ATM/DSL connection:

- RFC 1483/2684 Bridged
- PPPoE
- PPPoA

RFC 1483/2684 describes two methods for carrying the traffic over an ATM network. These methods are routed and bridged protocol data units (PDUs). This topic examines only the bridged method.

Using RFC 1483 Bridging, the ADSL CPE is bridging the Ethernet frame from the PC of the end user to the aggregation router (this process will be similar in PPPoE).

At the aggregation router, integrated routing and bridging (IRB) can be used to provide the ability to route between a bridge group and a routed interface using a concept called Bridge-Group Virtual Interface (BVI). The BVI, a virtual interface within the router, acts like a normal routed interface that does not support bridging, but represents the corresponding bridge group to routed interfaces within the router.

Some of the advantages of bridging are as follows:

- Bridging is simple to understand and to implement because there are no complex issues of routing, authentication requirements for users, and so forth.
- The CPE in bridge mode acts as a *dumb* device and does not require any routing functionalities.
- Troubleshooting is minimal because whatever comes in from the Ethernet side passes (bridged) over to the ATM WAN side.
- Bridging architecture is easy to install because of its simple nature.
- Bridging is ideal for single-user Internet access, because the CPE acts as a set-top box. There is no complex troubleshooting required for upper-layer protocols and there is no requirement for additional client software installation on the end-user PCs.

Some of the disadvantages of bridging are as follows:

- Bridging depends heavily on broadcasts to establish connectivity.
- Bridging broadcasts to thousands of users and is inherently unscalable. It consumes bandwidth across the xDSL loop of users and requires resources at the headend router to replicate packets for the broadcast over a point-to-point (ATM permanent virtual circuit [PVC]) medium.
- Bridging is inherently insecure and requires a trusted environment because Address Resolution Protocol (ARP) replies can be spoofed and a network address can be hijacked.
- Broadcast attacks can be initiated on the local subnet, which will deny service to all members of the local subnet.
- IP address hijacking is possible in a bridge environment.
- In a bridged environment, a DHCP server located at the service provider traditionally allocates IP addresses to the end-user PC. The BVI IP address is the end-user PCs default gateway.

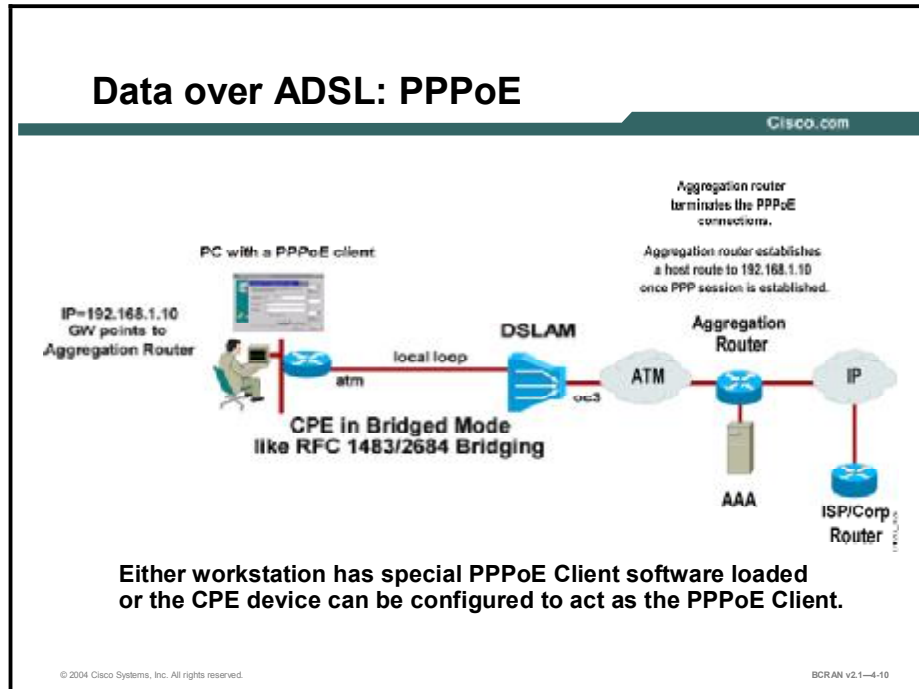
Certain Internet service providers (ISPs) have used an approach of providing illegal IP addresses to their subscribers and then performing Network Address Translation (NAT) at the service provider aggregation router. However, this approach does not scale very well as the number of subscribers increases because the large number of address translations tax the processing power and memory requirements of the router.

RFC 1483 Bridging is more suitable for smaller ISPs or corporate access, where scalability does not become an issue. RFC1483 Bridging has become the choice of many smaller ISPs because it is very simple to understand and implement. However, security and scalability issues are causing bridging architecture to lose its popularity.

ISPs are now opting for PPPoA or PPPoE, which are more scalable and much more secure than bridging, but are more complex and not very easy to implement.

Data over ADSL: PPPoE

This topic describes PPPoE functionality.



PPPoE is also a bridged solution, similar to RFC 1483/2684 Bridging. As with RFC 1483/2684 Bridging, the CPE is bridging the Ethernet frames from the PC of the end user to an aggregation router over ATM. But in this case, the Ethernet frame is carrying a PPP frame inside it. The PPP session is established between the end-user PC (the PPPoE client) and the aggregation router.

In the PPPoE architecture, the PC of the end user runs the PPPoE client software to connect to the ADSL service. The PPPoE client software first encapsulates the end-user data into a PPP frame, and then the PPP frame is further encapsulated inside an Ethernet frame. The IP address allocation for the PPPoE client is based on the same principle as PPP in dial mode, which is via IP Control Protocol (IPCP) negotiation, with Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication. The aggregation router that authenticates the users can use either a local database on the aggregation router or a RADIUS (authentication, authorization, and accounting [AAA]) server.

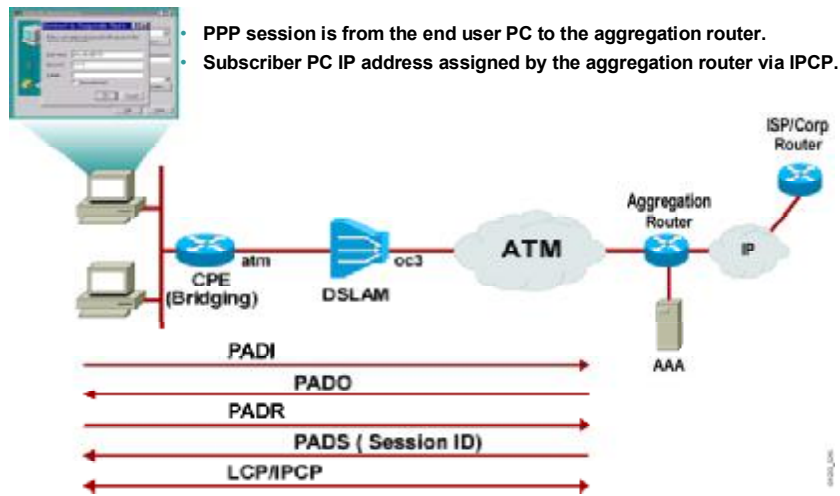
PPPoE provides the ability to connect a network of hosts over a simple bridging CPE to an aggregation router. With this model, a host uses its own PPP stack and the user is presented with a familiar user interface (using the PPPoE client software) similar to establishing a dialup connection. Unlike PPPoA, access control, billing, and type of service can be controlled on a per-user, rather than a per-site, basis.

Note If supporting end-user PPPoE client software is undesirable, then CPE such as the Cisco 827 router can be configured as the PPPoE client. In this case, the Cisco 827 router acts as a router rather than as a simple bridge. It can also act as the DHCP server and use NAT/Port Address Translation (PAT) to allow multiple users behind the router to connect to the service providers using a single ADSL connection and a single PPP username and password.

Note If an external ADSL modem is used, a Cisco 806 router can be used behind the ADSL modem, and the Cisco 806 router can be configured as the PPPoE client. The Cisco 806 router can also act as the DHCP server and use NAT/PAT to allow multiple users behind the router to connect to the service providers using a single ADSL connection and a single PPP username and password.

Data over ADSL: PPPoE (Cont.)

Cisco.com



PPP normally works over a point-to-point connection only. Additional enhancements to PPP were needed to support PPP over an Ethernet multiaccess environment.

As specified in RFC 2516, PPPoE has two distinct stages, a discovery stage and a PPP session stage.

When the discovery stage is complete, both PPPoE peers know the PPPoE session ID and the other Ethernet address of the peer, which together uniquely define the PPPoE session. There are four steps to the discovery stage:

- Step 1** The PPPoE client (end-user PC) broadcasts a PPPoE Active Discovery Initiation (PADI) packet.
- Step 2** The PPPoE server (aggregation router) sends a PPPoE Active Discovery Offer (PADO) packet.
- Step 3** The PPPoE client sends a unicast PPPoE Active Discovery Request (PADR) packet to the PPPoE server.
- Step 4** The PPPoE server sends a PPPoE Active Discovery Session-Confirmation (PADS) packet.

PPP then goes through the normal link control protocol (LCP) and Network Control Protocol (NCP)-(IPCP) process.

When a host initiates a PPPoE session, it must first perform discovery to identify which PPPoE server can meet the client request. Then, the host must identify the Ethernet MAC address of the peer and establish a PPPoE session ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client-server relationship. In the discovery process, a host (the PPPoE client) discovers an aggregation router (the PPPoE server).

There may be more than one PPPoE server that the host (the PPPoE client) can communicate with, based on the network topology. The discovery stage allows the host to discover all PPPoE servers and then select one.

When discovery has been completed successfully, both the host and the selected PPPoE server have the information they will use to build their point-to-point connection over the Ethernet. After the PPPoE session begins, PPP goes through the normal LCP and NCP (IPCP) process.

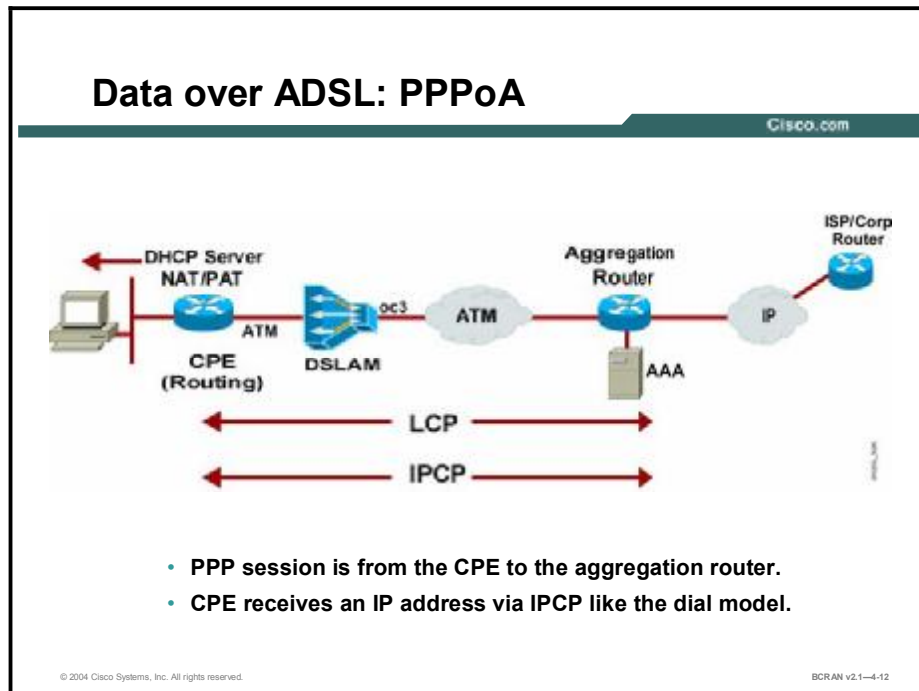
A PPPoE Active Discovery Terminate (PADT) packet may be sent anytime after a session has been established to indicate that a PPPoE session has been terminated. Either the host or the PPPoE server may send it.

For more information on the PPPoE specification, refer to RFC 2516.

Note As per RFC 2516, the maximum-receive-unit (MRU) option must not be negotiated to a size larger than 1492 bytes, because Ethernet has a maximum payload size of 1500 octets. The PPPoE header is 6 octets and the PPP protocol ID is 2 octets, so the PPP MTU must not be greater than $(1500 - 8) 1492$ bytes.

Data over ADSL: PPPoA

This topic describes PPPoA functionality.



PPPoA is a routed solution, unlike RFC 1483 Bridged and PPPoE, where the CPE is set up as a bridge. With PPPoA, the CPE is routing the packets from the PC of the end user over ATM to an aggregation router. The PPP session is established between the CPE and the aggregation router. Unlike PPPoE, PPPoA does not require a host-based software.

The CPE device must have a PPP username and password configured for authentication to the aggregation router that terminates the PPP session from the CPE. The aggregation router that authenticates the users can either use a local database on the aggregation router or a RADIUS (AAA) Server. The PPPoA session authentication can be based on PAP or CHAP. After the PPP username and password have been authenticated, IPCP negotiation takes place and the IP address is assigned to the CPE. After the IP address has been assigned, a host route is established both on the CPE and the aggregation router. The aggregation router must assign only one IP address to the CPE, and the CPE can be configured as a DHCP server and use NAT/PAT to support multiple hosts connected via Ethernet behind the CPE.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **ADSL provides faster downloading speed than uploading speed.**
- **SDSL provides exactly the same downloading and uploading speeds.**
- **ADSL is designed to co-exist with POTS because there is a POTS splitter at the CO.**
- **The trade-off between different DSL types is reach versus speed.**
- **The three common encapsulation methods are: RFC1483/2684 Bridging, PPPoE, and PPPoA.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—4-13

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) DSL utilizes high transmission frequencies up to what limit?
- A) 1 MHz
 - B) 2 MHz
 - C) 3 MHz
- Q2) Which of the following DSL variants offers symmetric speed up to 2.3 Mbps and is an ITU standard?
- A) IDSL
 - B) ADSL
 - C) SDSL
 - D) G.SHDSL
- Q3) Which DSL variant offers the highest speed but the shortest reach?
- A) VDSL
 - B) ADSL
 - C) IDSL
 - D) SDSL
 - E) G.SHDSL
- Q4) The typical maximum distance limit for ADSL service is _____.
- A) 18,000 feet
 - B) 22,000 feet
 - C) 30,000 feet
 - D) 5,000 feet
- Q5) Which three of the following are ADSL modulation methods? (Choose three.)
- A) CAP
 - B) DMT
 - C) G.lite
 - D) 2B1Q

- Q6) ADSL is designed to coexist with POTS because_____.
- A) the ADSL CPE combines voice and data signals
 - B) the DSLAM can be configured to separate the voice and data traffic
 - C) separate sets of transmission wires are used to transmit the voice and data traffic
 - D) a POTS splitter at the CO separates voice and data frequency
- Q7) Which ADSL modulation method uses 250 subchannels that are 4 kHz each?
- A) CAP
 - B) DMT
 - C) G.lite
 - D) 2B1Q
- Q8) Which three of the following are among the advantages of bridging? (Choose three.)
- A) The CPE in bridge mode acts as a dumb device.
 - B) IP address hijacking is possible in a bridge environment.
 - C) Bridging architecture is easy to install because of its simple nature.
 - D) Bridging is very simple to understand and implement because there are no complex issues about routing, authentication requirement for users, and so forth.
- Q9) With the PPPoE client software running on the end-user PC, the PPP session is established between which two devices?
- A) the end-user PC and the aggregation router
 - B) the ADSL CPE and the aggregation router
 - C) the end-user PC and the ADSL CPE
 - D) the ADSL CPE and the DSLAM
- Q10) PPPoE is specified in _____.
- A) RFC 2516
 - B) RFC 2545
 - C) RFC 2216
 - D) RFC 2534
- Q11) When using PPPoE, the MTU should be set to what size?
- A) 1492 bytes
 - B) 1500 bytes
 - C) 1508 bytes
 - D) 1518 bytes

- Q12) PPP over ATM requires which two of the following: (Choose two.)
- A) host-based software on the end-user PC
 - B) no host-based software on the end-user PC
 - C) the CPE to be set up as a bridge
 - D) the CPE to be set up as a router
- Q13) With PPPoA, the PPP session is established between which two devices?
- A) the end-user PC and the aggregation router
 - B) the ADSL CPE and the aggregation router
 - C) the end-user PC and the ADSL CPE
 - D) the ADSL CPE and the DSLAM

Quiz Answer Key

- Q1) A
Relates to: DSL Features
- Q2) D
Relates to: DSL Types
- Q3) A
Relates to: DSL Limitations
- Q4) A
Relates to: DSL Limitations
- Q5) A, B, C
Relates to: ADSL
- Q6) D
Relates to: ADSL and POTS Coexistence
- Q7) B
Relates to: ADSL Channels and Encoding
- Q8) A, C, D
Relates to: Data over ADSL: Bridging
- Q9) A
Relates to: Data over ADSL: PPPoE
- Q10) A
Relates to: Data over ADSL: PPPoE
- Q11) A
Relates to: Data over ADSL: PPPoE
- Q12) B, D
Relates to: Data over ADSL: PPPoA
- Q13) B
Relates to: Data over ADSL: PPPoA

Configuring the CPE as the PPPoE Client

Overview

PPPoE provides the ability to connect a network of hosts over a simple bridging access device to an aggregation router. Normally, the end-user PC uses the PPPoE client software on the PC to connect to the DSL service. However, instead of using the PPPoE client software on the end-user PC, the CPE can be configured as the PPPoE client. This configuration will allow multiple PCs behind the CPE to connect to the DSL service using a single DSL connection and PPP username and password. In this case, the CPE would be configured for routing. This lesson discusses how to configure the Cisco 827 router CPE as the PPPoE client.

Relevance

This lesson provides an overview of the configuration of a PPPoE client on the Cisco 827 router CPE.

Objectives

Upon completing this lesson, you will be able to:

- List the tasks required to successfully configure a PPPoE client connection on a Cisco 827 router
- List and explain the commands required to configure a PPPoE client on a Cisco 827 router
- List and explain the commands required to enable a dynamic IP address to be assigned via IPCP
- List and explain the commands required to configure PAT to scale DSL operations
- List and explain the commands required to configure DHCP to scale DSL operations

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Configuration of a Cisco 827 Router as the PPPoE Client
- Configuration of PPPoE in a VPDN Group
- Configuration of a PPPoE Client
- Configuration of the PPPoE DSL Dialer Interface
- Configuration of PAT
- PAT Configuration Example
- DHCP to Scale DSL
- Configuration of a DHCP Server
- Configuration of a Static Default Route
- PPPoE Sample Configuration
- Summary
- Quiz

Configuration of a Cisco 827 Router as the PPPoE Client

This topic describes the configuration tasks that are required to configure a Cisco 827 router as the PPPoE client. Configuring DSL requires global and interface configuration commands.

Configuration Tasks: Configuring the CPE as the PPPoE Client

Cisco.com

- **Configure a PPPoE virtual private data network (VPDN) group**
- **Configure the ATM Interface**
- **Configure a Dialer Interface**
- **Configure Port Address Translation**
- **Configure DHCP Server**
- **Configure a Static Default Route**

© 2004 Cisco Systems, Inc. All rights reserved.

BICRAN v2.1-4-2

Use the PPPoE DSL configuration tasks listed here in addition to dial-on-demand routing (DDR)-derived commands.

1. Configure a PPPoE virtual private dialup network (VPDN) group.
2. Configure the ATM interface (ADSL interface) of the Cisco 827 router with an ATM PVC and encapsulation.
3. Create and configure the dialer interface of the Cisco 827 for PPPoE with a negotiated IP address and an MTU size of 1492.
4. Configure PAT on the Cisco 827 router to allow sharing of the dynamic public IP address of the dialer interface.
5. Configure the Cisco 827 router to allow it to be the DHCP server for the end-user PCs behind it.
6. Configure a static default route on the Cisco 827 router.

Configuration of PPPoE in a VPDN Group

This topic describes how to configure PPPoE in a VPDN group. VPDN is a Cisco standard that enables a private network dial-in service to span remote access servers.

PPPoE VPDN Configuration

Cisco.com

```
Router (config) #vpdn enable
```

- Enables VPDN on the router

```
Router (config) #vpdn-group name
```

- Creates a VPDN group

```
Router (config-vpdn-req-in) #request-dialin  
Router (config-vpdn-req-in) #protocol pppoe
```

- Creates a request-dialin VPDN subgroup and enables the subgroup to establish PPPoE sessions

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.3

VPDN permits networks to extend beyond the physical central network while giving to remote users the appearance and functionality of being directly connected to a central network.

To enable PPPoE in a VPDN, use the **enable vpdn** command in global configuration mode.

Next, use the **vpdn-group name** command in global configuration mode to create a VPDN group. Use the commands in the table to configure the VPDN group parameters in config-vpdn mode.

VPDN Commands

Command	Description
request-dialin	Creates a request-dial-in VPDN subgroup
protocol pppoe	Enables the VPDN subgroup to establish PPPoE sessions

Configuration of a PPPoE Client

This topic describes how to configure a PPPoE client. After the VPDN group has been defined, the ATM interface must be configured.

PPPoE Client Configuration

Cisco.com

```
Router(config)#interface atm number
```

- **Configure the ATM interface**

```
Router(config)#pvc vpi/vci
```

- **Identify the VPI/VCI virtual circuits**

```
Router(config-if-atm-vc)#pppoe-client dial-pool-number number
```

- **Bind a dialer profile to the ATM interface**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.4

Configure the ATM interface (ADSL interface) of the Cisco 827 router with an ATM PVC and encapsulation.

To configure a PPPoE client on an ATM interface, use the **interface atm number** command in global configuration mode to enter interface configuration mode.

Next, specify the virtual path identifier/virtual channel identifier (VPI/VCI). A virtual path is a logical grouping of virtual circuits (VCs) that allows an ATM switch to perform operations on groups of VCs. A virtual channel describes a logical connection between the two ends of an ATM VC. A PPPoE deployment offers no easy way to dynamically discover the PVC (VPI/VCI) values. The DSL service provider will provide the VPI/VCI value to use in the Cisco 827 router.

To configure the VPI/VCI, use the **pvc vpi/vci** command.

Note ATM cells consist of five bytes of header information and 48 bytes of payload data. The VPI and VCI fields in the ATM header are used to route cells through ATM networks. The VPI and VCI fields of the cell header identify the next network segment that a cell must transmit on its way to its final destination.

Next, configure the PPPoE client encapsulation and specify which dialer interface to use. Use the **pppoe-client dial-pool-number number** command to bind the ATM interface to a dialer interface to set the encapsulation to PPPoE client.

Finally, configure the ATM interface by default with the **dsl operating-mode auto** command. This default value should not be altered because it allows the Cisco 827 router to automatically detect the proper modulation method to use.

Configuration of the PPPoE DSL Dialer Interface

This topic describes the commands that are required to configure a DSL dialer interface. After the ATM interface has been configured, the dialer interface must be configured.

Configuring the PPPoE Dialer Interface

Cisco.com

```
interface ATM0/0
no ip address
dsl operating-mode auto
pvc 8/35
pppoe-client dial-pool-number 1
!

interface Dialer0
ip address negotiated
encapsulation ppp
dialer pool 1
no cdp enable
ip mtu 1492
ppp chap hostname cisco
ppp chap password cisco
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.5

Use the commands in the table for PPPoE DSL dialer configuration.

Dialer Commands for DSL

Command	Description
ip address negotiated	Enables a dynamic address from the service provider using IPCP. With IPCP, DSL routers automatically negotiate a globally unique (registered or public) IP address for the dialer interface from the service provider aggregation router.
encapsulation ppp	Specifies PPP encapsulation for the dialer interface.
dialer pool <i>number</i>	Specifies to which pool the dialer interface is assigned.
no cdp enable	Stops Cisco Discovery Protocol (CDP) advertisements from going out the dialer interface.
ip mtu 1492	Reduces the maximum Ethernet payload size from 1500 to 1492. (PPPoE header requires 8 bytes).
dialer-group <i>number</i>	Configures the dialer group number that will correspond with a dialer list to identify interesting traffic.

Note Unlike ISDN DDR configuration, DSL is always *on*. Therefore, a dialer list is not required to identify interesting traffic.

Configuration of PAT

This topic describes how to configure addressing translations using PAT.

Configure PAT

Cisco.com

```
Router(config)#ip nat inside source list 101 interface Dialer0
overload
```

- Enable dynamic translation of addresses using the assigned IP address of the Dialer0 interface

```
Router(config)#access-list 101 permit ip 10.0.0.0 0.255.255.255 any
```

- Specify the addresses that may be translated

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#ip nat outside
```

- Ethernet interface as inside and the Dialer interface as outside

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-6

NAT overload, commonly referred to as PAT, and PPP/PCP are popular techniques used to scale limited addresses. Using NAT overload means that you can use one registered IP address for the interface to access the Internet from all devices in the network.

PAT Configuration Example

This topic describes an example of configuring PAT.

PAT Configuration Example

Cisco.com

```
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
!
interface Dialer0
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp chap hostname cisco
 ppp chap password 7 1511021F0725
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
!
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.7

The figure illustrates a sample PAT configuration on the Cisco 827 router.

The access list will match any source address in the 10.0.0.0 network.

In this example, the Dialer0 interface is the outside interface, and the Ethernet0 interface is the inside interface.

The 10.x.x.x source addresses will be translated using PAT to the Dialer0 IP address. The Dialer0 interface receives its IP address from the service provider aggregation router using IPCP.

DHCP to Scale DSL

This topic describes how to scale DSL.

Configure a DHCP Server

Cisco.com

```
Router(config)#ip dhcp pool [pool name]
```

- Enable a DHCP pool for use by hosts

```
Router(dhcp-config)#import all
```

- Import DNS and WINS information from IPCP

```
Router(dhcp-config)#network [network address] [subnet mask]
```

- Specify the network and subnet mask of the pool

```
Router(dhcp-config)#default-router [host address]
```

- Specify the default router for the pool to use

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-8

The Cisco IOS DHCP Server feature is a full implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client.

The Cisco IOS DHCP Server was enhanced to allow configuration information to be updated automatically. Network administrators can configure one or more centralized DHCP servers to update specific DHCP options within the DHCP pools. The remote servers can request or “import” these option parameters from the centralized servers.

Configuration of a DHCP Server

This topic describes how to configure the Cisco 827 router as the DHCP server for the end-user PCs behind the router Ethernet interface.

DHCP Server Configuration Example

Cisco.com

```
hostname dslrouter
!
ip dhcp pool team1
  import all
  network 10.0.0.0 255.0.0.0
  default-router 10.0.0.1
!
interface Ethernet0
  ip address 10.0.0.1 255.0.0.0
  ip nat inside
!
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.9

To configure a DHCP address pool on a Cisco IOS DHCP Server and enter DHCP pool configuration mode, use the **ip dhcp pool name** global configuration command.

To import DHCP option parameters into the Cisco IOS DHCP Server database, use the **import all** DHCP pool configuration command. This example uses PPP IPCP.

To configure the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server, use the **network network-number [mask | prefix-length]** DHCP pool configuration command.

To specify the default router list for a DHCP client, use the **default-router address [address2...address8]** DHCP pool configuration command. Note that the DHCP server excludes this address from the pool of assignable addresses.

The commands in the table here allow individual configuration of which DHCP option parameters are requested.

ppp ipcp Commands

Command	Description
ppp ipcp dns request	Requests the Domain Name System (DNS) server addresses from the peer
ppp ipcp wins request	Requests the Windows Internet Name Service (WINS) server addresses from the peer

Configuration of a Static Default Route

This topic describes how to configure a default static route.

Configuring a Static Default Route

Cisco.com

```
Router(config)#ip route 0.0.0.0 0.0.0.0 dialer0
```

- **The CPE can use a static default route to reach all remote destinations**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-10

Configure a static default route on the Cisco 827 router to allow the router to reach all unknown destinations toward the dialer interface. In most DSL installations, the CPE will not be running a dynamic routing protocol to the aggregation router of the service provider. Therefore, a static default route is required on the Cisco 827 router.

When the PPPoE session has been established between the Cisco 827 router and the aggregation router of the service provider, the dialer interface IP address is assigned from the service provider aggregation router via IPCP. The service provider aggregation route will automatically build a host route to reach the Cisco 827 router-dialer interface.

PPPoE Sample Configuration

This topic describes an example of a complete PPPoE configuration.

PPPoE Sample Configuration

Cisco.com

```
hostname dsrouter
!
ip dhcp pool team1
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
!
vpcn enable
!
vpcn-group pppoe
 request-dialin
 protocol pppoe
!
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 8/35
 pppoe-client dial-pool-number 1
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
```

```
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ip mtu 1492
 ip nat outside
 ppp authentication chap callin
 ppp chap password mysecret
!
ip nat inside source list 101
 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0
 0.255.255.255 any
ip route 0.0.0.0 0.0.0.0 Dialer0
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-11

The sample shows the commands for configuring DHCP services and the commands for setting up static default routing.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configuring DSL requires global and interface configuration commands.**
- **In DSL, an ATM VCI/VPI pair must be configured to match the service provider.**
- **After the ATM interface is configured, the dialer interface must be configured.**
- **The Cisco 827 router performs PAT and serve as a DHCP server for the end-user PCs.**
- **A static default routes is configured on the Cisco 827 router.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—4-12

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) When configuring a PPPoE client on the Cisco 827 router, on which interface is the MTU size set to 1492?
- A) the Ethernet interface
 - B) the ATM interface
 - C) the serial interface
 - D) the dialer interface
- Q2) Which PPPoE configuration command is used to establish PPPoE sessions?
- A) **request-dialin**
 - B) **protocol pppoe**
 - B) **enable vpdn**
 - C) **vpdn enable**
 - D) **vpdn-group *name***
- Q3) Which ATM interface configuration command is used to set the VPI/VCI on a Cisco router?
- A) **encapsulation pvc 1/32**
 - B) **pvc 1/32**
 - C) **interface-dlci 1/32**
 - D) **vpi/vci 1/32**
- Q4) Which dialer interface command sets the maximum Ethernet payload size from 1500 to 1492?
- A) **mtu 1492**
 - B) **ip mtu 1492**
 - B) **1492 mtu**
 - C) no such command

Quiz Answer Key

Q1) D

Relates to: Configuration of a Cisco 827 Router as the PPPoE Client

Q2) B

Relates to: Configuration of PPPoE in a VPDN Group

Q3) B

Relates to: Configuration of a PPPoE Client

Q4) B

Relates to: Configuration of the PPPoE DSL Dialer Interface

Configuring DSL with PPPoA

Overview

DSL is an ideal solution for high bandwidth remote access to a central site.

Relevance

This lesson provides an overview of the concepts and configuration of PPPoA on a Cisco 827 router CPE.

Objectives

Upon completing this lesson, you will be able to:

- List the tasks required to successfully configure a Cisco 827 router for PPPoA DSL connection
- List and explain the commands required to configure an ATM interface for PPPoA
- List and explain the commands required to configure a dialer interface for PPPoA operations
- List and explain the commands required to configure PAT to scale DSL operations
- List and explain the commands required to configure a DHCP server to scale DSL operations

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Configuration of a PPPoA DSL Connection
- DSL Modulation Configuration
- Configuration of the DSL ATM Interface
- Configuration of the DSL Dialer Interface
- Configuration of PAT
- PAT Configuration Example
- DHCP to Scale DSL
- Configuration of a Static Default Route
- PPPoA Sample Configuration
- Summary
- Quiz

Configuration of a PPPoA DSL Connection

This topic provides a list of configuration tasks that are required to configure a PPPoA DSL connection. Configuring DSL requires global and interface configuration commands.

Configuration Tasks for DSL

Cisco.com

- **Configure the ATM Interface**
- **Configure a Dialer Interface**
- **Configure Port Address Translation**
- **Configure DHCP**
- **Configure a Static Default Route**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-2

Use the tasks listed here in addition to DDR-derived commands to configure DSL:

1. Configure the ATM interface (ADSL interface) of the Cisco 827 router with an ATM PVC and encapsulation. Specify the VCI/VPI that has been assigned by the service provider. Assign the ATM interface to a dialer pool.
2. Configure a dialer interface. Use IPCP IP address negotiation and PPP CHAP or PAP authentication.
3. Configure PAT.
4. Configure DHCP. The Cisco 827 router can be the DHCP server for the end-user PCs.
5. Configure a static default route.

DSL Modulation Configuration

This topic describes the **dsl operating-mode** command. Selecting the correct DSL modulation is crucial when configuring DSL.

DSL Modulation Configuration

Cisco.com

```
Router(config)#interface atm 0
Router(config-if)#dsl operating-mode auto
```

- **Permits the router to automatically determine the service provider's DSL modulation.**
- **This is the default setting on the Cisco router.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.3

Use the **dsl operating-mode auto** interface configuration command to specify that the router will automatically detect the DSL modulation that the service provider is using and set the DSL modulation to match.

An incompatible DSL modulation configuration can result in failure to establish a DSL connection to the DSLAM of the service provider.

Configuration of the DSL ATM Interface

This topic lists and explains the command required to configure the ATM interface on the Cisco 827 ADSL router. In DSL, an ATM VC must be configured to communicate with the service provider.

Configure the DSL ATM Interface

Cisco.com

```
Router(config-if)#pvc 1/32
```

- **Create an ATM PVC for the router.**
NOTE: the PVC VPI/VCI must match the provider.

```
Router(config-atm-vc)#encapsulation aal5mux ppp dialer
```

- **Use the encapsulation command to identify the layer 2 encapsulation.**

```
Router(config-atm-vc)#dialer pool-member 1
```

- **Specify a dialer pool-member.**

NOTE: DSL only runs between the CPE and the DSLAM.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.4

Use the **pvc** interface configuration command with the VPI/VCI to set the VPI/VCI that is used by the DSL service provider, as shown in the table here. Settings for the VPI/VCI value on the Cisco 827 router must match the DSLAM of the service provider switch configuration. ATM uses the VPI/VCI to identify an ATM VC.

pvc Commands

Command	Description
vpi	Virtual path identifier from service provider
vci	Virtual circuit identifier from service provider

The encapsulation method must correspond with that configured on the aggregation router. The table here shows encapsulation commands.

Use the **dialer pool-member** command to specify which dialer interfaces may use the ATM physical interface on the Cisco router.

Encapsulation Commands

Command	Description
encapsulation aal5mux ppp dialer	Sets the encapsulation for PPPoA, which uses ATM adaptation layer 5 (AAL5) in the mux mode
dialer pool-member	Links the ATM interface to a dialer interface

Configuration of the DSL Dialer Interface

This topic lists and reviews the commands that are required for configuring the DSL dialer interface. After the ATM interface has been configured, the dialer interface must be configured.

Configuring the DSL Dialer Interface

Cisco.com

```
!  
interface ATM 0  
no ip address  
pvc 8/35  
    encapsulation aal5mux ppp dialer  
    dialer pool-member 1  
!  
interface dialer0  
ip address negotiated  
encapsulation ppp  
dialer pool 1  
no cdp enable  
ppp chap hostname cisco  
ppp chap password cisco  
!
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.5

Use the commands in the table for DSL dialer configuration.

Dialer Commands for DSL

Command	Description
ip address negotiated	Enables a dynamic address from the service provider aggregation router using IPCP. With IPCP, DSL routers automatically negotiate a globally unique (registered or public) IP address for the dialer interface from the aggregation router of the service provider.
encapsulation ppp	Specifies PPP encapsulation for the dialer interface.
dialer pool 1 <i>number</i>	Specifies to which pool the dialer interface is assigned. Links the dialer interface to the ATM interface.
no cdp enable	Stops CDP advertisements from going out the dialer interface.
ppp chap hostname	Specifies the hostname for CHAP authentication.
ppp chap password	Specifies the password for CHAP authentication.

Configuration of PAT

This topic describes how to configure address translations using PAT.

Configure PAT

Cisco.com

```
Router(config)#ip nat inside source list 101 interface
Dialer0 overload
```

- Enable dynamic translation of addresses using the assigned IP address of the Dialer0 interface.

```
Router(config)#access-list 101 permit ip 10.0.0.0
0.255.255.255 any
```

- Specify the addresses that may be translated.

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#ip nat outside
```

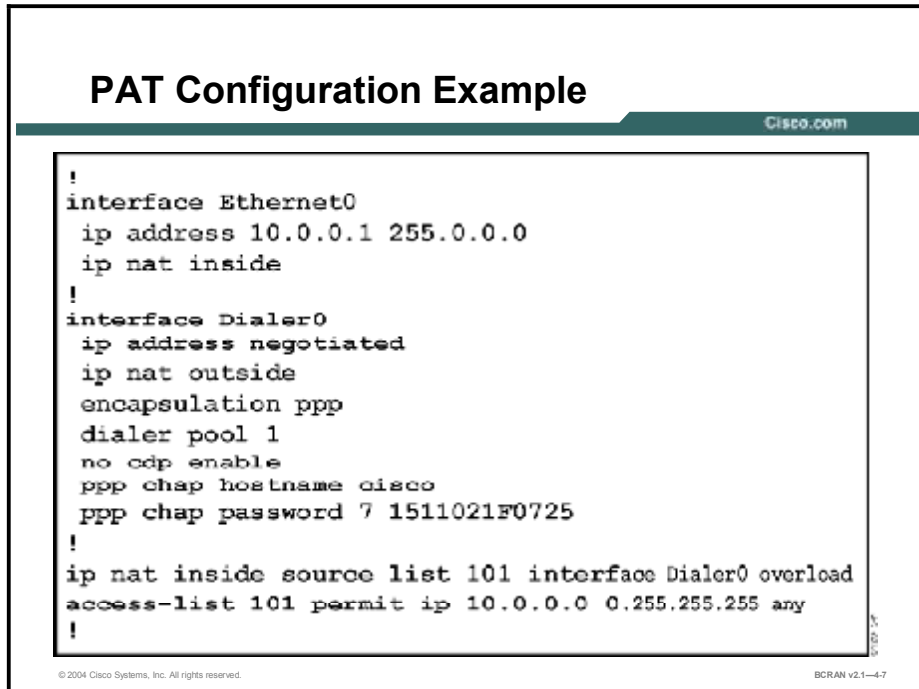
- Establish the Ethernet interface as inside and the Dialer interface as outside.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-6

NAT overload, commonly referred to as PAT, and PPP/PCP are popular techniques that are used to scale limited addresses. Using NAT overload means that you can use one registered IP address for the interface to access the Internet from all devices in the network.

PAT Configuration Example

This topic describes an example for configuring PAT.



```
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
!
interface Dialer0
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp chap hostname cisco
 ppp chap password 7 1511021F0725
!
ip nat inside source list 101 interface Dialer0 overload
access-list 101 permit ip 10.0.0.0 0.255.255.255 any
!
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4-7

The figure illustrates a sample PAT configuration on the Cisco 827 router.

The access list will match any source address in the 10.0.0.0 network.

In this example, the Dialer0 interface is the outside interface and the Ethernet0 interface is the inside interface.

The 10.x.x.x source addresses will be translated using PAT to the Dialer0 IP address. The Dialer0 interface receives its IP address from the service provider aggregation router using IPCP.

DHCP to Scale DSL

This topic describes how to scale DSL with DHCP.

Using DHCP to Scale DSL

Cisco.com

```
Router(config)#ip dhcp pool [pool name]
```

- Enable a DHCP pool for use by hosts

```
Router(dhcp-config)#import all
```

- Import DNS and WINS information from IPCP

```
Router(dhcp-config)#network [network address] [subnet mask]
```

- Specify the network and subnet mask of the pool

```
Router(dhcp-config)#default-router [host address]
```

- Specify the default router for the pool to use

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-8

The Cisco IOS DHCP Server feature is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router. After a DHCP client has booted, the client begins sending packets to the default router. The IP address of the default router should be on the same subnet as the client.

The Cisco IOS DHCP Server was enhanced to allow configuration information to be updated automatically. Network administrators can configure one or more centralized DHCP servers to update specific DHCP options within the DHCP pools. The remote servers can request, or “import” these option parameters from the central servers.

Configuration of a Static Default Route

This topic describes how to configure a static default route.

Configuring a Static Default Route

Cisco.com

```
Router(config)#ip route 0.0.0.0 0.0.0.0 dialer0
```

- **The CPE can use a static default route to reach all remote destinations**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.9

Configuring a static default route on the Cisco 827 router allows the router to reach all unknown destinations toward the dialer interface. In most DSL installations, the CPE will not be running a dynamic routing protocol to the aggregation router of the service provider. Therefore, a static default route is required on the Cisco 827 router.

When the PPP session has been established between the Cisco 827 router and the aggregation router of the service provider, the dialer interface IP address is assigned from the aggregation router of the service provider via IPCP. The aggregation router of the service provider will automatically build a host route to reach the Cisco 827 router dialer interface.

PPPoA Sample Configuration

This topic describes an example of a PPPoA configuration.

PPPoA Sample Configuration

Cisco.com

```
hostname delrouter
!
ip dhcp pool team1
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
!
del operating-mode auto
!
Interface ATM0/0
 no ip address
 pvc 1/32
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
```

```
interface Dialer0
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ip nat outside
 ppp chap hostname cisco
 ppp chap password 7 104D00A0618
!
ip nat inside source list 101
                interface Dialer0 overload
access-list 101 permit ip 10.0.0.0
                0.255.255.255 any
ip route 0.0.0.0 0.0.0.0 Dialer0
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4-10

The sample shows an example of the commands that are used for configuring PPPoA.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configuring DSL requires global and interface configuration commands.**
- **In DSL, an ATM VCI/VPI pair must be configured to communicate with the service provider.**
- **Once the ATM interface is configured, the dialer interface must be configured.**
- **The Cisco 827 router performs PAT and serves as a DHCP server for the end-user PCs.**
- **A static default routes is configured on the Cisco 827 router.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—4-11

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers follow in the Quiz Answer Key.

- Q1) When configuring DSL on a Cisco router, where does the information for the correct VCI/VPI come from?
- A) the DSL service provider
 - B) the DSL modem manufacturer
 - C) the local electronics retail store
 - D) can be any number that is locally assigned by the customer
- Q2) Which Cisco router command is used to permit the DSL router to determine modulation automatically?
- A) **dsl modulation auto**
 - B) **dsl operating-mode auto**
 - B) **dsl hub-type auto**
 - C) **dsl dmt-type auto**
- Q3) Which ATM interface configuration command is used to set the encapsulation method to PPPoA?
- A) **encapsulation aal5mux ppp dialer**
 - B) **encapsulation ppp**
 - C) **encapsulation pppoa**
 - D) **encapsulation aal5 dialer pool-member 1**
- Q4) Which dialer interface configuration command is used to stop CDP advertisements on a Cisco router?
- A) **no cdp run**
 - B) **no cdp enable**
 - C) **no cdp adv**
 - D) **cdp disable**

Quiz Answer Key

Q1) A

Relates to: Configuration of a PPPoA DSL Connection

Q2) B

Relates to: DSL Modulation Configuration

Q3) A

Relates to: Configuration of the DSL ATM Interface

Q4) B

Relates to: Configuration of the DSL Dialer Interface

Troubleshooting DSL

Overview

The lesson presents some common reasons why the ADSL connection might fail to be established and describes how to repair the connection if it fails.

Relevance

This lesson provides an overview of troubleshooting methods for Layer 1 and Layer 2.

Objectives

Upon completing this lesson, you will be able to:

- List the tasks required to troubleshoot Layer 1 (physical) issues
- List the tasks required to troubleshoot Layer 2 (data link) issues

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Layer Troubleshooting
- Layer 1 Issues
- Administratively Down State for an ATM Interface
- Correct Power Supply
- Correct DSL Operating Mode
- Layer 2 Issues
- Data Received from the ISP
- Proper PPP Negotiation
- Summary
- Quiz

Layer Troubleshooting

This topic describes the first troubleshooting step, determining which layer of the ADSL service is failing. There could be many reasons why the DSL connection might not be functioning properly.

Determining the Layer to Troubleshoot

Cisco.com

```
827-1#show dsl int atm 0

Modem Status: ATU-R (DS)          ATU-C (US)
                Showtime (DMTDSL_SHOWTIME)
DSL Mode:      ITU G.992.1 (G.DMT)
ITU STD NUM:   0x01                0x1
Vendor ID:     'ALCB'              'GSPN'
Vendor Specific: 0x0000            0x0002
Vendor Country: 0x00                0x00
Capacity Used: 97%                 100%
Noise Margin:  5.0 dB              6.0 dB
Output Power:  9.5 dBm             12.0 dBm
<output omitted>

Speed (kbps):      Interleave   Fast   Interleave   Fast
<output omitted> 7616           0     896           0
```

• Showtime will appear after the DSL modem has trained.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAM v2.1-4.2

Failure can occur at Layer 1, Layer 2, or Layer 3. This topic focuses on Layer 1 and Layer 2.

To troubleshoot Layer 1 problems, you can use the **show dsl interface atm 0** command to verify that the Cisco 827 router is trained to the DSLAM. If the router is successfully trained to the DSLAM, this command will also display the trained upstream and downstream speed in kbps.

If training is successful, the problem could be a Layer 2 problem.

If training is not successful, as shown in the following sample output, you must continue troubleshooting to isolate the Layer 1 problem.

```
827-1# sh dsl int atm 0
Line not activated: displaying cached data from last
activation
Log file of training sequence:
<output omitted>
```

Layer 1 Issues

This topic describes the steps that are used to determine whether Layer 1 is the cause of the problem.

Layer 1 Issues

Cisco.com

- **Is the Carrier Detect (CD) light on the front panel of the Cisco 827 on or off?**
 - If the CD light is on, go to the **Layer 2 Issues** section of this document.
 - If the CD light is off, continue with the next question.
- **Is your service provider using a DSLAM that supports the Alcatel DSL chipset? Does the modulation match with what the DSLAM is using?**
 - Verify this information with your service provider.
- **Is the DSL (ATM) port on the back of the Cisco 827 plugged into the wall jack?**
 - If the DSL (ATM) port is not plugged into the wall jack, connect the port to the wall with a 4-pin or 6-pin RJ-11 cable. This is a standard telephone cable.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.3

If the ATM 0 interface status is down and down, the router is not seeing a carrier on the ADSL line. To determine the ATM 0 interface status, issue the **show interface atm 0** command from enable mode of the router:

```
Router# show interface atm 0
ATM0 is down, line protocol is down
```

This message generally indicates one of two issues:

1. The active pins on the DSL wall jack may be incorrect.
2. The service provider may not be providing DSL service on this wall jack.

Determine whether the cable pinout is correct.

Cisco 827 Router xDSL Port Pinouts

Pin	Description
3	XDSL_Tip
4	XDSL_Ring

The RJ-11 connector provides an xDSL connection to external media via a standard RJ-11 6-pin modular jack. If the ATM interface is down and down, not just administratively down, check the pinout of the DSL wall jack. The Cisco 827 router uses a standard RJ-11 cable to provide the ADSL connection to the wall jack. The center pair of pins on the RJ-11 cable is used to carry the ADSL signal (pins 3 and 4 on a 6-pin cable, or pins 2 and 3 on a 4-pin cable).

If the correct pins on the wall jack are being used, and the ATM 0 interface is still down and down, replace the RJ-11 cable between the DSL port and the wall jack.

If the interface is still down and down after you have replaced the RJ-11 cable, contact the service provider to verify that ADSL service has been enabled on the wall jack that is being used.

Administratively Down State for an ATM Interface

This topic describes troubleshooting situations where the interface is down because of an administrative action.

Is the ATM Interface in an Administratively Down State?

Cisco.com

```
Router#show interface
atm 0 ATM0 is administratively down, line protocol is down
<...output.omitted ...>
```

If the ATM0 interface status is administratively down, issue the `no shutdown` command under the ATM0 interface.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface atm 0
Router(config-if)#no shut
Router(config-if)#end
Router#copy run start
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.4

To determine if the ATM 0 interface is administratively down, issue the commands shown in the figure in enabled mode.

Correct Power Supply

This topic discusses checking for the correct power supply.

Is the Correct Power Supply Being Used?

Cisco.com

- **To determine the correct power supply, on the back of the power adapter look for:**
 - Output +12V 0.1A, -12V 0.1A, +5V 3A, -24V 0.12A, and -71V 0.12A.
- **If the power supply is missing the +12V and -12V feeds, then it is for a different Cisco 800 series router and will not work on the 827.**
- **Note that if using the wrong power supply, the Cisco 827 will power up but will be unable to train up (connect) to the ISP DSLAM.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-4-5

If the DSL cable is good and the proper pinouts are being used, the next step is to make sure that the correct power supply for the Cisco 827 router is being used.

Note The Cisco 827 router does not use the same power supply as other Cisco 800 Series routers.

Correct DSL Operating Mode

This topic describes determining whether the DSL operating mode is correct.

Is the DSL Operating Mode Correct?

Cisco.com

- The command to configure operating-mode auto-detection is as follows:

```
Router#config t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#interface atm 0
Router(config-if)#dsl operating-mode auto
Router(config-if)#end
Router#copy run start
```
- The default operating mode for DSL is **AUTO**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.6

If everything that was checked up to this point in the Layer 1 troubleshooting procedure is correct, the next step is to make sure that the correct DSL operating mode is being used.

Cisco Systems recommends using the default **dsl operating-mode auto** command when the DSL modulation being used by the service provider is unknown.

Layer 2 Issues

This topic discusses Layer 2 troubleshooting issues.

Layer 2 Issues

Cisco.com

```
827#debug atm events
2d16h: Data Cell received on vpi = 2 vci =
      32 PPPoA MUX
2d16h: Data Cell received on vpi = 2 vci =
      32 PPPoA MUX
2d16h: Data Cell received on vpi = 2 vci =
      32 PPPoA MUX
```

- The `debug atm events` command shows the VPI/VCI values that the DSLAM expects.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.7

Complete the following steps to determine whether the correct VPI/VCI values are configured on the router.

Use the **debug atm events** command on the Cisco 827 router, and then go to a working Internet connection and begin to ping the static IP address assigned by your ISP. It is important that the ATM interface is up and up and that the IP address provided by the ISP is being pinged. Contact the ISP for support if the ping test is not successful.

Verify the VPI/VCI values, and then make the necessary changes to the configuration. If there is no output during 60 seconds of debugging, contact the ISP.

Note Use the Router# **undebug all** command to turn *off* the debug events.

Data Received from the ISP

This topic describes determining whether data is being received from the ISP.

Is Data Being Received from the ISP?

Cisco.com

```
Router#show int atm0
ATM0 is up, line protocol is up
Hardware is DSLAR (with Alcatel ADSL Module)
MTU 4470 bytes, sub MTU 4470, BW 128 Kbit, DLY 16000 usec, reliability
255/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Encapsulation(s): AAL5, PVC mode
24 maximum active VCs, 256 VCS per VP, 1 current VCs
VC idle disconnect time: 300 seconds
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queuing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 5 bits/sec, 0 packets/sec
5 minute output rate 7 bits/sec, 0 packets/sec
100 packets input, 5500 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
250 packets output, 1400 bytes, 0 underruns
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-4.8

If the correct VPI/VCI values are being used, the next step is to verify that data is being sent and received on the ATM interface. Issue the **show int atm0** command and check the input and output packet.

If the packet counters are incrementing in both directions, the router should be sending and receiving packets from the ISP.

If packets are incrementing in both directions, continue with the troubleshooting steps in this lesson.

Proper PPP Negotiation

This topic describes determining whether PPP is negotiating successfully.

Is PPP Negotiating Successfully?

Cisco.com

```
Router#debug ppp negotiation
PPP protocol negotiation debugging is on
Router# 2w3d: Vll PPP: No remote authentication for call-out
2w3d: Vll PPP: Phase is ESTABLISHING
2w3d: Vll LCP: O CONFREQ [Open] id 146 Len 10
2w3d: Vll LCP: MagicNumber 0x00CF0E1E (0x050680CF0E1E) 2w3d: Vll LCP: O
CONFACK [Open] id 102 Len 15
2w3d: Vll LCP: AuthProto CHAP (0x0305C22305)
2w3d: Vll LCP: MagicNumber 0xB945AD0A (0x050680945AD0A)
2w3d: Da1 IPCP: Remove route to 20.20.2.1
2w3d: Vll LCP: I CONFACK [ACKsent] id 146 Len 10
2w3d: Vll LCP: MagicNumber 0x00CF0E1E (0x050680CF0E1E)
2w3d: Vll LCP: State is Open
2w3d: Vll PPP: Phase is AUTHENTICATING, by the peer
2w3d: Vll CHAP: I CHALLENGE id 79 Len 33 from "6400-J-NRP-2"
2w3d: Vll CHAP: O RESPONSE id 79 Len 28 from "John"
2w3d: Vll CHAP: I SUCCESS id 79 Len 4
2w3d: Vll PPP: Phase is UP
<.output..omitted.>
2w3d: Vll IPCP: State is Open
Router#
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-4.9

There are four main points of failure in a PPP negotiation:

1. No response from the remote device (ISP)
2. LCP not open
3. PAP or CHAP authentication failure
4. IPCP failure

If Layer 1 is up and if the correct VPI/VCI is being used, the next step is to make sure that PPP is coming up properly. Run a series of debug commands on the Cisco 827 router and interpret the output. The primary debug command to use is the **debug ppp negotiation** command. The output shown in the figure is an example of a successful PPP negotiation.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **First step in troubleshooting is to determine the Layer to troubleshoot.**
- **For layer 1**
 - **Is the ATM interface in an administratively down state?**
 - **Is the correct power supply being used?**
 - **Is the DSL operating mode correct?**
- **Layer 2 Issues**
 - **Are data being received from the ISP?**
 - **Are PPP negotiating successful?**
 - **Are the PAP username and password correct?**
 - **Are the CHAP username and password correct?**
- **Knowledge of troubleshooting show commands**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—4-10

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 4-1: E-Lab: Simulation for Configuring a Cisco 827 Router for NAT with PPPoA

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) If the CD LED on the front panel of the Cisco 827 router is *off*, at which layer should you be troubleshooting?
- A) Layer 1
 - B) Layer 2
 - C) Layer 3
 - D) Layer 4
- Q2) The Cisco 827 router uses which type of standard cable?
- A) crossover
 - B) RJ-45
 - C) RJ-11 (4-pin or 6-pin)
 - D) RJ-31x
- Q3) Routers in the Cisco 800 Series all use the same power supply.
- A) true
 - B) false
- Q4) When configuring operating mode autodetection, the router should be in which mode?
- A) #
 - B) (config)#
 - C) configure terminal
 - D) (config-if)#
- Q5) Which command is used to determine the VPI/VCI that the DSLAM expects?
- A) **show interface**
 - B) **debug atm events**
 - C) **show vlan**
- Q6) Use the **show int atm0** command to check which type of packets?
- A) input and output
 - B) input only
 - C) output only

Quiz Answer Key

- Q1) A
Relates to: Layer 1 Issues
- Q2) C
Relates to: Layer 1 Issues
- Q3) B
Relates to: Correct Power Supply
- Q4) D
Relates to: Correct DSL Operating Mode
- Q5) B
Relates to: Layer 2 Issues
- Q6) A
Relates to: Data Received from the ISP

Module 5

Virtual Private Networks

Overview

This module is an introduction to Virtual Private Network (VPN) concepts, processes, and procedures that are available on Cisco IOS software-based router products.

The lessons in this module focus primarily on IPsec encryption and Internet Key Exchange (IKE), although there is mention of other tunneling protocols and VPN alternatives. Procedures and labs focus on router-based tasks. Other products such as the Cisco PIX Firewall, VPN concentrator, and Unity VPN client are briefly mentioned.

Objectives

Upon completing this module, you will be able to:

- Describe the fundamental concepts of VPNs and tunneling, and define commonly used VPN terms
- Describe the fundamental concepts and operations used in Cisco IOS cryptosystems for encryption, authentication, and key management
- Identify the main IPsec technologies and the major tasks necessary to configure IPsec on Cisco routers
- Verify proper IPsec and IKE configuration with available Cisco IOS commands

Outline

The module contains these lessons:

- Identifying VPN Features
- Identifying Cisco IOS Cryptosystem Features
- Identifying IPsec Technologies
- Task 1: Preparing for IKE and IPsec
- Task 2: Configuring IKE
- Task 3: Configuring IPsec
- Task 4: Testing and Verifying IPsec

Identifying VPN Features

Overview

Virtual Private Networks (VPNs) provide the same secure site-to-site network connectivity for remote users over the Internet as they would over a secure private network. Enabling this secure connectivity requires policies and technologies for VPN cryptographic services to support user authentication, data integrity, and encryption. This lesson provides a high-level, conceptual overview of VPN alternatives, elements, and terms.

Relevance

This lesson helps the learner identify the various VPN alternatives, the network connectivity supported by each, and the main terminology used. The lesson offers the learner a knowledge baseline to use for understanding VPN and to set a foundation for more in-depth learning after this lesson.

Objectives

Upon completing this lesson, you will be able to:

- Define a VPN and describe its advantages over alternative WAN access technologies
- Describe the functions performed by encryption and network tunnels
- Describe the scenarios for using VPNs for remote access and site-to-site network traffic
- Identify the main components, or attributes, of VPN implementations
- Select the best VPN technology for providing network connectivity for VPN design scenarios
- Match key VPN terms with their definition or descriptions

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

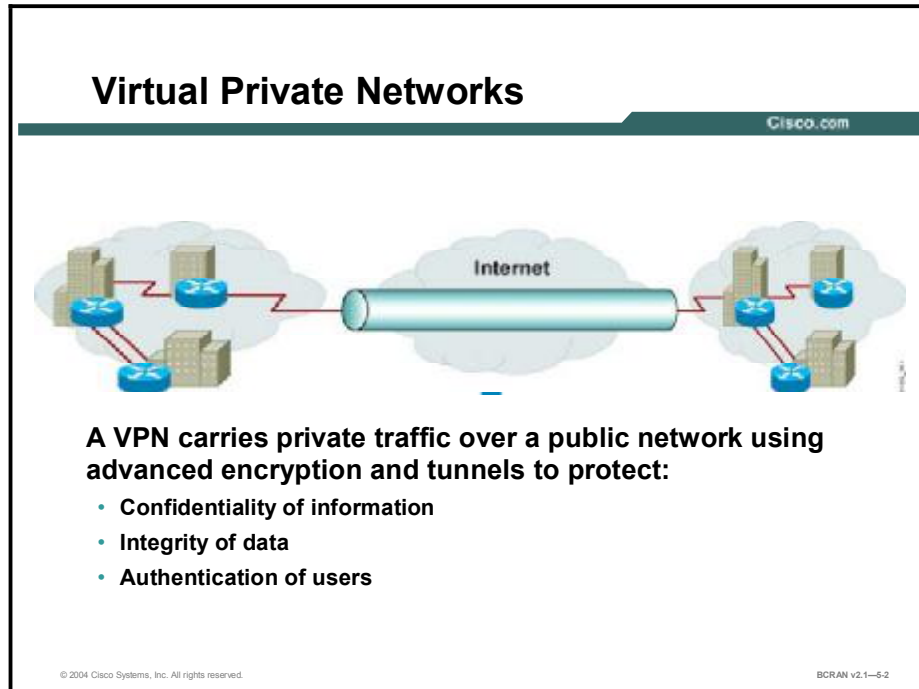
Outline

This lesson includes these topics:

- Overview
- VPN Features and Advantages
- Tunneling and Encryption
- VPN Usage Scenarios
- VPN Technologies
- VPN Protocols
- VPN and IPSec Terms
- Summary
- Quiz

VPN Features and Advantages

This topic describes the basic functions and advantages of VPNs.



A VPN is defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.

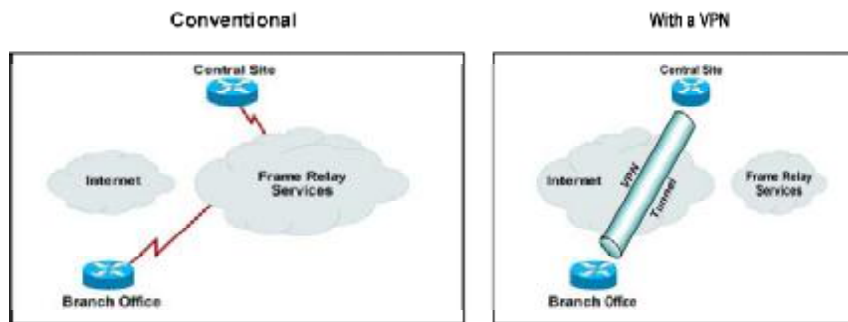
A VPN is established between two end systems, or between two or more networks. A VPN can be built using tunnels, encryption, or both, at essentially any layer of the OSI protocol stack. A VPN is an alternative WAN infrastructure that replaces or augments existing private networks that use leased-line or enterprise-owned Frame Relay ATM networks.

VPNs provide three critical functions:

- **Confidentiality (encryption):** The sender can encrypt the packets before transmitting them across a network, thereby prohibiting anyone from eavesdropping on the communication. If intercepted, the communication cannot be read.
- **Data integrity:** The receiver can verify that the data was transmitted through the Internet without being changed or altered in any way.
- **Origin authentication:** The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.

Why Have VPNs?

Cisco.com



- Higher cost
- Less flexible
- WAN management
- Complex topologies

- Lower cost
- More flexible
- Simpler management
- Tunnel topology

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—5-3

VPNs offer many advantages over traditional, leased-line networks. The primary benefits include the following:

- **Lower cost than private networks:** Total cost of ownership is reduced through lower-cost transport bandwidth, backbone equipment, and operations. Costs of LAN-to-LAN connectivity are typically reduced by 20 to 40 percent over domestic leased-line networks; cost reduction for remote access is in the range of 60 to 80 percent.
- **Flexibility for enabling the Internet economy:** VPNs are inherently more flexible and scalable network architectures than classic WANs, thereby enabling enterprises to quickly and cost-effectively extend connectivity. In this way, VPNs can facilitate connection or disconnection of remote offices, international locations, telecommuters, roaming mobile users, and external business partners as business requirements demand.
- **Simplified management burdens:** Enterprises may outsource some or all of their WAN functions to a service provider, enabling the enterprises to focus on core business objectives instead of managing a WAN or dial-access network.
- **Tunneled network topologies, thus reducing management burdens:** Using an IP backbone eliminates static permanent virtual circuits (PVCs) associated with connection-oriented protocols such as Frame Relay and ATM, thereby creating a fully-meshed network topology while actually decreasing network complexity and cost.

Virtual Private Networking

Cisco.com

- Virtual Network → Tunneling



- Private Network → Encryption



- Virtual Private Network = Tunneling + Encryption

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-5.4

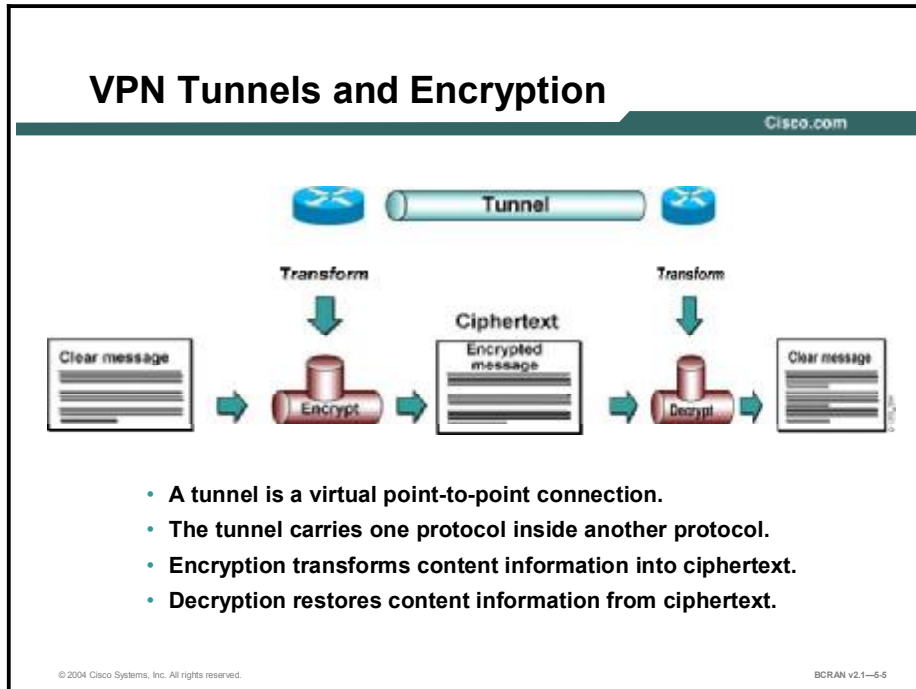
VPNs provide the greatest benefits of a private network, that is, privacy and the use of multiple protocols. VPNs enable these benefits over the larger shared IP infrastructure of the Internet.

A virtual network is created through the ability to tunnel multiple protocols over a standard IP connection. Generic routing encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) are two methods of tunneling. Both tunneling methods are configurable on Cisco routers. A third method, IPsec, is also configurable on Cisco routers and is the key focus of this VPN module.

A private network is one that ensures Confidentiality, Integrity, and Authentication (CIA). Encrypting traffic and using the IPsec protocol enables traffic to traverse the shared public infrastructure with the same CIA as with a private network.

Tunneling and Encryption

VPNs allow the creation of private networks across the Internet, enabling tunneling or encryption of TCP/IP (and non-TCP/IP) protocols. This topic describes tunneling and encryption.



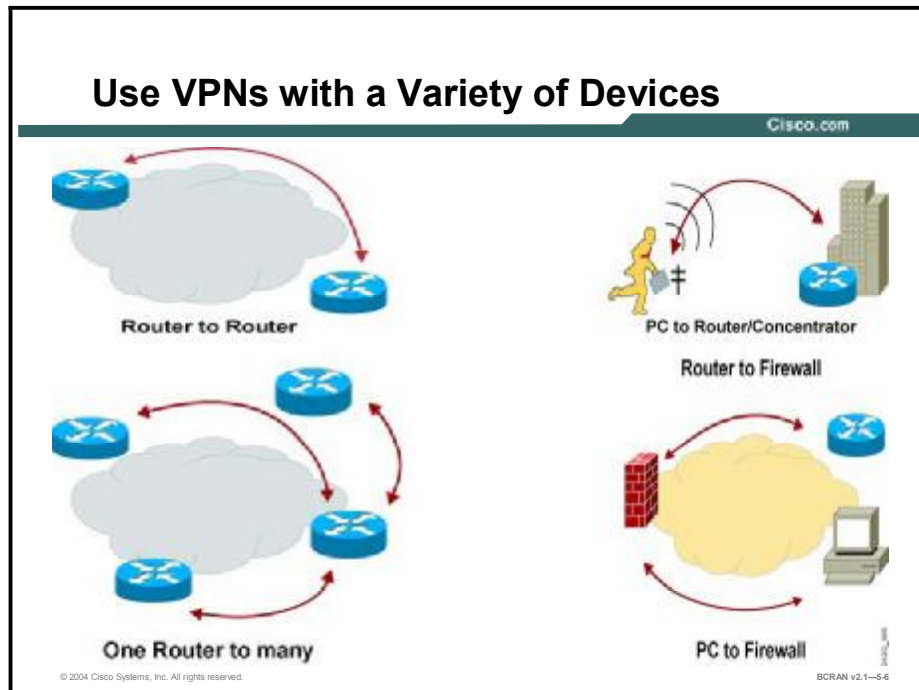
The Internet has created new opportunities for companies to streamline business processes, enter new markets, and work with partners and customers more effectively. At the same time, it has also created a greater reliance on networks and a need to protect against a wide range of security threats. The main function that a VPN offers for this protection is encryption through a tunnel.

Tunnels provide logical, point-to-point connections across a connectionless IP network, enabling application of advanced security features. Tunnels for VPN solutions employ encryption to protect data from being viewed by unauthorized entities and to perform multiprotocol encapsulation, if necessary. Encryption is applied to the tunneled connection to scramble data, thus making data legible to authorized senders and receivers only.

Encryption ensures that messages cannot be read by anyone but the intended recipient. As more information travels over public networks, the need for encrypting the information becomes more important. Encryption transforms content information into a ciphertext that is meaningless in its encrypted form. The decryption function restores the ciphertext back into content information intended for the recipient.

VPN Usage Scenarios

The topic describes the variety of options for deploying VPNs with modern networking devices and ecosystems. This topic also shows how VPN encryption and tunnels are used.



Networked VPN tunnels can carry encrypted data in four topologies:

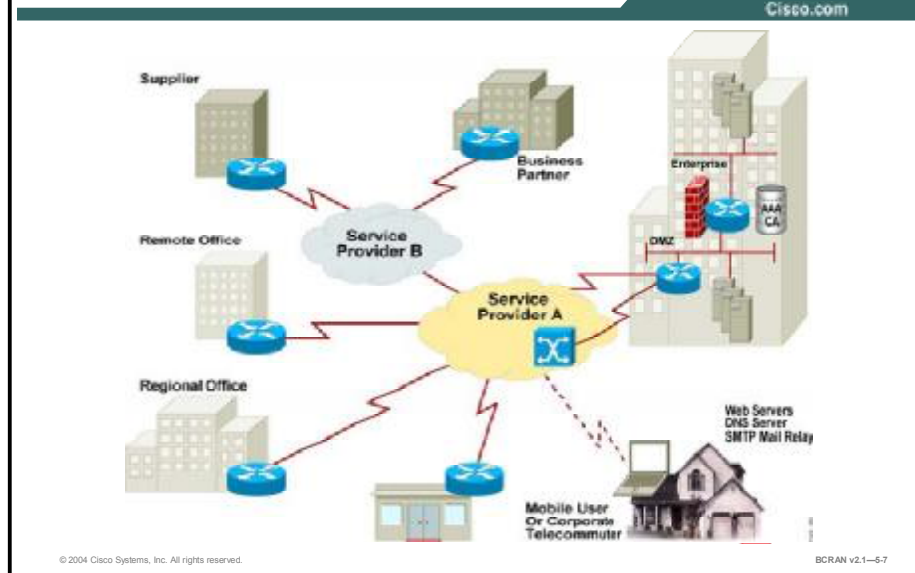
- **From router to router:** This is the focus of the BCRAN labs.
- **From one router to many other routers:** Each tunnel is a point-to-point connection.
- **From PC to router or VPN concentrator:** This option enables the mobility of network transactions.
- **Router to firewall and PC to firewall:** The firewall monitors traffic that crosses network perimeters and imposes restrictions according to security policy.

The proliferation of the networked economy supported by these and other network devices has spawned a fundamental change in how corporations conduct business. Corporate staff is no longer defined by where they do their jobs as much as how well they perform their job functions. Virtual Private Networking can be done from anywhere using routers, firewalls, or dedicated VPN concentrators.

Competitive pressures in many industries have spawned alliances and partnerships among enterprises, requiring separate corporations to act and function as one when facing customers.

Although such developments have increased productivity and profitability for many corporations, they have also created new demands on the corporate network. Connectivity that is focused solely on connecting fixed corporate sites—such as branch and regional offices connected to the headquarters campus—is no longer sufficient connectivity for many enterprises. In addition to these standard network connections, connectivity must focus on business-to-business and business-to-customer connections within an expanding ecosystem.

Cisco VPN Solution Ecosystem



VPNs help remote users, such as telecommuters and external business partners, to access enterprise computing resources. This access may use several service provider networks accessing and traversing the Internet.

There may be firewalls operating that help to separate the internal network of an enterprise from its extended external network and the Internet at large. The enterprise may offer a variety of web services and network applications, including those that use Domain Name System (DNS) and Simple Mail Transfer Protocol (SMTP).

The classic WAN must be extended to accommodate these new remote users. Consequently, many enterprises are using VPNs that help to complement their existing classic WAN infrastructure.

VPN solutions are organized into two main types:

- **Remote-access VPNs:** Securely connect remote users, such as mobile users and telecommuters, to the enterprise
- **Site-to-Site VPNs:** Securely connect remote and branch offices to the enterprise (intranet VPNs), and connect third parties, such as customers, suppliers, and business partners, to the enterprise (extranet VPNs).

VPN—Types

Cisco.com

- **Remote-access**
 - **Client-initiated**
 - **Network access server**
- **Site-to-site**
 - **Intranet**
 - **Extranet**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—5.8

There are two types of remote-access VPNs:

- **Client-initiated:** Remote users use clients to establish a secure tunnel across an ISP shared network to the enterprise.
- **Network access server (NAS)-initiated:** Remote users dial in to an Internet service provider (ISP). The NAS establishes a secure tunnel to the enterprise private network that might support multiple remote user-initiated sessions.

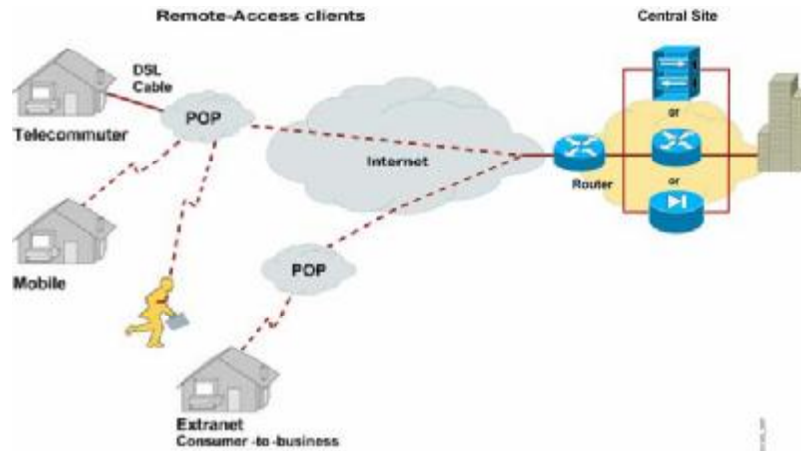
Site-to-site VPNs include two main types:

- **Intranet VPNs:** Connect corporate headquarters, remote offices, and branch offices over a public infrastructure.
- **Extranet VPNs:** Link customers, suppliers, partners, or communities of interest to a corporate intranet over a public infrastructure.

A more detailed description of the scenarios for these various VPN types will illustrate solutions and benefits.

Remote-Access VPN Solutions

Cisco.com



- VPN replacing toll and toll - free dial connectivity

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-5.9

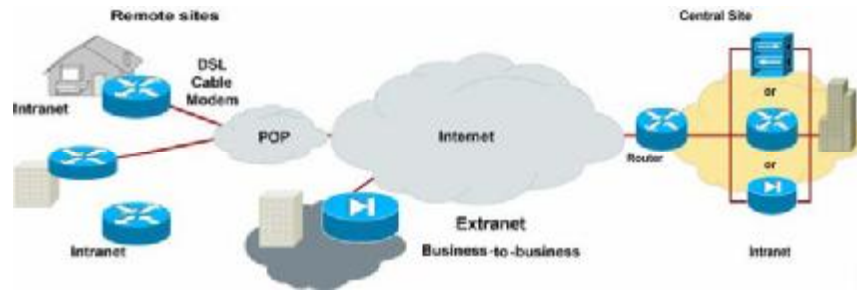
Remote-access VPN solutions are targeted to mobile users and home telecommuters. In the past, corporations supported remote users via dial-in networks, typically requiring a toll or toll-free call to access the corporation. Remote-access VPNs are an extension of dial networks.

With the advent of VPNs, mobile users can make a local call to their ISP to access the corporation via the Internet, regardless of their location.

Remote-access VPNs can terminate on headend devices such as Cisco routers, PIX Firewalls, or VPN concentrators. Remote-access clients can include Cisco routers and VPN clients.

Site-to-Site VPN Solutions

Cisco.com



- Extension of classic WAN

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-5-10

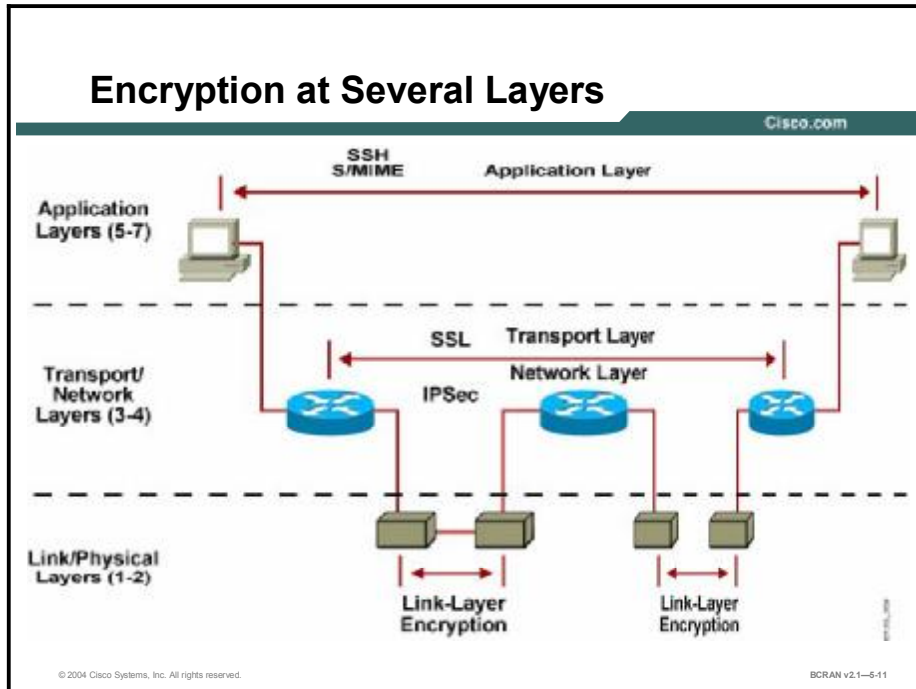
VPN site-to-site solutions can be used to connect corporate sites. In the past, a leased line or Frame Relay connection was required to connect sites. Today, most corporations have Internet access.

With Internet access, leased lines and Frame Relay lines can be replaced with site-to-site VPN to provide the network connection. VPN can support company intranets and business partner or customer extranets.

Site-to-site VPN is an extension of the classic WAN network. Site-to-site VPNs can be built using Cisco routers, PIX Firewalls, and VPN concentrators.

VPN Technologies

This topic describes the main VPN technologies that are available and compares them to the various Open System Interconnection (OSI) layers. The topic then focuses on the preferred layer for selecting a VPN technology and the preferred choices at that layer.



Various methods for VPN protection are implemented on different layers. Providing privacy and other cryptographic services at the application layer was very popular in the past, and in some situations is still done today. For example, Secure Shell Protocol (SSH) offers Internet-based data security technologies and solutions, especially cryptography and authentication products.

The Internet Engineering Task Force (IETF) has a standards-based protocol called Secure Multipurpose Internet Mail Extensions (S/MIME) for VPN applications generated by a number of communication system components (for example, message transfer agents, guards, and gateways).

However, application-layer security is application-specific and protection methods must be implemented anew in every application.

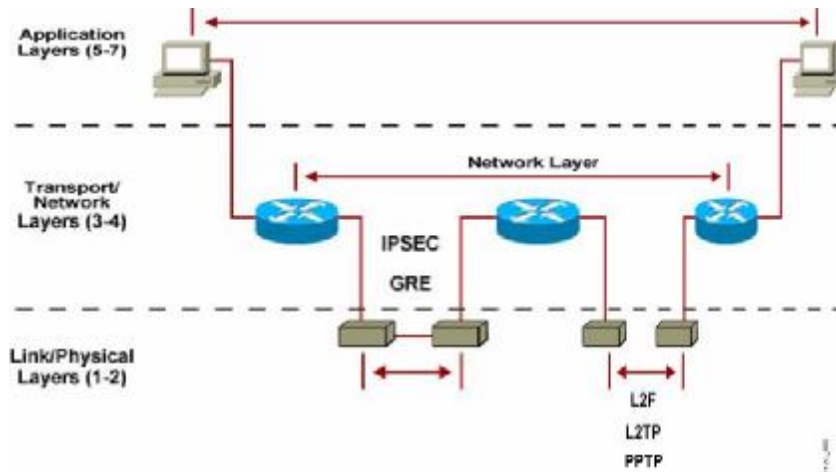
Some standardization has been successful at layer four (transport) of the OSI model, with protocols such as Secure Socket Layer (SSL) providing privacy, authenticity, and integrity to TCP-based applications. SSL is popular in modern e-commerce sites, but fails to address the issues of flexibility, ease of implementation, and application independence.

Protection at lower levels of the OSI stack, especially the data-link layer, was also used in communication systems of the past, as it provided protocol-independent protection on specific untrusted links. However, data-link layer protection is expensive to deploy on a large scale (protecting every link separately), therefore allowing a “man-in-the-middle” attack (hijacking a network session) on intermediate stations (routers).

Because of the limitations discussed, layer three has become the most popular level on which to apply cryptographic protection to network traffic.

Tunneling Protocols

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—5-12

With implementation of encryption on Layer 1, this layer and all layers above it are automatically protected. Network-layer protection offers one of the most flexible solutions, as it is media-independent and application-independent at the same time.

VPN Protocols

This topic describes a variety of network-layer technologies that are available to enable tunneling of protocols through networks to create a VPN. The main focus of this topic is on three of these technologies: Layer 2 Tunneling Protocol (L2TP), Cisco generic routing encapsulation (GRE), and the IPSec.

The screenshot shows a document titled "VPN Protocols" with the Cisco.com logo in the top right corner. Below the title is a table with three rows and three columns. The columns are labeled "Protocol", "Description", and "Standard". The rows list L2TP, GRE, and IPSec with their respective descriptions and RFC numbers. At the bottom left of the screenshot is the copyright notice "© 2004 Cisco Systems, Inc. All rights reserved." and at the bottom right is "BCRAN v2.1--6-13".

	Description	Standard
L2TP	Layer 2 Tunneling Protocol	RFC 2661
GRE	Generic Routing Encapsulation	RFC 1701 and 2784
IPSec	Internet Protocol Security	RFC 2401

The figure describes three VPN tunneling protocols: L2TP, GRE, and IPSec.

L2TP

Prior to the L2TP standard (August 1999), Cisco used Layer 2 Forwarding (L2F) as its proprietary tunneling protocol. L2TP is 100 percent backward-compatible with L2F. L2F is not forward-compatible with L2TP.

L2TP, defined in RFC 2661, is a combination of Cisco L2F and Microsoft Point-to-Point Tunneling Protocol (PPTP). Microsoft supports PPTP in its earlier versions of Windows, and PPTP and L2TP in Windows NT and 2000.

L2TP is used to create a media-independent, multiprotocol virtual private dialup network (VPDN). L2TP allows users to invoke corporate security policies across any VPN or VPDN link as an extension of their internal networks.

L2TP does not provide encryption and can be monitored with a protocol analyzer.

GRE

This multiprotocol transport encapsulates IP, Connectionless Network Protocol (CLNP), and any other protocol packets inside IP tunnels.

With GRE tunneling, a Cisco router at each site encapsulates protocol-specific packets in an IP header, creating a virtual point-to-point link to Cisco routers at other ends of an IP cloud where the IP header is stripped off.

By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment. GRE tunneling allows desktop protocols to take advantage of the enhanced route selection capabilities of IP.

GRE does not provide encryption and can be monitored with a protocol analyzer.

IPSec

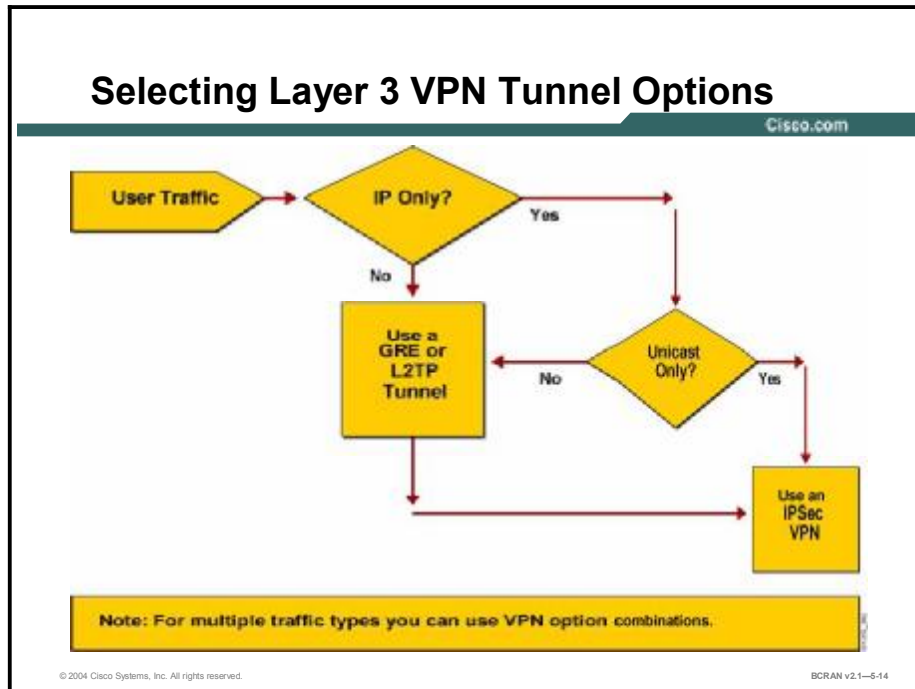
IPSec is the choice for secure corporate VPNs. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers.

IPSec provides these security services using Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec.

Selecting a VPN Technology

Depending on your traffic needs, select the best VPN technology to provide network connectivity.

The flow chart shows a process for selecting a network-layer VPN tunneling option that is based on your VPN design scenarios.



IPSec is the main option that is featured in this topic for securing enterprise VPNs. Unfortunately, IPSec supports IP unicast traffic only. If IP unicast packets are being tunneled, then a single encapsulation provided by IPSec is sufficient and much less complicated to configure and troubleshoot.

For multiprotocol or IP multicast tunneling, you must use GRE or L2TP.

For network traffic that uses Microsoft networking, L2TP may be the best choice. Because of its ties to PPP, L2TP may also be suited for remote-access VPNs that require multiprotocol support.

GRE is best suited for site-to-site VPNs that require multiprotocol support. It is typically used to tunnel multicast packets such as routing protocols. GRE encapsulates all traffic, regardless of its source and destination.

Neither L2TP nor GRE tunneling protocols support data encryption or packet integrity. For these valuable functions, you must combine the protocol or protocols with IPSec. You can use IPSec in combination with L2TP or GRE protocols to provide IPSec encryption, such as L2TP/IPSec or GRE/IPSec.

VPN and IPSec Terms

This topic describes commonly used VPN and IPSec terms that will help you to make the best use of VPN and IPSec protocols.

Identifying Key VPN Terms

Cisco.com

- **Tunnel**
- **Encryption and decryption**
- **Cryptosystem**
- **Hashing**
- **Authentication**
- **Authorization**
- **Key management**
- **CA—certification authority service**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—5-15

These terms define key components and elements that can be commonly used in VPNs:

- **Tunnel:** A virtual point-to-point connection that is used in a network to carry traffic from one protocol (for example, encrypted ciphertext) encapsulated inside another protocol (for example, an IP packet).
- **Encryption and decryption:** Encryption is the process of transforming information content—called clear text or plain text—into a hidden form called ciphertext so that it will not be readable by unauthorized users. Decryption transforms ciphertext back into clear or plain text so that it is accessible for reading by authorized users.
- **Cryptosystem:** A system to accomplish encryption and decryption, user authentication, hashing, and key-exchange processes. A cryptosystem may use one of several different methods, depending on the policy intended for various user traffic situations.
- **Hashing:** A data integrity technology that uses a formula or algorithm to convert a variable-length message and shared secret key into a single fixed-length string of digits, or hash. The message, key, and hash traverse the network from source to destination. At the destination, the recalculated hash is used to verify that the message and key have not changed while traversing the network.
- **Authentication:** The process of identifying a user or process attempting to access a computer system or network connection. Authentication ensures that the individual or process is who they claim to be. Authentication does not confer associated access rights.
- **Authorization:** The process of giving authenticated individuals or processes access to a computer system or network connection resources.

- **Key management:** A key is information (usually a sequence of random or pseudorandom binary digits) that is used initially to set up and then to periodically change the operations that are performed in a cryptosystem. Key management is the supervision and control of the process whereby keys are generated, stored, protected, transferred, loaded, used, and destroyed.
- **Certification authority (CA) service:** A third-party service that is trusted to help secure the communications between network entities or users by creating and assigning digital certificates (for example, public key certificates) for encryption purposes. A CA vouches for the binding between the data security items in the certificate. Optionally, a CA creates user encryption keys.

As the VPN of choice, IPSec uses a number of terms and acronyms, as noted here.

Identifying Key IPSec VPN Terms

Cisco.com

- **AH: Authentication Header**
- **ESP: Encapsulating Security Payload**
- **IKE: Internet Key Exchange**
- **ISAKMP: Internet Security Association and Key Management Protocol**
- **SA: security association**
- **AAA: authentication, authorization, and accounting**
- **TACACS+: Terminal Access Controller Access Control System Plus**
- **RADIUS: Remote Authentication Dial-In User Service**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1--5-16

These terms define key protocols and elements that are components of IPSec:

- **Authentication Header (AH):** A security protocol that provides data authentication, data integrity, and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).
- **Encapsulating Security Payload (ESP):** A security protocol that provides data confidentiality, data integrity, protection services, optional data origin authentication, and anti-replay services. ESP encapsulates the data to be protected.
- **IKE:** A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Oakley and Skeme each define a method to establish an authenticated key exchange. This includes payload construction, the information payloads carried, the order in which keys are processed, and how the keys are used.
- **Internet Security Association and Key Management Protocol (ISAKMP):** A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of an SA.
- **Security association (SA):** A policy and key or keys that are used to protect information. The ISAKMP SA is the shared policy and key or keys that are used by the negotiating peers in this protocol to protect their communication.
- **Authentication, authorization, and accounting (AAA):** The network security services that provide the primary framework through which you set up access control on your router or access server. Two major protocols that support AAA are TACACS+ and RADIUS.
- **TACACS+:** A security application that provides centralized validation of users attempting to gain access to a router or network access server.
- **RADIUS:** A distributed client-server system that secures networks against unauthorized access.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- A VPN carries private user traffic over the Internet, securing the traffic using encryption and tunneling.
- VPNs take advantage of cost, flexibility, management, and topology benefits compared to legacy WAN connections.
- Encryption converts clear text into cyphertext; cyphertext traverses the VPN tunnel.
- Decryption converts cypher text back into clear text.
- In VPN tunnels, one protocol carries traffic from another protocol for a variety of VPN usage scenarios.
- Remote-access VPN types evolve and extend dialup; Site-to-site VPN types extend classic WANs.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-5-17

Summary (Cont.)

Cisco.com

- VPN solution at the Network Layer 3 are recommended compared to application or data-link alternatives.
- L2TP is recommended for Microsoft Networks and traffic that can use PPP capabilities.
- GRE is recommended for multi-protocol traffic and for non-unicast traffic.
- IPSec, largely due to its encryption facilities is the VPN of choice and is recommended for unicast IP traffic.
- Combinations of IPSec with L2TP and GRE allow maximum VPN flexibility but can be complex to set up and manage.
- Knowing commonly-used VPN and IPSec terms or acronyms can help communications and simplify additional learning.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-5-18

References

For additional information, refer to these resources:

- IETF IPsec home page at <http://www.ietf.org/html.charters/ipsec-charter.html>
- Cisco.com Technologies section, “Security and VPN” category, at <http://www.cisco.com/>
- Federal Standard 1037C telecommunications glossary at <http://www.its.bldrdoc.gov/fs-1037/>
- Networking and Telecom definitions at <http://whatis.techtarget.com/>

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which of the following is NOT a reason for using VPN?
- A) VPNs provide secure communication over a public infrastructure.
 - B) VPNs reduce cost when compared to maintaining dedicated circuits.
 - C) VPNs allow users to shield information from others on the Internet.
 - D) VPNs allow communication at 20-40 percent faster rates than non-VPN connections.
- Q2) Tunnels permit which two of the following? (Choose two.)
- A) multiple protocols to cross an IP network
 - B) packet encryption to cross an IP network
 - C) packets to move faster through a congested network
 - D) overhead of packet size and process to be reduced
- Q3) Which of the following devices can terminate a VPN connection?
- A) Cisco firewall
 - B) Cisco router
 - B) Cisco VPN concentrator
 - C) all of the above
- Q4) Which of the following is NOT a benefit of Layer 3 (IPSec) encryption?
- A) Layer 3 encryption can be used independent of the type of application.
 - B) Layer 3 encryption hides the port number and the type of application being used.
 - C) Layer 3 encryption prevents intruders from seeing the addresses of the host conversations.
 - D) Layer 3 encryption is easily scalable.
- Q5) A GRE or L2TP tunnel can be encapsulated within an IPSec tunnel to keep data private.
- A) true
 - B) false

- Q6) If a corporate network uses a multicast protocol, how can traffic be sent securely from a corporate headquarters to a branch office?
- A) Multicast protocols natively control security between offices.
 - B) A GRE tunnel will provide adequate security.
 - C) An L2TP tunnel will provide adequate security.
 - D) A GRE tunnel encapsulated in IPSec will provide adequate security.
- Q7) A cryptosystem can best be defined as_____.
- A) a method of enabling two devices to negotiate security protocols
 - B) the ability to use a substance like Kryptonite to weaken security
 - C) the system of securing traffic by using encryption

Quiz Answer Key

- Q1) D
Relates to: VPN Features and Advantages
- Q2) A, B
Relates to: Tunneling and Encryption
- Q3) D
Relates to: VPN Usage Scenarios
- Q4) C
Relates to: VPN Technologies
- Q5) A
Relates to: VPN Technologies
- Q6) D
Relates to: VPN Technologies
- Q7) C
Relates to: VPN and IPSec Terms

Identifying Cisco IOS Cryptosystem Features

Overview

The Cisco IOS cryptosystem, which performs encryption, authentication, and key management, is a complex tool and supports many technologies.

Relevance

Understanding cryptosystem is helpful in understanding encryption and key exchanges.

Objectives

Upon completing this lesson, you will be able to:

- List the various encryptions, authentications, hash functions, and key management systems used in cryptography
- Describe the fundamentals of symmetric encryption (secret-key encryption)
- Describe the fundamentals of asymmetric encryption (public-key encryption)
- Identify the steps in a key exchange operation using the Diffie-Hellman algorithm
- Describe the fundamentals of hashing, including the HMAC-MD5 and HMAC-SHA-1 hashing algorithms

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

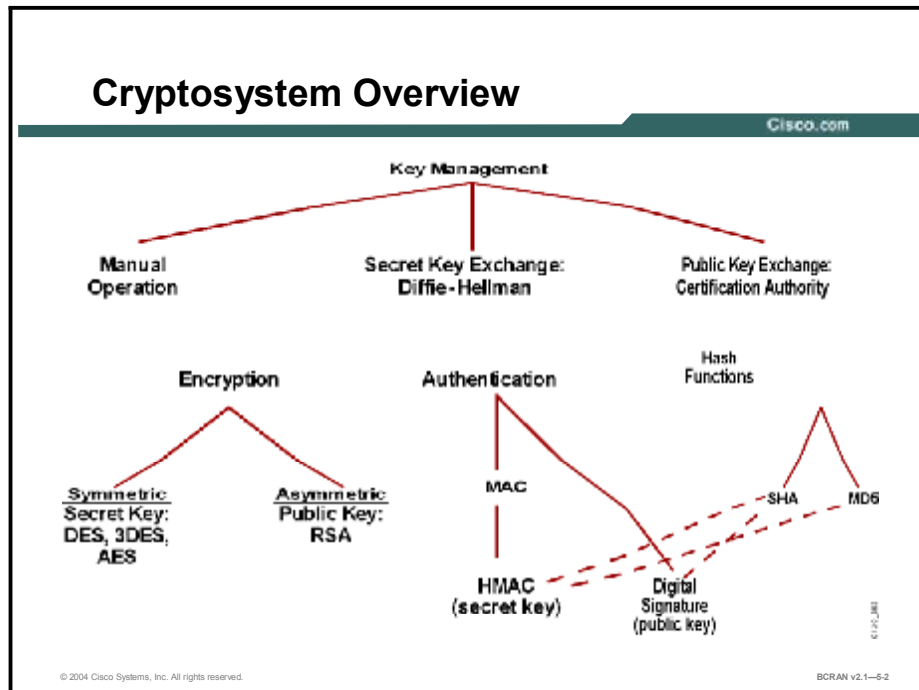
Outline

This lesson includes these topics:

- Overview
- Cryptosystem Overview
- Symmetric Encryption
- Asymmetric Encryption
- Key Exchange—Diffie-Hellman
- Hashing
- Summary
- Quiz

Cryptosystem Overview

This topic describes encryptions, authentications, hash functions, and key management systems that are used in cryptography.



There are numerous encryption technologies that are available to provide confidentiality, including Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). DES encrypts packet data with a 56-bit key. At its development in the 1970s, DES was thought to be unbreakable. Today, supercomputers can crack DES encryption in a few days. 3DES uses a double-length key (112 bits) and performs three DES operations in sequence. 3DES is 2^{56} times stronger than DES. AES currently specifies keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits (all nine combinations of key length and block length are possible). Cisco intends AES to be available on all Cisco products that currently have IPsec DES and 3DES functionality, such as Cisco IOS routers, Cisco Secure PIX Firewalls, Cisco VPN concentrators, and Cisco VPN clients.

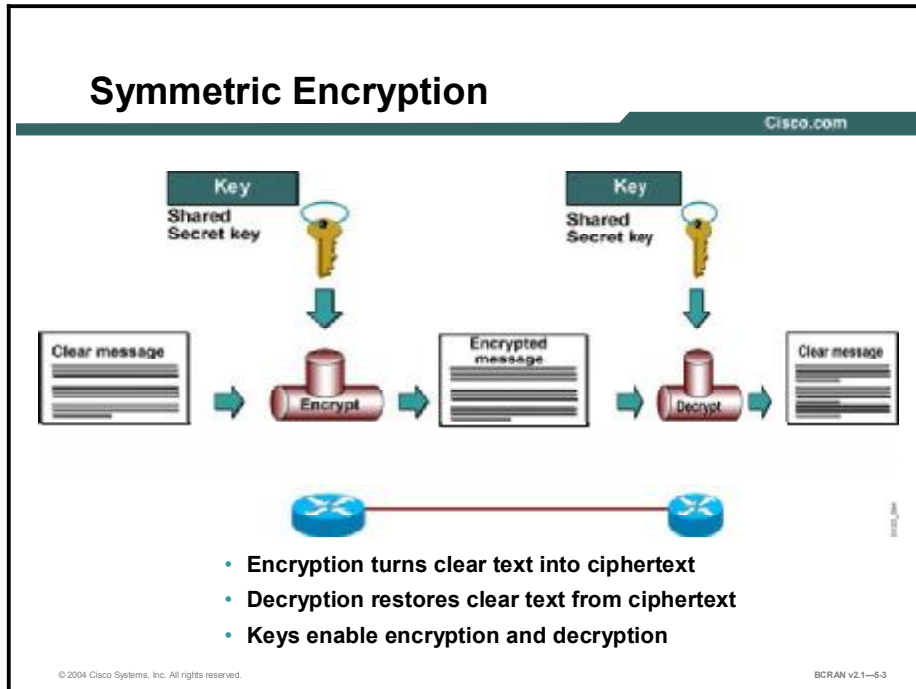
Many standards have emerged to protect the secrecy of keys and to facilitate the changing of these keys. Diffie-Hellman implements key exchange without exchanging the actual keys. This is the most well-known and widely used algorithm for establishing session keys to encrypt data.

Note Cisco IOS images with strong encryption are subject to United States government export controls and have a limited distribution. Please check license availability before installing an encryption technology. This course uses the less powerful DES rather than 3DES due to more flexible export restrictions.

Rivest, Shamir, and Adelman (RSA) is the public-key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA signatures provide nonrepudiation while RSA-encrypted nonces (randomly generated values) provide repudiation. There are several technologies that provide authentication, including message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA).

Symmetric Encryption

This topic describes the fundamentals of symmetric encryption (secret-key encryption).



The figure shows symmetric encryption, also known as secret-key encryption. It is used for large volumes of data. During the data exchange, the keys may change several times. Asymmetric encryption, or public-key encryption such as RSA, is several times more CPU-intensive, so it is usually used only for key exchanges.

With block ciphers, it is possible to further guarantee the integrity of the data received by using feedback. Cisco encryption algorithm incorporates cipher feedback (CFB), which does an Exclusive-OR of the plain text data with each block of encrypted data. CFB provides a means to verify that all data was received as transmitted.

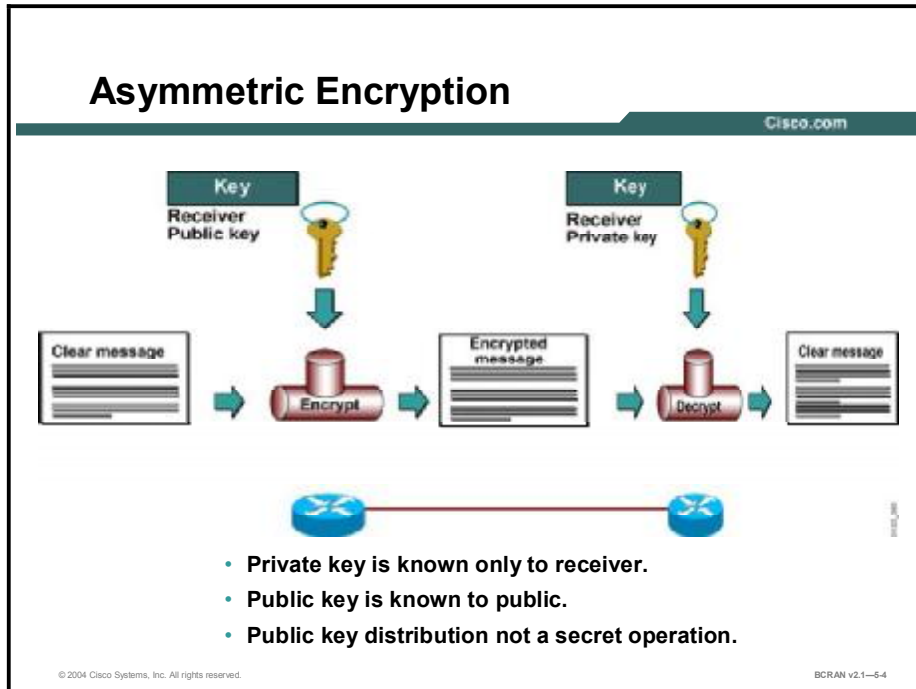
The most important feature of a cryptographic algorithm is its security against being compromised. The security of a cryptosystem, or the degree of difficulty for an attacker to determine the contents of the ciphertext, is the function of a few variables. In most protocols, the cornerstone to security lies in the secrecy of the key used to encrypt data. The DES algorithm is built so that it is too difficult for anyone to be able to determine the clear text without having this key. In any cryptosystem, great lengths are taken to protect the secrecy of the encryption key.

DES is one of the most widely used symmetric encryption standards. DES turns clear text into ciphertext via an encryption algorithm. The decryption algorithm on the remote end restores clear text from ciphertext. Keys enable the encryption and decryption. DES is the most widely used symmetric encryption scheme today. It operates on 64-bit message blocks. The algorithm uses a series of steps to transform 64-bit input into 64-bit output. In its standard form, the algorithm uses 64-bit keys, of which 56 bits are chosen randomly. The remaining eight bits are parity bits, one for each seven-bit block of the 56-bit random value.

3DES is an alternative to DES that preserves the existing investment in software but makes a brute-force attack more difficult. 3DES takes a 64-bit block of data and performs the operations of encrypt, decrypt, and encrypt. 3DES can use one, two, or three different keys. The advantage of using one key is that, with the exception of the additional processing time that is required, 3DES with one key is the same as standard DES (for backward compatibility). Although DES and 3DES algorithms are in the public domain and freely available, 3DES software is controlled by United States export laws.

Asymmetric Encryption

This topic describes the fundamentals of asymmetric encryption (public-key encryption).



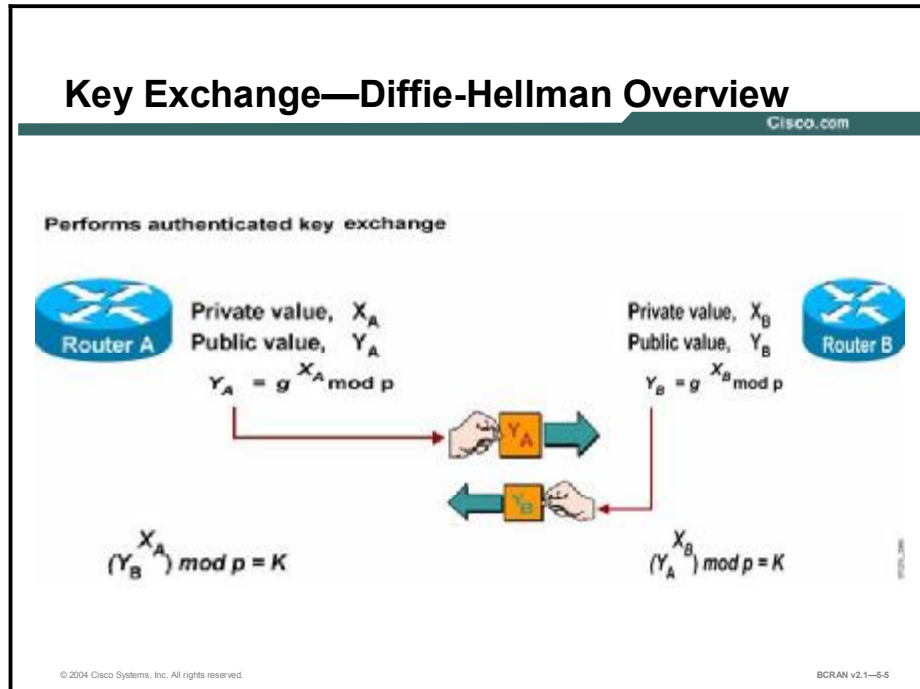
Asymmetric encryption is often referred to as public-key encryption. It can use either the same algorithm to encrypt and decrypt data, or different but complementary algorithms. Two different, but related, key values are required: a public key and a private key. For example, if Alice and Bob want to communicate using public-key encryption, both need a public-key and private-key pair. Alice has to create her public-key or private-key pair, and Bob has to create his own public-key or private-key pair. When communicating with each other securely, Alice and Bob use different keys to encrypt and decrypt data.

Although the mechanisms that are used to generate these public or private key pairs are complex, they result in the generation of two very large random numbers, one of which becomes the public key and the other the private key. Because these numbers must adhere to stringent mathematical criteria to preserve the uniqueness of each public or private key pair, generating these numbers is processor-intensive. Public-key encryption algorithms are rarely used for data confidentiality because of their performance constraints, but instead are typically used in applications involving authentication that uses digital signatures and key management.

Two common public-key algorithms are the RSA algorithm and the El Gamal algorithm.

Key Exchange—Diffie-Hellman

This topic describes the steps in a key exchange operation using the Diffie-Hellman algorithm.



One of the most important aspects of creating a secure VPN involves exchanging the keys. The Diffie-Hellman algorithm provides a way for two parties, Router A and Router B in the figure, to establish a shared secret key that only they know, even though they are communicating over an insecure channel.

This secret key is then used to encrypt data using their favorite secret-key encryption algorithm. Two numbers, “p” (a prime) and “g” (a number less than “p” but with some restrictions), are shared.

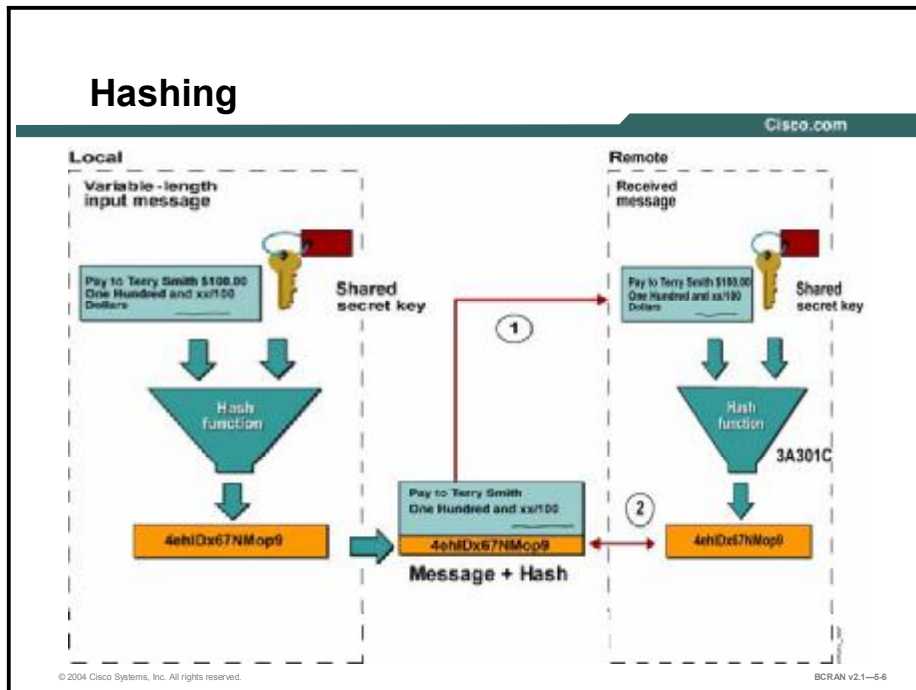
Router A and Router B each create a large random number that is kept secret, “ X_A ” and “ X_B .” The Diffie-Hellman algorithm is now performed, whereby both Router A and Router B carry out some computations and exchange results.

The final exchange results in a common value “K.” Anyone who knows “p” or “g” cannot guess or easily calculate the shared secret value—largely because of the difficulty in factoring large prime numbers.

It is important to note that a means for knowing with whom the key is established has not yet been created, so the exchange is subject to a “man-in-the-middle” attack (hijacking a network session between the source and destination). Diffie-Hellman provides for confidentiality but not for authentication. Authentication is achieved via the use of digital signatures in the Diffie-Hellman message exchanges.

Hashing

This topic describes the fundamentals of hashing, including the Hash-based Message Authentication Code (HMAC)-MD5 and HMAC-SHA-1 hashing algorithms.



Hashing guarantees the integrity of the message. At the local end, the message and a shared secret key are sent through a hash algorithm, which produces a hash value. Basically, a hash algorithm is a formula that is used to convert a variable-length message into a single string of fixed-length digits. It is a one-way algorithm. A message can produce a hash but a hash cannot produce the original message. It is analogous to dropping a plate on the floor. The plate can produce a multitude of pieces, but the pieces cannot be recombined to reproduce the plate in its original form. The message and hash are sent over the network.

At the remote end, there is a two-step process. First, the received message and shared secret key are sent through the hash algorithm, resulting in a recalculated hash value. Second, the receiver compares the recalculated hash with the hash that was attached to the message. If the original hash and the recalculated hash match, the integrity of the message is guaranteed. If any part of the original message is changed while in transit, the hash values are different.

There are two common hashing algorithms:

- **HMAC-MD5:** Uses a 128-bit shared secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.
- **HMAC-SHA-1:** Uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

HMAC-SHA-1 is considered cryptographically stronger than HMAC-MD5.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- In systematic encryption, clear text is turned into ciphertext, and then decrypted back into clear text, by use of keys.
- Asymmetric encryption uses either the same algorithm, or different but complementary algorithms, to scramble and unscramble data.
- The Diffie-Hellman algorithm provides a way for two parties to establish a shared secret key that only they know, while communicating over an insecure channel.
- A hash algorithm is a formula used to convert a variable-length message into a single string of digits of a fixed length.

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-7

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which technology can provide authentication?
- A) DES
 - B) Digital Signatures
 - C) Diffie-Hellman
 - D) RSA
- Q2) Symmetric encryption requires that the same key be used during encryption and decryption.
- A) true
 - B) false
- Q3) Which of the following is a form of asymmetric encryption?
- A) shared secret
 - B) RSA
 - C) SHA
 - D) MD5
- Q4) Diffie-Hellman provides for confidentiality and authentication.
- A) true
 - B) false
- Q5) What is the key size difference between HMAC-MD5 and HMAC-SHA-1?
- A) HMAC-MD5 = 64 bit, HMAC-SHA-1 = 128 bit
 - B) HMAC-MD5 = 128 bit, HMAC-SHA-1 = 160 bit
 - C) HMAC-MD5 = 160 bit, HMAC-SHA-1 = 128 bit
 - D) HMAC-MD5 = 128 bit, HMAC-SHA-1 = 64 bit

Quiz Answer Key

- Q1) B
Relates to: Cryptosystem Overview
- Q2) A
Relates to: Symmetric Encryption
- Q3) B
Relates to: Asymmetric Encryption
- Q4) B
Relates to: Key Exchange—Diffie-Hellman
- Q5) B
Relates to: Hashing

Identifying IPSec Technologies

Overview

IPSec is a set of security protocols and algorithms that are used to secure data at the network layer. Prior to the IPSec standard, Cisco implemented its proprietary Cisco Encryption Technology (CET) to provide protection at the packet level.

IPSec consists of two protocols and two protection modes. The first protocol is ESP, which encapsulates the data but does not provide protection to the outer headers. ESP encrypts the payload for data confidentiality, authenticity, and integrity. The second protocol is AH, which verifies the authenticity and integrity of the IP datagram by including a keyed MAC in the header.

Relevance

IPSec and the underlying protocols are important for establishing SAs as a way to secure all confidential communications running through insecure public networks.

Objectives

Upon completing this lesson, you will be able to:

- Describe the fundamentals of IPSec
- List the differences in how the ESP and AH are applied using transport mode and tunnel mode
- Describe the concepts of SAs
- List the five steps of IPSec operation
- Describe how IKE enhances IPSec
- Describe the IPSec process using SAs and CAs

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

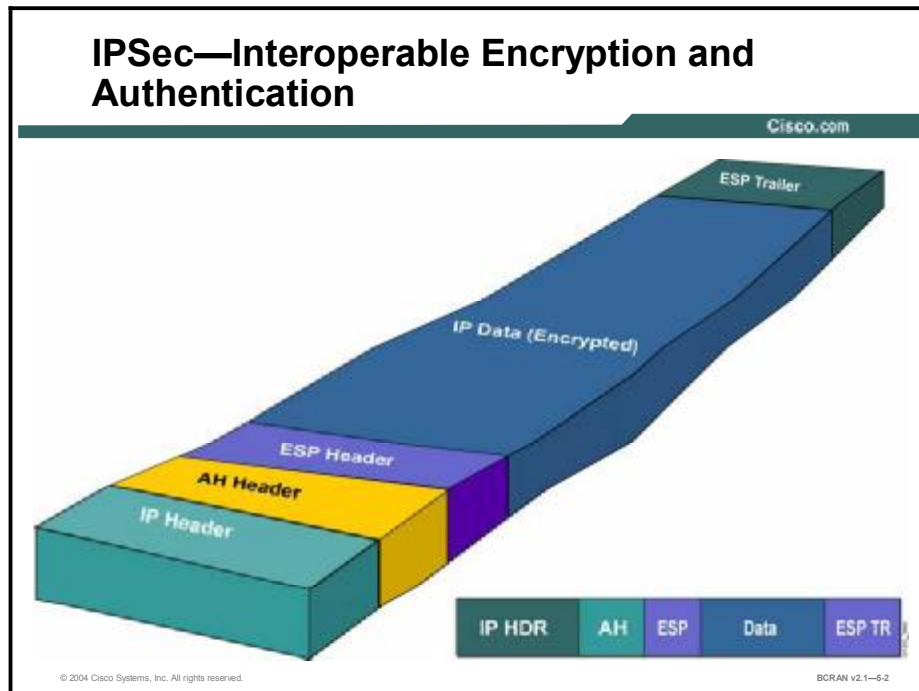
Outline

This lesson includes these topics:

- Overview
- IPsec
- Tunnel vs. Transport Mode
- Security Associations
- Five Steps to IPsec
- IPsec and IKE Relationship
- IKE and IPsec Flowchart
- Tasks to Configure IPsec
- Summary
- Quiz

IPSec

This topic describes the fundamentals of IPSec.



The IPSec feature is supported across Cisco IOS-based 1600, 2x00, 36x0, 4x00, 5x00, and 7x00 platforms using Cisco IOS Software Release 12.0(x), Cisco PIX Firewalls, and VPN Client and Concentrators.

RFC 2401 describes the general framework for this architecture. Like all security mechanisms, RFC 2401 helps to enforce a security policy. The policy defines the need for security on various connections—these will be IP sessions. The framework provides data integrity, authentication, and confidentiality, in addition to security association and key management.

Authentication Header

The IP AH is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays. The receiver can elect protection against replays when a security association is established. Although the default calls for the sender to increment the sequence number that is used for anti-replay, the service is effective only if the receiver checks the sequence number. AH, defined in RFC 2402, provides authentication for as much of the IP header as possible, in addition to upper-level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus, the protection provided to the IP header by AH is limited.

AH may be applied alone, in combination with the IP ESP, or in a nested fashion through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP may be used to provide the same security services, and it also provides a confidentiality (encryption) service. The primary difference between the authentication services provided by

ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless they are encapsulated by ESP (tunnel mode).

Encapsulating Security Payload

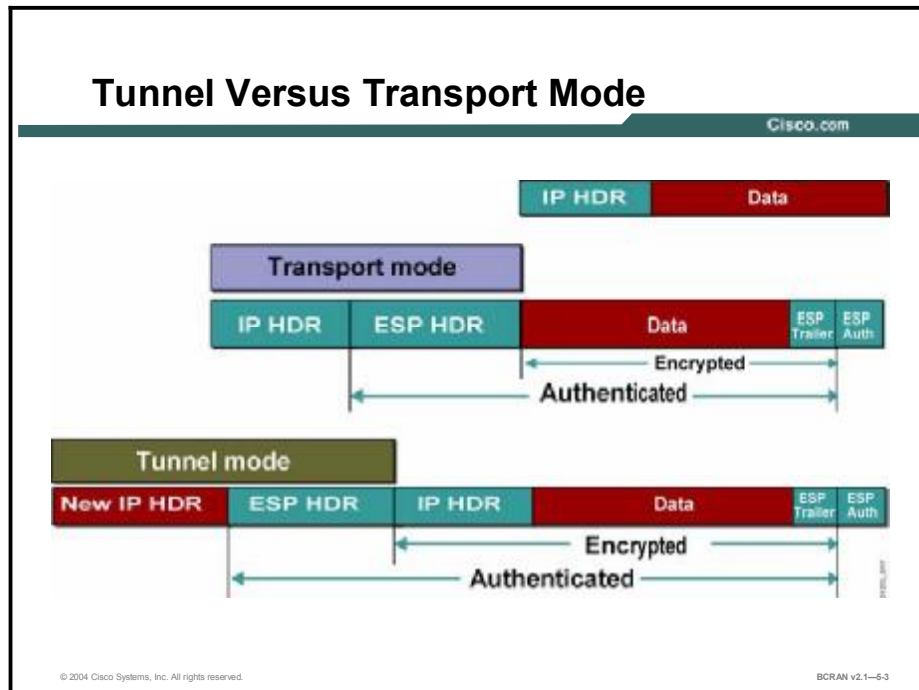
The ESP header is inserted after the IP header and before the upper-layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).

ESP, defined in RFC 2406, is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality by defeating traffic-flow analysis. The set of services provided depends on the options that are selected at the time of security association establishment and upon placement of the implementation. Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity or authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service.

Data origin authentication and connectionless integrity are joint services and are offered as an option in conjunction with (optional) confidentiality. The anti-replay service may be selected only if data origin authentication is selected, and its election is solely at the discretion of the receiver. Although the default calls for the sender to increment the sequence number that is used for anti-replay, the service is effective only if the receiver checks the sequence number. Traffic flow confidentiality requires the selection of tunnel mode, and is most effective if it is implemented at a security gateway, where traffic aggregation may be able to mask true source-destination patterns. Although both confidentiality and authentication are optional, at least one of them *must* be selected.

Tunnel vs. Transport Mode

This topic describes the differences in how the ESP and AH are applied using transport mode and tunnel mode.



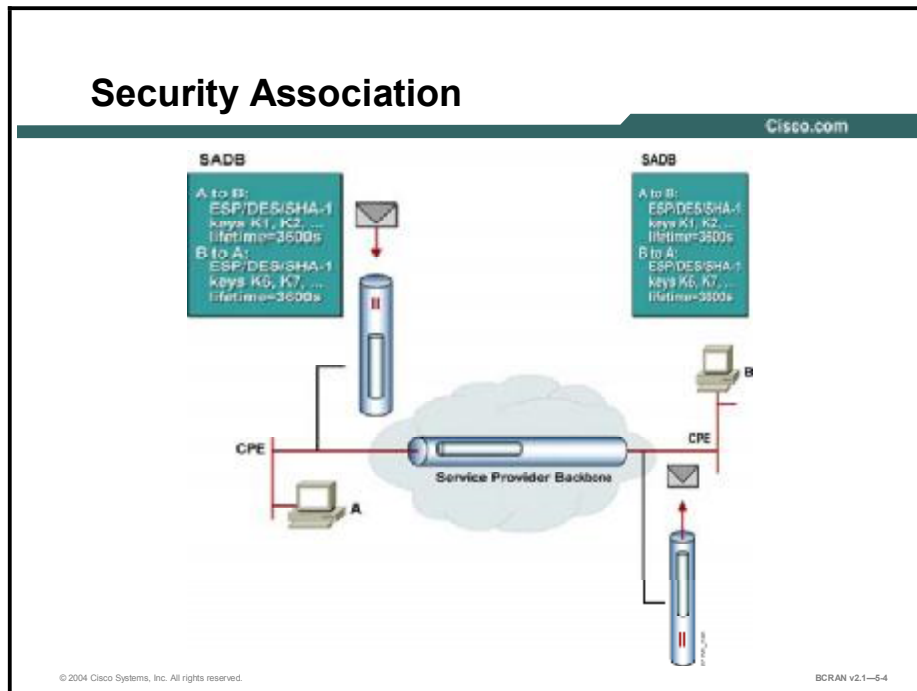
This figure shows an IPsec-protected path in basic scenarios in tunnel and transport modes. In transport mode, end hosts do IPsec encapsulation of their own data (host-to-host). Therefore, IPsec has to be implemented on end-hosts. The application endpoint must also be the IPsec endpoint. In tunnel mode, IPsec gateways provide IPsec services to other hosts in peer-to-peer tunnels, and end-hosts are not aware of the IPsec that are being used to protect their traffic. IPsec gateways provide transparent protection of other host traffic over untrusted networks.

ESP and AH can be applied to IP packets in two different ways, referred to as modes:

- **Transport mode:** In transport mode, security is provided for the upper protocol layers—transport layer and above only. Transport mode protects the payload of the packet but leaves the original IP address in the clear. The original IP address is used to route the packet through the Internet. ESP transport mode is used between hosts.
- **Tunnel mode:** Provides security for the whole original IP packet. The original IP packet is encrypted. Next, the encrypted packet is encapsulated in another IP packet. The outside IP address is used to route the packet through the Internet.

Security Associations

This topic describes the concepts of security associations.



SAs are one of the most basic concepts of IPsec. They represent a policy contract between two peers or hosts, and describe how the peers will use IPsec security services to protect network traffic. SAs contain all the security parameters that are needed to securely transport packets between peers or hosts, and they practically define the security policy used in IPsec.

The figure illustrates the concept of an SA. The routers in the figure use IPsec to protect traffic between hosts A and B, and therefore need two SAs (one in each direction) to describe traffic protection in both directions. Establishment of SAs is a prerequisite for IPsec traffic protection to work. When relevant SAs are established, IPsec refers to them for all parameters that are needed to protect a particular traffic flow. For example, an SA might enforce the following policy: “For traffic between hosts A and B use ESP 3DES with keys K1, K2, and K3 for payload encryption, SHA-1 with K4 for authentication...”

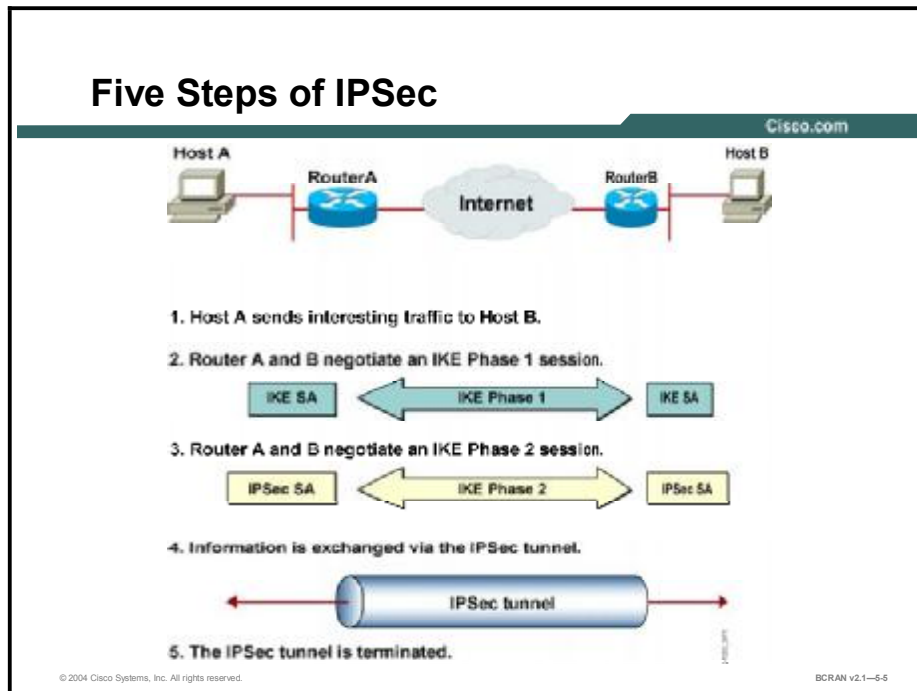
IPsec SAs always contain unidirectional (one-way) specifications. They are also encapsulation protocol specific. For each given traffic flow, there is a separate SA for each encapsulation protocol, AH and ESP. If two hosts A and B are communicating securely using both AH and ESP, then each host builds separate SAs (inbound and outbound) for each protocol. VPN devices store all their active SAs in a local database called the SA database.

An SA contains these security parameters:

- Authentication encryption algorithm, key length, and other encryption parameters (such as key lifetime, for example) that are used with protected packets.
- Session keys for authentication (HMACs) and encryption fed to the above algorithms. Those can be entered manually or negotiated automatically with the help of the IKE protocol.
- A specification of network traffic to which the SA will be applied (that is, all IP traffic, only TELNET sessions, and so forth).
- IPSec encapsulation protocol (AH or ESP) and mode (tunnel or transport).

Five Steps to IPSec

This topic describes the five steps of IPSec operation.

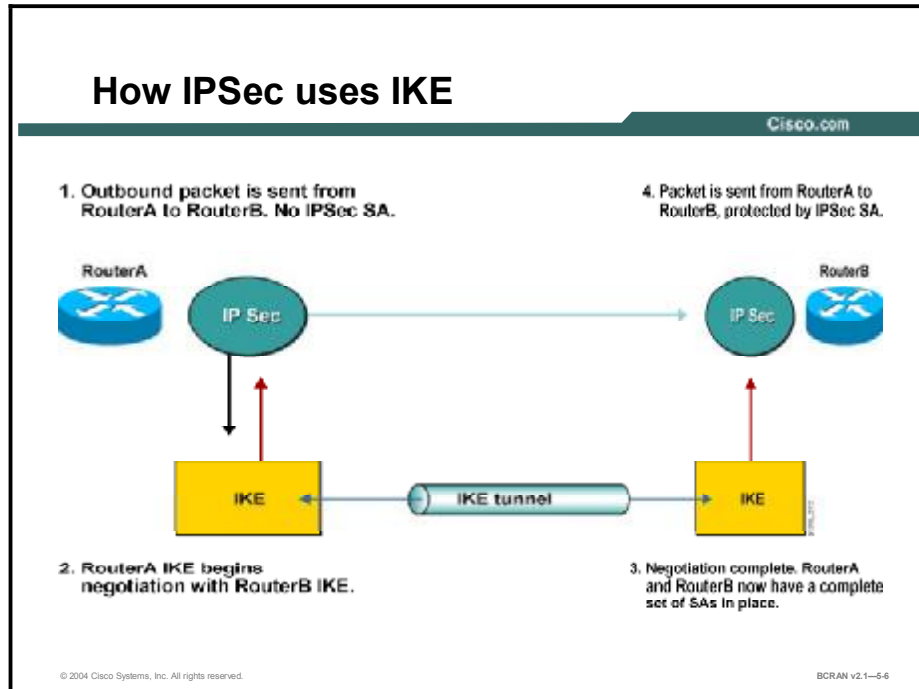


The goal of IPSec is to protect the desired data with the necessary security and algorithms. The figure shows only one of the two bidirectional IPSec SAs. IPSec operation can be broken down into five primary steps:

- Step 1** Interesting traffic initiates the IPSec process. Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send must be protected.
- Step 2** IKE Phase 1. IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure communications channel for negotiating IPSec SAs in Phase 2.
- Step 3** IKE Phase 2. IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages that are exchanged between endpoints.
- Step 4** Data transfer. Data is transferred between IPSec peers, based on the IPSec parameters and keys stored in the SA database.
- Step 5** IPSec tunnel termination. IPSec SAs terminate through deletion or by timing out.

IPSec and IKE Relationship

This topic describes how IKE enhances IPSec.



IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE, defined in RFC 2409, is a hybrid protocol which implements the Oakley and Skeme key exchanges inside the ISAKMP framework. ISAKMP is defined in RFC 2408. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec SAs.

The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects the data that A and B exchange.

IKE mode configuration allows a gateway to download an IP address (and other network-level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an *inner* IP address encapsulated under IPSec. This provides a known IP address for the client, which can be matched against IPSec policy.

This feature implements IKE mode configuration into existing Cisco IOS IPSec software images. Using IKE mode configuration, you can configure a Cisco access server to download an IP address to a client as part of an IKE transaction. IKE automatically negotiates IPSec SAs and enables IPSec secure communications without costly manual preconfiguration.

IKE provides these benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers
- Allows you to specify a lifetime for the IPSec SA
- Allows you to change encryption keys during IPSec sessions
- Allows IPSec to provide anti-replay services
- Permits CA support for a manageable, scalable IPSec implementation
- Allows dynamic authentication of peers

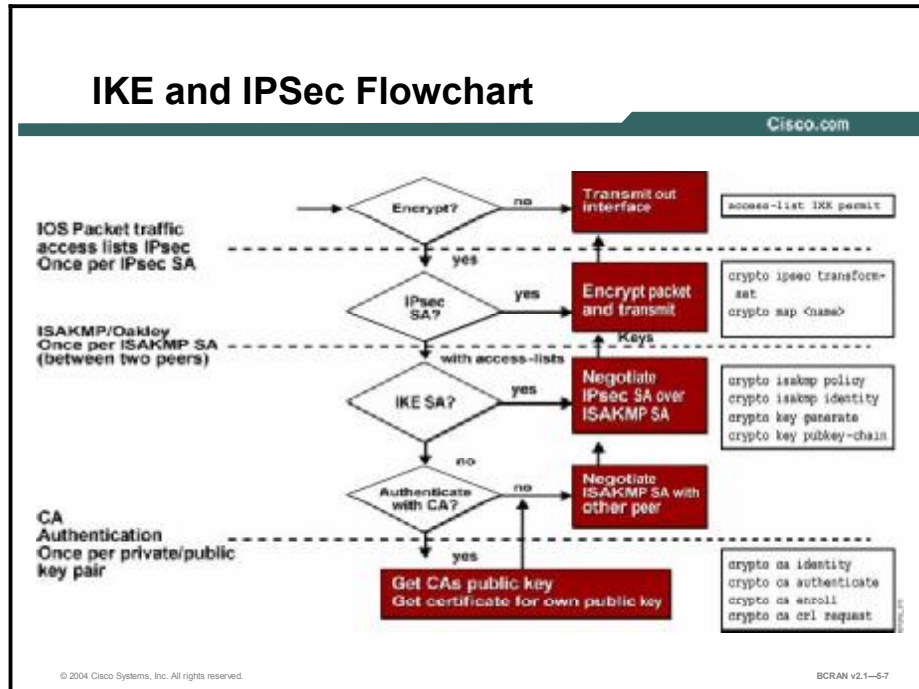
The component technologies implemented for use by IKE include:

- **DES:** DES is used to encrypt packet data. IKE implements the 56-bit DES-cipher block chaining (CBC) with explicit initialization value (IV) standard.
- **3DES:** 168-bit encryption.
- **AES:** Advanced Encryption Standard is the new standard that provides stronger encryption (128-bit, 192-bit, 256-bit) and is less CPU-intensive.
- **CBC:** Requires an IV to start encryption. The IV is explicitly given in the IPSec packet.
- **Diffie-Hellman:** A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.
- **MD5 (HMAC variant):** MD5 is a hash algorithm that is used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **SHA (HMAC variant):** SHA-1 is a hash algorithm that is used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **RSA signatures and RSA encrypted nonces:** RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA signatures provide nonrepudiation while RSA-encrypted nonces (uniquely occurring numbers) provide repudiation.

X.509v3 digital certificates are used with the IKE protocol when authentication requires public keys. This certificate support allows the protected network to scale by providing the equivalent of a digital ID card for each device. When two devices must communicate, they exchange digital certificates to prove their identity, thus removing the need to exchange public keys manually with each peer or to specify a shared key manually at each peer.

IKE and IPsec Flowchart

This topic describes the IPsec process using SAs and CAs.



IPsec in Cisco IOS software processes packets as shown in the figure. The process assumes that you have already created your own public and private keys, and that at least one access list exists. The steps are listed here:

- Step 1** Access lists applied to an interface and crypto maps are used by Cisco IOS software to select interesting traffic to be encrypted.
- Cisco IOS software checks to see if IPsec SAs have been established.
 - If the SA has already been established by manual configuration using the **crypto ipsec transform-set** and **crypto map** commands, or previously set up by IKE, the packet is encrypted based on the policy that is specified in the crypto map, and is transmitted out the interface.
- Step 2** If the SA has not been established, Cisco IOS software checks to see if an ISAKMP SA has been configured and set up. If the ISAKMP SA has been set up, the ISAKMP SA governs negotiation of the IPsec SA as specified in the ISAKMP policy configured by the **crypto isakmp policy** command. Then the packet is encrypted by IPsec and is transmitted.
- Step 3** If the ISAKMP SA has not been set up, Cisco IOS software checks to see if certification authority has been configured to establish an ISAKMP policy. If CA authentication is configured with **crypto ca** commands, the router uses public and private keys previously configured, gets the public certificate of the CA, gets a certificate for its own public key, uses the key to negotiate an ISAKMP SA, which in turn is used to establish IPsec SA. Finally, it encrypts and transmits the packet. This is usually a one-time enrollment process with the CA.

Tasks to Configure IPSec

This topic describes the tasks to configure IPSec.

Tasks to Configure IPSec

Cisco.com

Task 1 – Prepare for IKE and IPSec

- Step 1: Determine IKE (IKE Phase 1) policy**
- Step 2: Determine IPSec (IKE Phase 2) policy**
- Step 3: Check the current configuration**
- Step 4: Ensure that the network works without encryption**
- Step 5: Ensure that access lists are compatible with IPSec**

Task 2 – Configure IKE

- Step 1: Enable or disable IKE**
- Step 2: Create IKE policies**
- Step 3: Configure ISAKMP identity**
- Step 4: Configure preshared keys**
- Step 5: Verify IKE configuration**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5.8

Tasks to Configure IPSec (Cont.)

Cisco.com

Task 3 – Configure IPSec

- Step 1: Configure transform set suites**
- Step 2: Configure global IPSec lifeline**
- Step 3: Create crypto ACLs**
- Step 4: Create crypto ACLs using extended access lists**
- Step 5: Create crypto maps**
- Step 6: Configure IPSec crypto maps**

Task 4 – Test and Verify IPSec

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5.9

The use of IKE preshared keys for authentication of IPSec sessions is relatively easy to configure, yet does not scale well for a large number of IPSec clients.

The process for configuring IKE preshared keys in Cisco IOS software for Cisco routers consists of four major tasks. Subsequent lessons of this module discuss each configuration task in more detail. The four major tasks are as follows:

- **Task 1—Prepare for IPSec:** This task involves determining the detailed encryption policy. This includes identifying the hosts and networks that you must protect, determining details about the IPSec peers, determining the IPSec features that you need, and ensuring that existing ACLs are compatible with IPSec.
- **Task 2—Configure IKE:** This task involves enabling IKE, creating the IKE policies, and validating the configuration.
- **Task 3—Configure IPSec:** This task includes defining the transform sets, creating crypto ACLs, creating crypto map entries, and applying crypto map sets to interfaces.
- **Task 4—Test and verify IPSec:** Use **show**, **debug**, and related commands to test and verify that IPSec encryption works, and to troubleshoot problems.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **IPSec is a set of security protocols and algorithms used to secure data at the network layer.**
- **IPSec consists of the Encapsulating Security Payload (ESP) and Authentication Header (AH).**
- **Internet Key Exchange (IKE) enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—6-10

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) IPSec supports which two encapsulation protocols?
- A) MD5 and SHA-1
 - B) SH1 and ESP
 - C) ESP and AH
 - D) AH and MD5
- Q2) Transport mode provides protection for which layer and above?
- A) network
 - B) transport
 - C) session
 - D) application
- Q3) How many security associations are generated for IPSec tunnels between routers?
- A) 1
 - B) 2
 - C) 3
 - D) 4
- Q4) What is the first step in terminating an IPSec tunnel?
- A) IKE Phase 1 is negotiated.
 - B) IKE Phase 2 is negotiated.
 - C) IPSec peers terminate a tunnel.
 - D) Interesting traffic must be generated.
- Q5) Internet Key Exchange increases the functionality of IPSec.
- A) true
 - B) false
- Q6) To use IKE with IPSec, you must have a CA setup.
- A) true
 - B) false

- Q7) To configure IKE, you must enable IKE, create the IKE policies, and _____.
- A) apply crypto ACLs
 - B) validate the configuring
 - C) identify the host
 - D) use the **show** command

Quiz Answer Key

- Q1) C
Relates to: IPSec
- Q2) B
Relates to: Tunnel vs. Transport Mode
- Q3) C
Relates to: Security Associations
- Q4) D
Relates to: Five Steps to IPSec
- Q5) A
Relates to: IPSec and IKE Relationship
- Q6) B
Relates to: IKE and IPSec Flowchart
- Q7) B
Relates to: Tasks to Configure IPSec

Task 1: Preparing for IKE and IPSec

Overview

Successful implementation of an IPSec network requires advance planning before beginning the configuration of individual routers.

Relevance

Before configuring IPSec it is necessary to establish a proper IPSec security policy.

Objectives

Upon completing this lesson, you will be able to:

- Identify the steps in creating an IKE and IPSec security policy
- Describe the process for determining the IKE Phase 1 policy
- Define the IKE Phase 1 policy parameters
- Describe the process for determining the IKE Phase 2 policy
- Identify the IPSec transforms supported by Cisco IOS software
- Describe an example of an IPSec policy
- Describe the importance of identifying the IPSec peer
- Identify the commands that are used to check for existing IPSec security policies
- Identify the commands that are used to ensure connectivity between IPSec peers
- Describe how to ensure that access lists are compatible with IPSec

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Networking Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- IKE Creation and IPSec Security Policy
- Step 1: Determine IKE (IKE Phase 1) Policy
- IKE Phase 1 Policy Parameters
- Step 2: Determine IPSec (IKE Phase 2) Policy
- IPSec Transforms Supported in Cisco IOS Software
- IPSec Policy Example
- IPSec Peers
- Step 3: Check Current Configuration
- Step 4: Ensure That the Network Works
- Step 5: Ensure That Access Lists Are Compatible with IPSec
- Summary
- Quiz

IKE Creation and IPSec Security Policy

This topic identifies the steps for creating an IKE and IPSec security policy.

Task 1—Prepare for IKE and IPSec

Cisco.com

Task 1 – Prepare for IKE and IPSec

Step 1—Determine IKE (IKE Phase 1) policy.

Step 2—Determine IPSec (IKE Phase 2) policy.

Step 3—Check the current configuration.

show running-configuration

show crypto isakmp policy

show crypto map

Step 4—Ensure the network works without encryption.

ping

Step 5—Ensure access lists are compatible with IPSec.

show access-lists

Task 2 – Configure IKE

Task 3 – Configure IPSec

Task 4 – Test and Verify IPSec

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1–6.2

Configuring IPSec encryption can be complicated. You must plan in advance if you desire to configure IPSec encryption correctly the first time and minimize misconfiguration. You should begin this task by defining the IPSec security policy based on the overall company security policy. Some planning steps are as follows:

- Step 1 Determine IKE (IKE Phase 1) policy:** Determine the IKE policies between IPSec peers based on the number and location of the peers.
- Step 2 Determine IPSec (IKE Phase 2) policy:** Identify IPSec peer details such as IP addresses, IPSec transform sets, and IPSec modes. Then configure crypto maps to gather all IPSec policy details together.
- Step 3 Check the current configuration:** Use the **show running-configuration**, **show isakmp [policy]**, and **show crypto map** commands, and many other **show** commands to check the current configuration of the router. This is covered later in this lesson.
- Step 4 Ensure the network works without encryption (no excuses!):** Ensure that basic connectivity has been achieved between IPSec peers using the desired IP services before configuring IPSec. You can use the **ping** command to check basic connectivity.
- Step 5 Ensure that access control lists (ACLs) are compatible with IPSec:** Ensure that perimeter routers and the IPSec peer router interfaces permit IPSec traffic. In this step you need to enter the **show access-lists** command.

Step 1: Determine IKE (IKE Phase 1) Policy

This topic describes the process for determining the IKE Phase 1 policy

Step 1—Determine IKE (IKE Phase 1) Policy

Cisco.com

Determine the following policy details:

- **Key distribution method**
- **Authentication method**
- **IPSec peer IP addresses and hostnames**
- **IKE Phase 1 policies for all peers**
 - **Encryption algorithm**
 - **Hash algorithm**
 - **IKE SA lifetime**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5.3

Configuring IKE is complicated. You should determine the IKE policy details to enable the selected authentication method, and then configure it. Having a detailed plan reduces the chances of improper configuration. Some of the planning steps include:

- **Determine the key distribution method:** Determine the key distribution method that is based on the numbers and locations of IPSec peers. For a small network, you may want to manually distribute keys. For a larger network, you may want to use a CA server to support scalability of IPSec peers. You must then configure the ISAKMP to support the selected key distribution method.
- **Determine the authentication method:** Choose the authentication method that is based on the key distribution method. Cisco IOS software supports either preshared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using preshared keys.
- **Identify IPSec peer IP addresses and hostnames:** Determine details of all of the IPSec peers that will use ISAKMP and preshared keys for establishing SAs. You will use this information to configure IKE.

- **Determine ISAKMP policies for peers:** An ISAKMP policy defines a combination, or suite, of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins by each peer agreeing on a common (shared) ISAKMP policy. The ISAKMP policy suites must be determined in advance of configuration. You must then configure IKE to support the policy details that you determined. Some ISAKMP policy details include:
 - Encryption algorithm
 - Hash algorithm
 - IKE SA lifetime

The goal of this planning step is to gather the precise data that you will need in later steps to minimize misconfiguration.

IKE Phase 1 Policy Parameters

This topic describes the IKE Phase 1 policy parameters.

Parameter	Strong	Stronger
Encryption Algorithm	DES	3DES AES
Hash Algorithm	MD5	SHA-1
Authentication Method	Preshare	RSA Encryption RSA Signature
Key Exchange	D-H Group 1	D-H Group 2
IKE SA Lifetime	86400 seconds	<86400 seconds

© 2004 Cisco Systems, Inc. All rights reserved. BCRAV v2.1-54

An IKE policy defines a combination of security parameters that are used during the IKE negotiation. A group of policies make up a “protection suite” of multiple policies that enable IPSec peers to establish IKE sessions and establish SAs with a minimal configuration. The figure shows an example of possible combinations of IKE parameters to form either a strong or a stronger policy suite.

Create IKE Policies for a Purpose

Because IKE negotiations must be protected, each IKE negotiation begins with each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, an SA established at each peer identifies the security parameters of the policy. These SAs apply to all subsequent IKE traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer policy.

Define IKE Policy Parameters

You can select specific values for each IKE parameter, according to the IKE standard. You select one value over another based on the security level you want and the type of IPSec peer to which you will connect.

There are five parameters to define in each IKE policy, as shown in the figure and in the table here. The figure shows the relative strength of each parameter. The table shows the default values.

IKE Policy Parameters

Parameter	Accepted Values	Keyword	Default
Message encryption algorithm	DES 3DES	des 3des	56-bit DES-CBC
Message integrity (hash) algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha md5	SHA-1
Peer authentication method	Preshared keys RSA encrypted nonces RSA signatures	pre-share rsa-encr rsa-sig	RSA signatures
Key exchange parameters (Diffie-Hellman group identifier)	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768-bit Diffie-Hellman
ISAKMP-established security association lifetime	Can specify any number of seconds	—	86,400 sec (one day)

You can select specific values for each ISAKMP parameter per the ISAKMP standard. You select one value over another based on the security level you want and the type of IPSec peer to which you will connect. There are five parameters to define in each IKE policy as presented in the table here. The table shows the relative strength of each parameter.

Parameter	Strong	Stronger
Message encryption algorithm	DES	3DES
Message integrity (hash) algorithm	MD5	SHA-1
Peer authentication method	Preshare	RSA encryption RSA signature
Key exchange parameters (Diffie-Hellman group identifier)	D-H Group 1	D-H Group 2
ISAKMP-established security association lifetime	86,400 sec	<86,400 sec

You should determine IKE policy details for each peer before configuring IKE. The figure shows a summary of IKE policy details that will be configured in examples and later, in labs for this lesson. The authentication method of preshared keys is also covered in this lesson.

Step 2: Determine IPSec (IKE Phase 2) Policy

This topic describes the process for determining the IKE Phase 2 policy.

Step 2—Determine IPSec (IKE Phase 2) Policy

Cisco.com

Determine the following policy details:

- **IPSec algorithms and parameters for optimal security and performance**
- **Transforms and, if necessary, transform sets**
- **IPSec peer details**
- **IP address and applications of hosts to be protected**
- **Manual or IKE-initiated SAs**

Goal: Minimize misconfiguration

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—5.5

An IPSec policy defines a combination of IPSec parameters that are used during the IPSec negotiation. Planning for IPSec (IKE Phase 2) is another important step you should complete before actually configuring IPSec on a Cisco router. Policy details to determine at this stage include:

- **Select IPSec algorithms and parameters for optimal security and performance:** Determine what type of IPSec security to use when securing interesting traffic. Some IPSec algorithms require that you make tradeoffs between high performance and stronger security. Some algorithms have import and export restrictions that may delay or prevent implementation of your network.
- **Select transforms and, if necessary, transform sets:** Use the IPSec algorithms and parameters previously decided upon to help select IPSec transforms, transform sets, and modes of operation.
- **Identify IPSec peer details:** Identify the IP addresses and host names of all IPSec peers to which you will connect.
- **Determine IP address and applications of hosts to be protected:** Decide which IP addresses and applications of hosts should be protected at the local peer and remote peer.
- **Select manual or IKE-initiated SAs:** Choose whether SAs are manually established or are established via IKE.

The goal of this planning step is to gather the precise data that you will need in later steps to minimize misconfiguration.

IPSec Transforms Supported in Cisco IOS Software

This topic describes the IPSec transforms that are supported by Cisco IOS software.

IPSec Transforms Supported in Cisco IOS Software

Cisco.com

Cisco IOS software supports the following IPSec transforms:

```
CentralA (config)# crypto ipsec transform -set transform -set-name ?
ah-md5-hmac    AH - HMAC-MD5 transform
ah-sha-hmac    AH - HMAC-SHA transform
esp-3des       ESP transform using 3DES (EDE) cipher (168 bits)
esp-des        ESP transform using DES cipher (56 bits)
esp-md5-hmac   ESP transform using HMAC -MD5 auth
esp-sha-hmac   ESP transform using HMAC -SHA auth
esp-null       ESP transform w/o cipher
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-5-6

Cisco IOS software supports the IPSec transforms as shown in the figure. Newer Cisco IOS software includes support for Advanced Encryption Standard (AES).

Note AH is rarely used because authentication is now available with the esp-sha-hmac and esp-md5-hmac transforms. AH is also not compatible with NAT or PAT.

Note IOS Release 12.2(13)T adds the AES feature support for the new encryption standard AES. The National Institute of Standards and Technology (NIST) has created AES, which is a new Federal Information Processing Standards (FIPS) publication that describes an encryption method. AES is a privacy transform for IPSec and IKE, and has been developed to replace DES. AES is designed to be more secure than DES in that AES offers a larger key size. The algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

Encapsulating Security Payload

Transform	Description
esp-des	ESP transform using DES cipher (56 bits)
esp-3des	ESP transform using 3DES(EDE) cipher (168 bits)
esp-md5-hmac	ESP transform with HMAC-MD5 authentication used with an ESP-DES or ESP-3DES transform to provide additional integrity of ESP packet
esp-sha-hmac	ESP transform with HMAC-SHA authentication used with an ESP-DES or ESP-3DES transform to provide additional integrity of ESP packet
esp-null	ESP transform without a cipher. May be used in combination with ESP-MD5-HMAC or ESP-SHA-HMAC if one wants ESP authentication with no encryption

Caution Never use esp-null in a production environment because it does not protect data flows.

Examples of acceptable transforms that can be combined into sets are shown in the table here.

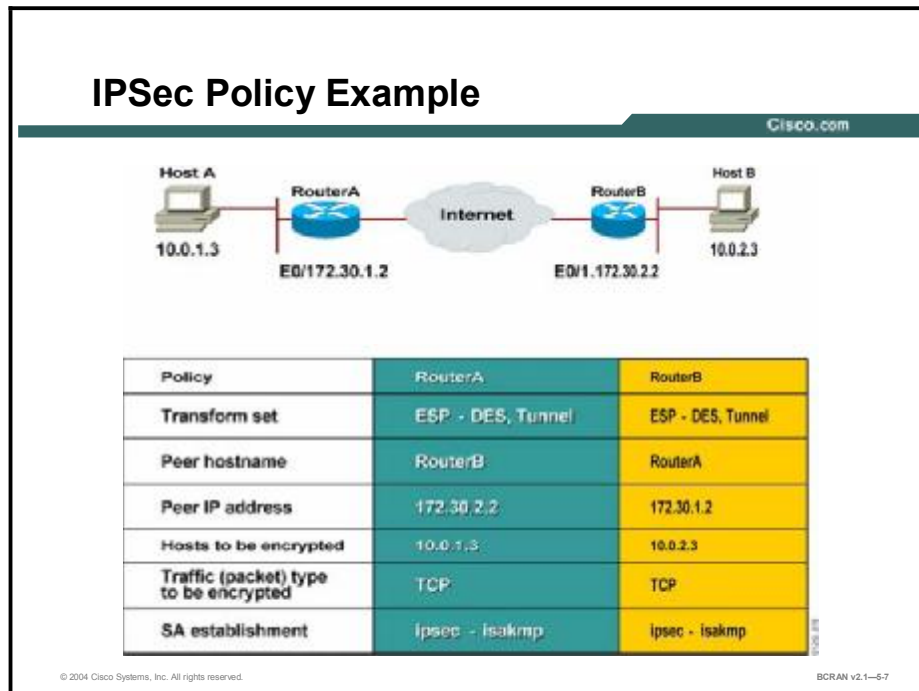
Acceptable Transforms

Transform Type	Allowed Transform Combinations
AH transform (Pick up to one)	<ul style="list-style-type: none">■ ah-md5-hmac—AH with the MD5 (HMAC variant) authentication algorithm■ ah-sha-hmac—AH with the SHA (HMAC variant) authentication algorithm
ESP encryption transform (Pick up to one)	<ul style="list-style-type: none">■ esp-des—ESP with the 56-bit DES encryption algorithm■ esp-3des—ESP with the 168-bit DES encryption algorithm (3DES)■ esp-null—Null encryption algorithm■ esp-aes—ESP with 128-bit AES encryption■ esp-aes 192—ESP with 192-bit AES encryption■ esp-aes 256—ESP with 256-bit AES encryption
ESP authentication transform (Pick up to one)	<ul style="list-style-type: none">■ esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm■ esp-sha-hmac—ESP with the SHA (HMAC variant) authentication algorithm
IP compression transform	<ul style="list-style-type: none">■ comp-lzs—IP compression with the LZS algorithm

The Cisco IOS command parser prevents you from entering invalid combinations; for example, after you specify an AH transform, it does not allow you to specify another AH transform for the current transform set.

IPSec Policy Example

This topic describes an example of an IPSec policy.



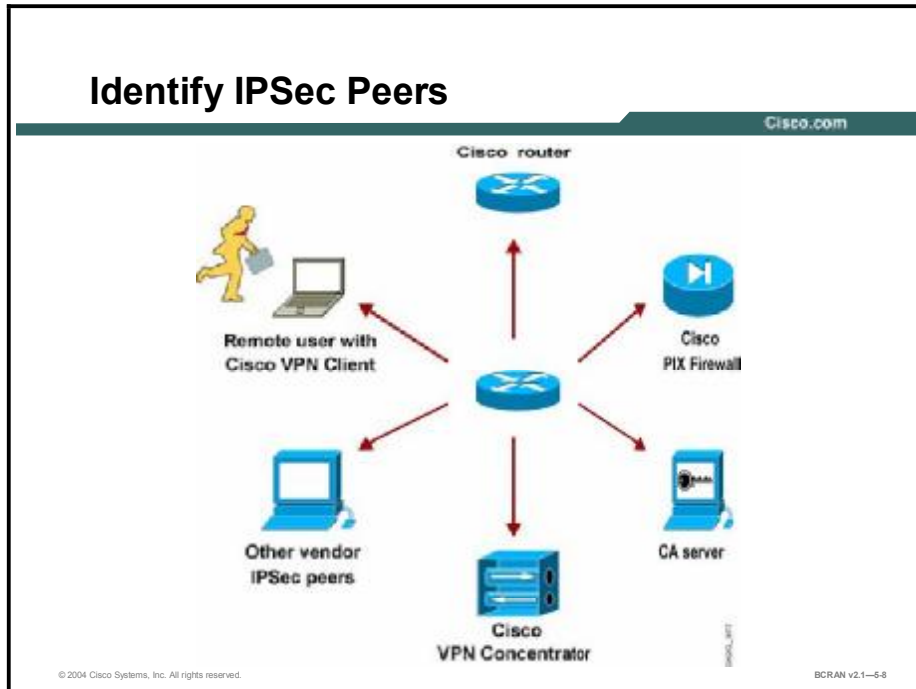
The figure shows a summary of IPSec encryption policy details that will be configured in examples in this lesson. (Details about IPSec transforms are covered later in this lesson.) The example policy specifies that TCP traffic between the hosts should be encrypted by IPSec that uses DES.

Determining network design details includes defining a more detailed IPSec policy for protecting traffic. You can then use the detailed policy to help select IPSec transform sets and modes of operation. Your IPSec policy should answer these questions:

- What protections are required or are acceptable for the protected traffic?
- Which IPSec transforms or transform sets should be used?
- What are the peer IPSec endpoints for the traffic?
- What traffic should or should not be protected?
- Which router interfaces are involved in protecting internal nets and external nets?
- How are SAs set up (manual or IKE negotiated) and how often should the SAs be renegotiated?

IPSec Peers

This topic describes the importance of identifying the IPSec peer.



An important part of determining the IPSec policy is to identify the IPSec peer with which the Cisco router will communicate. The peer must support IPSec as specified in the RFCs that are supported by Cisco IOS. Many different types of peers are possible. Before configuration, identify all the potential peers and their VPN capabilities. Possible peers include, but are not limited, to these:

- Other Cisco routers
- The Cisco PIX Firewall
- The Cisco VPN client (hardware or software)
- The Cisco VPN concentrator
- CA servers if they are used
- IPSec products of other vendors that conform to IPSec RFCs

Caution Incompatibilities may exist when configuring IPSec and IKE between older and newer IOS images; for example, configuring IPSec between a router with IOS 12.0.3 and another router with IOS 12.2.8. Compatibility matrixes should be checked in the planning stages.

Step 3: Check Current Configuration

This topic describes the commands that are used to check for existing IPsec security policies.

Step 3—Check Current Configuration

```
graph LR
    HA[Host A  
10.0.1.3] --- RA[RouterA  
172.30.1.2]
    RA --- Internet((Internet))
    Internet --- RB[RouterB  
172.30.2.2]
    RB --- HB[Host B  
10.0.2.3]
```

router#

`show running-config`

- View router configuration for existing IPsec policies.

`show crypto isakmp policy`

- View default and any configured IKE Phase 1 policies.

`show crypto map`

- View any configured crypto maps.

`show crypto ipsec transform-set`

- View any configured transform sets.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.9

The current Cisco router configuration should be checked to see if there are any IPsec policies already configured that are useful for—or may interfere with—the IPsec policies that you plan to configure. Previously configured IKE and IPsec policies and details can and should be used, if possible, to save configuration time. However, they can make troubleshooting more difficult if problems arise.

You can see if any IKE policies have previously been configured by using the **show running-config** command. You can also use the variety of **show** commands that are specific to IPsec. For example, you can use the **show crypto isakmp policy** command, shown in the figure, to examine IKE policies.

```
RouterA# show crypto isakmp policy
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56
bit keys)
  hash algorithm:        Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:  #1 (768 bit)
  lifetime:              86400 seconds, no volume limit
```

The default protection suite seen here is available for use without modification. You can also use the other available **show** commands covered in other lessons of this module to view IKE and IPsec configuration.

The **show crypto map** command shown in the figure is useful for viewing any previously configured crypto maps (crypto maps are covered in detail later in this module). Previously configured maps can and should be used to save configuration time. However, previously configured crypto maps can interfere with the IPsec policy that you are trying to configure.

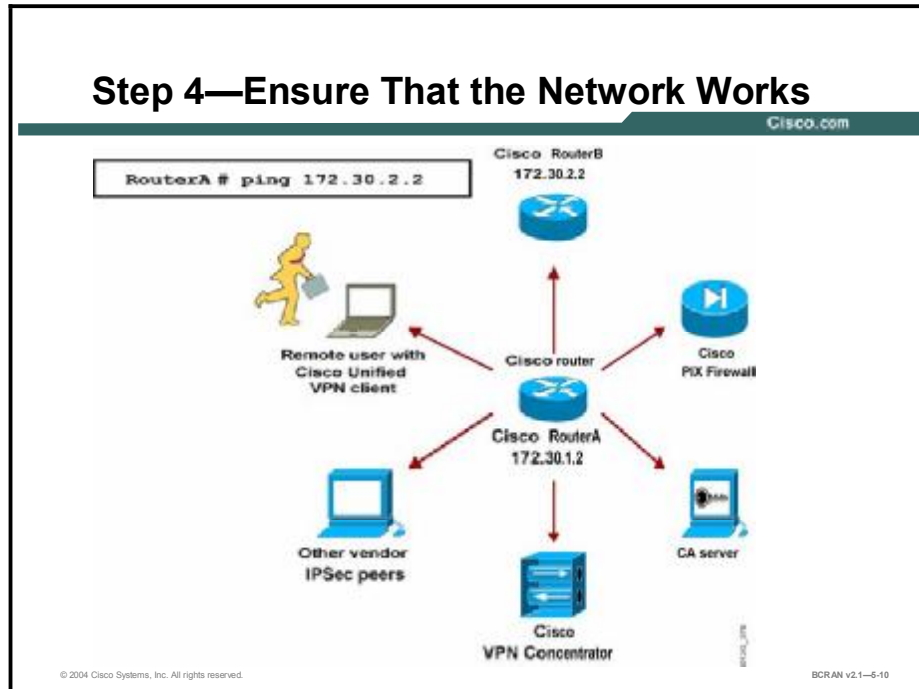
```
RouterA# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
    Peer = 172.30.2.2
    Extended IP access list 102
        access-list 102 permit ip host 172.30.1.2 host
        172.30.2.2
    Current peer: 172.30.2.2
    Security association lifetime: 4608000 kilobytes/3600
seconds
    PFS (Y/N) : N
    Transform sets={ mine, }
```

You can also use the **show crypto ipsec transform-set** command to view previously configured transform sets. Previously configured transforms can, and should, be used to save configuration time.

```
RouterA# show crypto ipsec transform-set mine
Transform set mine: { esp-des  }
    will negotiate = { Tunnel, },
```


Step 4: Ensure That the Network Works

This topic describes the commands that are used to ensure connectivity between IPSec peers.



Basic connectivity between peers must be checked before you begin configuring IPSec.

The router **ping** command can be used to test basic connectivity between IPSec peers. While a successful Internet Control Message Protocol (ICMP) echo (ping) will verify basic connectivity between peers, you should ensure the network works with any other protocols or ports you want to encrypt, such as Telnet, FTP, or SQL*NET before beginning IPSec configuration.

After IPSec is activated, basic connectivity troubleshooting can be difficult because the security configuration may mask a more fundamental networking problem. Previous security settings could result in no connectivity.

Note The **ping** command may be limited by access lists.

Step 5: Ensure That Access Lists Are Compatible with IPsec

This topic describes how to ensure that access lists are compatible with IPsec.

Step 5—Ensure That Access Lists Are Compatible with IPsec

Cisco.com

```
RouterA# show access-lists
access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq
isakmp
```

- Ensure that protocols 50 and 51, and UDP port 500 traffic are not blocked at interfaces used by IPsec.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5-11

You will need to ensure that existing ACLs on perimeter routers, firewalls, or other routers do not block IPsec traffic. Perimeter routers typically implement a restrictive security policy with ACLs, where only specific traffic is permitted and all other traffic is denied. Such a restrictive policy blocks IPsec traffic. Therefore, you must add specific **permit** statements to the ACL to allow IPsec traffic.

Ensure that your ACLs are configured so that ISAKMP, ESP, and AH traffic is not blocked at interfaces used by IPsec. ISAKMP uses User Datagram Protocol (UDP) port 500. ESP is assigned IP protocol number 50, and AH is assigned IP protocol number 51. In some cases, you may need to add a statement to router ACLs to explicitly permit this traffic. You may need to add the ACL statements to the perimeter router by performing these steps:

- Step 1** Examine the current ACL configuration at the perimeter router and determine if it will block IPsec traffic:

```
RouterA# show access-lists
```

- Step 2** Add ACL entries to permit IPSec traffic. To do this, copy the existing ACL configuration and paste it into a text editor as follows:
1. Copy the existing ACL configuration and paste it into a text editor.
 2. Add the ACL entries to the top of the list in the text editor.
 3. Delete the existing ACL with the **no access-list access-list number** command.
 4. Enter configuration mode and copy and paste the new ACL into the router.
 5. Verify that the ACL is correct with the **show access-lists** command.

A concatenated example showing ACL entries permitting IPSec traffic for RouterA is as follows:

```
RouterA# show running-config
!
interface Serial0/1
 ip address 172.30.1.2 255.255.255.0
 ip access-group 102 in
!
access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq
isakmp
```

Note that the protocol keyword of **esp** equals the ESP protocol (number 50), the keyword of **ahp** equals the AH protocol (number 51), and the **isakmp** keyword equals UDP port 500.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Determine the IKE policy details to enable the selected authentication method, and then configure it.**
- **An IKE policy defines a combination of security parameters used during the IKE negotiation.**
- **It is important to identify the IPsec that peer the Cisco router will communicate with.**
- **The current Cisco router configuration should be checked to see if there are any IPsec that policies already configured that are useful for, or may interfere with, the IPsec that policies you plan to configure.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—5-12

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the purpose of examining the access lists when preparing for IKE and IPSec?
- A) to enforce VPN security
 - B) to make sure VPN security is not blocked by an access list
 - C) to show which interfaces are serial interfaces
 - D) to implement unused security policies
- Q2) Which key distribution method is most effective for a number of VPN users?
- A) preshared keys
 - B) a network administrator PDA
 - C) hashing
 - D) certification authorities
- Q3) Which transform type is most secure?
- A) ah-sha-hmac
 - B) ah-md5-hmac
 - C) esp-null
 - D) esp-des
- Q4) It is not necessary to define a transform set when determining IPSec policy.
- A) true
 - B) false
- Q5) Which of the following devices may NOT be an IPSec peer?
- A) a PC with a VPN client
 - B) a Cisco network switch
 - C) a Cisco router
 - D) a VPN concentrator
- Q6) The **show crypto map** command will not define the peer of the map.
- A) true
 - B) false
- Q7) IPSec implementation makes basic troubleshooting difficult because _____.
- A) there are many commands to memorize
 - B) analyzing packets may be difficult if they are encrypted
 - C) it applies access lists that block traffic with the **implicit deny** command

- Q8) Which of the following does NOT need to be allowed through an access list to ensure that a VPN will function?
- A) protocol 50
 - B) protocol 51
 - C) UDP port 500
 - D) UDP port 53

Quiz Answer Key

- Q1) B
Relates to: IKE Creation and IPSec Security Policy
- Q2) D
Relates to: Step 1: Determine IKE (IKE Phase 1) Policy
- Q3) D
Relates to: IPSec Transforms Supported in Cisco IOS Software
- Q4) B
Relates to: IPSec Policy Example
- Q5) B
Relates to: IPSec Peers
- Q6) B
Relates to: Step 3: Check Current Configuration
- Q7) B
Relates to: Step 4: Ensure That the Network Works
- Q8) D
Relates to: Step 5: Ensure That Access Lists Are Compatible with IPSec

Task 2: Configuring IKE

Overview

The next major task in configuring Cisco IOS IPsec is to configure the IKE parameters that you gathered earlier. This lesson describes the steps that are used to configure IKE policies.

Relevance

A major task in configuring IPsec is to configure the proper IKE parameters that are used in IKE policies.

Objectives

Upon completing this lesson, you will be able to:

- List the steps to configure IKE
- Identify the command that is used to enable or disable ISAKMP
- Identify the command that is used to define an IKE policy
- Identify the command that is used to set ISAKMP parameters
- Describe the process and commands in IKE policy negotiation
- Identify the command that is used to configure the ISAKMP identity
- Identify the command that is used to configure a preshared authentication key
- Identify the command to verify IKE configuration

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- IKE Configuration
- Step 1: Enable or Disable IKE
- Step 2: Create IKE Policies
- IKE Policy Creation with the **crypto isakmp** Command
- IKE Policy Negotiation
- Step 3: Configure ISAKMP Identity
- Step 4: Configure Preshared Keys
- Step 5: Verify IKE Configuration
- Summary
- Quiz

IKE Configuration

This topic describes the steps that are required to configure IKE.

Task 2—Configure IKE

Cisco.com

Task 1 – Prepare for IKE and IPSec

Task 2 – Configure IKE

- Step 1—Enable or disable IKE.**
`crypto isakmp enable`
- Step 2—Create IKE policies.**
`crypto isakmp policy`
- Step 3—Configure ISAKMP**
`crypto isakmp identity`
- Step 4—Configure preshared keys.**
`crypto isakmp key`
- Step 5—Verify the IKE configuration.**
`show crypto isakmp policy`

Task 3 – Configure IPSec

Task 4 – Test and Verify IPSec

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1–6.2

Configuring IKE consists of these essential steps and commands:


- Step 1** Enable or disable IKE with the `crypto isakmp enable` command.
- Step 2** Create IKE policies with the `crypto isakmp policy` commands.
- Step 3** Configure preshared keys with the `crypto isakmp key` and associated commands.
- Step 4** Verify the IKE configuration with the `show crypto isakmp policy` command.

Step 1: Enable or Disable IKE

This topic describes the command that is used to enable or disable IKE.

Step 1—Enable IKE

Cisco.com



Router A `crypto isakmp enable`

- Globally enables or disables IKE at your router.
- IKE is enabled by default.
- IKE is enabled globally for all interfaces at the router.
- Use the **no** form of the command to disable IKE.
- An ACL can be used to block IKE on a particular interface.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—5.3

The first step in configuring IKE is to enable or disable ISAKMP, thereby enabling or disabling IKE. ISAKMP, and consequently IKE, is globally enabled and disabled with the **crypto isakmp enable** command. ISAKMP is enabled by default. Use the **no** form of the command to disable ISAKMP.


Although ISAKMP does not have to be enabled for individual interfaces, it is enabled globally for all interfaces at the router. You may choose to block ISAKMP access on interfaces that are not used for IPsec to prevent possible denial of service attacks by using an ACL statement that blocks UDP port 500 on the interfaces.

Step 2: Create IKE Policies

This topic describes the command that is used to create an IKE policy.

Step 2—Create IKE Policies

Cisco.com



```
router(config) #  
crypto isakmp policy priority
```

- Defines an IKE policy, which is a set of parameters used during IKE negotiation.
- Invokes the config-isakmp command mode.

```
RouterA ( config )# crypto isakmp policy 110
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.4

The next major step in configuring Cisco IOS ISAKMP support is to define a suite of ISAKMP policies. The goal of defining a suite of IKE policies is to establish ISAKMP peering between two IPsec endpoints. Use the IKE policy details that you gathered during the planning task.

Use the **crypto isakmp policy** command to define an IKE policy. IKE policies define a set of parameters that are used during the IKE negotiation. Use the **no** form of this command to delete an IKE policy. The command syntax and parameter definition is shown in the table.

```
crypto isakmp policy priority
```

crypto isakmp policy *priority* Command Parameter

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.

This command invokes the ISAKMP policy configuration (config-isakmp) command mode.

Note Assign the most secure policy the lowest priority number so that the most secure policy will find a match before any less-secure policies are configured.

IKE Policy Creation with the *crypto isakmp* Command

This topic describes the command that is used to set ISAKMP parameters.

Create IKE Policies with the *crypto isakmp* Command

Cisco.com

```
router(config) #  
crypto isakmp policy priority
```

- Defines the parameters within the IKE policy 110.

```
RouterA(config)# crypto isakmp policy 110  
RouterA(config-isakmp) # authentication pre-share  
RouterA(config-isakmp) # encryption des  
RouterA(config-isakmp) # group 1  
RouterA(config-isakmp) # hash md5  
RouterA(config-isakmp) # lifetime 86400
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5-6

The **crypto isakmp policy** command invokes the ISAKMP policy configuration command mode (config-isakmp) where you can set ISAKMP parameters. If you do not specify one of these commands for a policy, the default value will be used for that parameter. The table lists the keywords available to specify the parameters in the policy while you are in the config-isakmp command mode.

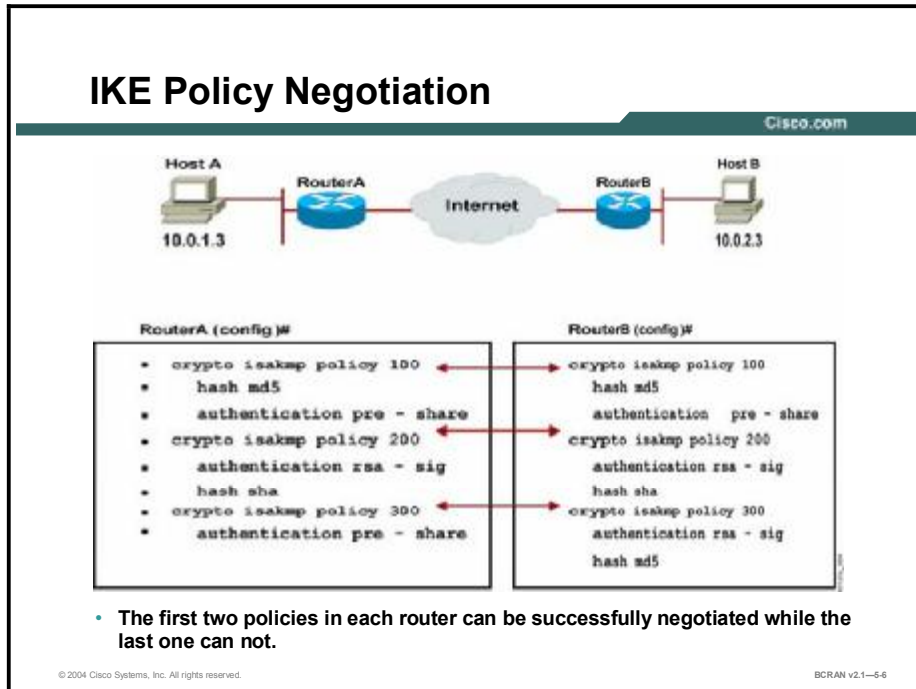
Keywords for ISAKMP Parameters

Parameter	Keyword	Accepted Values	Default Value	Description
Encryption	des	56-bit DES-CBC	des	Message encryption algorithm.
	aes	128-bit AES		
	aes 192	192-bit AES		
	aes 256	256-bit AES		
Hash	sha	SHA-1 (HMAC variant)	sha	Message integrity (Hash) algorithm.
	md5	MD5 (HMAC variant)		
Authentication	rsa-sig	RSA signatures	rsa-sig	Peer authentication method.
	rsa-encr	RSA encrypted nonces		
	pre-share	presared keys		
Group	1	768-bit Diffie-Hellman or	1	Key exchange parameters (Diffie-Hellman group identifier).
	2	1024-bit Diffie-Hellman		
Lifetime	seconds	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime. You can usually leave this value at the default.
	exit			

Multiple ISAKMP policies can be configured on each peer participating in IPSec. ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.

IKE Policy Negotiation

This topic describes the processes and commands in IKE policy negotiation.



ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPsec.

When the ISAKMP negotiation begins in IKE Phase 1 main mode, ISAKMP looks for an ISAKMP policy that is the same on both peers. The peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer tries to find a match with its policies. The remote peer looks for a match by comparing its own highest priority policy against the other peer received policies in its ISAKMP policy suite. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, Diffie-Hellman parameter values, and when the policy of the remote peer specifies a lifetime less than or equal to the lifetime of the policy being compared. If the lifetimes are not identical, the shorter lifetime from the remote peer policy is used. Assign the most secure policy the lowest priority number so that the most secure policy will find a match before any less secure policies are configured.


If an acceptable match is not found, ISAKMP refuses negotiation and IPsec is not established. If a match is found, ISAKMP completes the main mode negotiation, and IPsec SAs are created during IKE Phase 2 quick mode.

Step 3: Configure ISAKMP Identity

This topic describes the command that is used to configure the ISAKMP identity.

Step 3—Configure ISAKMP Identity

Cisco.com



```
router(config) #
crypto isakmp identity {address | hostname}
```

- Defines whether ISAKMP identity is done by IP address or hostname.
- Use consistently across ISAKMP peers.

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1-6.7

IPSec peers authenticate each other during ISAKMP negotiations by using the preshared key and the ISAKMP identity. The identity can either be the IP address or the host name of the router. Cisco IOS software uses the IP address identity method by default. A command indicating the address mode does not appear in the router configuration.

If you choose to use the host name identity method, you must specify the method with the **crypto isakmp identity** global configuration command. Use the **no** form of this command to reset the ISAKMP identity to the default value (address). The command syntax and parameter definitions are as follows:

```
crypto isakmp identity {address | hostname}
```

crypto isakmp identity (address | hostname) Command

crypto isakmp identity Command	Description
address	<p>Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during ISAKMP negotiations.</p> <p>The keyword is typically used when there is only one interface that will be used by the peer for ISAKMP negotiations, and the IP address is known.</p>
hostname	<p>Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.domain.com).</p> <p>The keyword should be used if there is more than one interface on the peer that might be used for ISAKMP negotiations, or if the interface IP address is unknown (such as with dynamically-assigned IP addresses).</p>

If you use the host name identity method, you may need to specify the host name for the remote peer if a DNS server is not available for name resolution. An example of this follows:

```
RouterA(config)# ip host RouterB.domain.com 172.30.2.2
```

Step 4: Configure Preshared Keys

This topic describes the command that is used to configure a preshared authentication key.

Step 4—Configure Preshared Keys

Cisco.com

```
router(config) #  
crypto isakmp key keystring address peer-address  
  
router(config) #  
crypto isakmp key keystring hostname hostname  
  
RouterA(config)# crypto isakmp key cisco1234  
address 172.30.2.2
```

- Assigns a keystring and the peer address.
- The peer IP address or hostname can be used.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.8

Configure a preshared authentication key with the **crypto isakmp key** global configuration command. You must configure this key whenever you specify preshared keys in an ISAKMP policy. Use the **no** form of this command to delete a preshared authentication key. The command syntax parameter definitions are as follows:

```
crypto isakmp key keystring address peer-address  
crypto isakmp key keystring hostname peer-hostname
```

crypto isakmp key Command Arguments

crypto isakmp key keystring Command	Description
keystring	Specify the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.
peer-address	Specify the IP address of the remote peer.
hostname	Specify the host name of the remote peer. This is the peer host name concatenated with its domain name (for example, myhost.domain.com).

Note A given preshared key is shared between two peers. At a given peer, you can specify the same key to share with multiple remote peers; however, a more secure approach is to specify different keys to share between different pairs of peers.

The following configuration example shows ISAKMP and preshared keys for routerA and routerB. Note that the keystore of *cisco1234* matches. The address identity method is specified. The ISAKMP policies are compatible. Default values do not have to be configured.

```
RouterA(config)# crypto isakmp key cisco1234 address  
172.30.2.2
```

```
RouterA(config)# crypto isakmp policy 110
```

```
RouterA(config-isakmp)# hash md5
```

```
RouterA(config-isakmp)# authentication pre-share
```

```
RouterA(config-isakmp)# exit
```

```
RouterB(config)# crypto isakmp key cisco1234 address  
172.30.1.2
```

```
RouterB(config)# crypto isakmp policy 110
```

```
RouterB(config-isakmp)# hash md5
```

```
RouterB(config-isakmp)# authentication pre-share
```

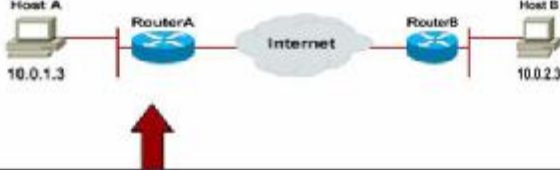
```
RouterB(config-isakmp)# exit
```

Step 5: Verify IKE Configuration

This topic describes the command that is used to verify IKE configuration.

Step 5—Verify IKE Configuration

Cisco.com



```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:      Message Digest 5
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #1 (768 bit)
 lifetime:             86400 seconds, no volume limit
Default protection suite
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:      Secure Hash Standard
 authentication method: Rivest - Shamir Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 lifetime:             86400 seconds, no volume limit
```

- Displays configured and default IKE policies.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.9

You can use the **show crypto isakmp policy** command to display configured and default policies. The resultant ISAKMP policy for routerA is shown in the output here and in the figure. RouterB configuration is identical.

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:      Message Digest 5
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #1 (768 bit)
 lifetime:             86400 seconds, no volume limit
Default protection suite
 encryption algorithm:  DES - Data Encryption Standard (56 bit
 keys).
  hash algorithm:      Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 lifetime:             86400 seconds, no volume limit
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configuring IKE consists of several essential steps and commands.**
- **Configure IKE to enable or disable ISAKMP with the `crypto isakmp enable` command.**
- **Use the `crypto isakmp policy` command to define an IKE policy.**
- **ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.**
- **IPSec peers authenticate each other during ISAKMP negotiations using the preshared key and the ISAKMP identity.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—5-10

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which command enables IKE?
- A) **crypto isakmp enable**
 - B) **crypto isakmp policy**
 - C) **crypto isakmp key**
 - D) **show crypto isakmp policy**
- Q2) The **crypto isakmp enable** command is defined on a per-interface basis.
- A) true
 - B) false
- Q3) Crypto isakmp policies are read in descending order of priority.
- A) true
 - B) false
- Q4) What types of authentication methods *cannot* be used by Cisco IOS ISAKMP peers?
- A) token cards
 - B) RSA signatures
 - C) RSA nonces
 - D) preshared keys
- Q5) If two identical isakmp policies are not configured on potential IPSec partners, what happens?
- A) The peers negotiate on all other parameters and use the defaults for dissimilar elements.
 - B) The peers refuse to negotiate and do not continue building an IPSec tunnel.
 - C) The peers build an IPSec tunnel but there is a risk that the traffic will not be encrypted.
 - D) The peers are forced to reboot and search their startup configuration.
- Q6) If there is *no* DNS server available in the network, you may NOT use the **crypto isakmp identity hostname** command.
- A) true
 - B) false

- Q7) What command is used to identify the preshared key?
- A) **crypto isakmp key** *key address peer-address*
 - B) **crypto isakmp pre-share** *key address peer-address*
 - C) **crypto ipsec key** *key address peer-address*
 - D) **crypto ipsec pre-share** *key address peer-address*
- Q8) The **show crypto isakmp policy** command displays all of the information below except _____.
- A) hash algorithm
 - B) encryption algorithm
 - C) authentication method
 - D) interface-type number

Quiz Answer Key

- Q1) A
Relates to: IKE Configuration
- Q2) B
Relates to: Step 1: Enable or Disable IKE
- Q3) B
Relates to: Step 2: Create IKE Policies
- Q4) A
Relates to: IKE Policy Creation with the `crypto isakmp` Command
- Q5) B
Relates to: IKE Policy Negotiation
- Q6) B
Relates to: Step 3: Configure ISAKMP Identity
- Q7) A
Relates to: Step 4: Configure Preshared Keys
- Q8) D
Relates to: Step 5: Verify IKE Configuration

Task 3: Configuring IPSec

Overview

The next major task in configuring Cisco IOS IPSec is to configure the IPSec parameters that you previously gathered. This lesson describes the steps that are used to configure IPSec.

Relevance

It is important to understand and properly configure all of the necessary features of IPSec.

Objectives

Upon completing this lesson, you will be able to:

- List the steps to configure IPSec encryption on Cisco routers
- Describe the process of configuring Cisco IOS IPSec to define a transform set objective
- Describe the process of transform set negotiation
- Describe how to configure global SAs
- Describe how to configure crypto ACLs
- Describe the process of using crypto ACLs to identify traffic flows that need to be protected
- Describe how to configure symmetric crypto ACLs for use by IPSec
- Define the purpose of crypto maps, examining the **crypto map** command and example crypto maps
- Describe the use of crypto maps and their parameters
- Provide an example of the use of IPSec on two routers
- Provide an example of configuring IPSec to apply the crypto map set to an interface

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- IPSec Configuration
- Step 1: Configure Transform Set Suites
- Set Negotiation Transformation
- Step 2: Configure Global IPSec Security Association Lifetimes
- Crypto Access Lists Functionality
- Step 3: Create Crypto ACLs Using Extended Access Lists
- Symmetric Peer Crypto Access Lists Configuration
- Crypto Maps Functionality
- Crypto Map Parameters
- Step 4: Configure IPSec Crypto Maps
- Crypto Map Commands Example
- Step 5: Apply Crypto Maps to Interfaces
- IPSec Configuration Examples
- Summary
- Quiz

IPSec Configuration

This topic describes the steps that are used to configure IPSec encryption on Cisco routers.

Task 3—Configure IPSec

Cisco.com

Task 1 – Prepare for IKE and IPSec

Task 2 – Configure IKE

Task 3 – Configure IPSec

- Step 1—Configure transform set suites**
`crypto ipsec transform-set`
- Step 2—Configure global IPSec SA lifetimes**
`crypto ipsec security-association lifetime`
- Step 3—Create crypto ACLs using extended access lists**
`crypto map`
- Step 4—Configure IPSec crypto maps**
- Step 5—Apply crypto maps to interfaces**
`crypto map map-name`

Task 4 – Test and Verify IPSec

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1–6.2

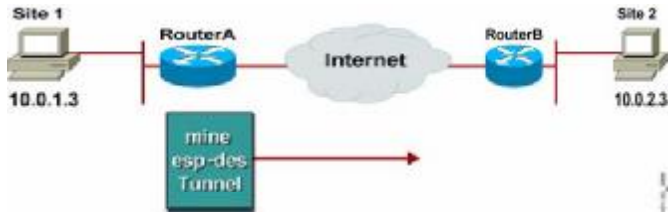
Configuring IPSec consists of these essential steps and commands:

- Step 1** Configure transform set suites with the `crypto ipsec transform-set` command.
- Step 2** If it is necessary to change the default, configure global IPSec security association lifetimes with the `crypto ipsec security-association lifetime` command.
- Step 3** Configure crypto ACLs with the `access-list` command.
- Step 4** Configure crypto maps with the `crypto map` command.
- Step 5** Apply the crypto maps to the terminating or originating interface with the `interface` and `crypto map` commands.

Step 1: Configure Transform Set Suites

This topic describes the first major step in configuring Cisco IOS IPsec, using the IPsec security policy to define a transform set.

Step 1—Configure Transform Sets



Cisco.com

```
router(config) #  
crypto ipsec transform -set transform -set-name  
transform1 [transform2 [transform3]]  
router (cfg-crypto -trans) #
```

```
RouterA(config)# crypto ipsec transform-set mine esp-des
```

- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- Sets are limited to up to one AH and up to two ESP transforms.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—63

A transform set is a combination of individual IPsec transforms that are designed to enact a specific security policy for traffic. During the ISAKMP IPsec SA negotiation that occurs in IKE Phase 2 quick mode, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine these IPsec factors:

- Mechanism for payload authentication: AH transform
- Mechanism for payload encryption: ESP transform
- IPsec mode (transport versus tunnel)

Transform sets equal a combination of an AH transform, an ESP transform, and the IPsec mode (either tunnel or transport mode). Transform sets are limited to one AH transform and one or two ESP transforms. Define a transform set with the **crypto ipsec transform-set** global configuration command. To delete a transform set, use the **no** form of the command. The command syntax and parameter definitions are as follows:

```
crypto ipsec transform-set transform-set-name transform1  
[transform2 [transform3]]
```

crypto ipsec transform-set Command Parameters

Command	Description
<i>transform-set-name</i>	Specifies the name of the transform set to create (or modify).
<i>transform1, transform2, transform3</i>	Specifies up to three transforms. These transforms define the IPsec security protocol(s) and algorithm(s).

The command invokes the crypto-transform configuration mode.

You can configure multiple transform sets and then specify one or more of the transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by the ACL of that crypto map entry. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of the IPsec SAs of both peers.

When ISAKMP is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

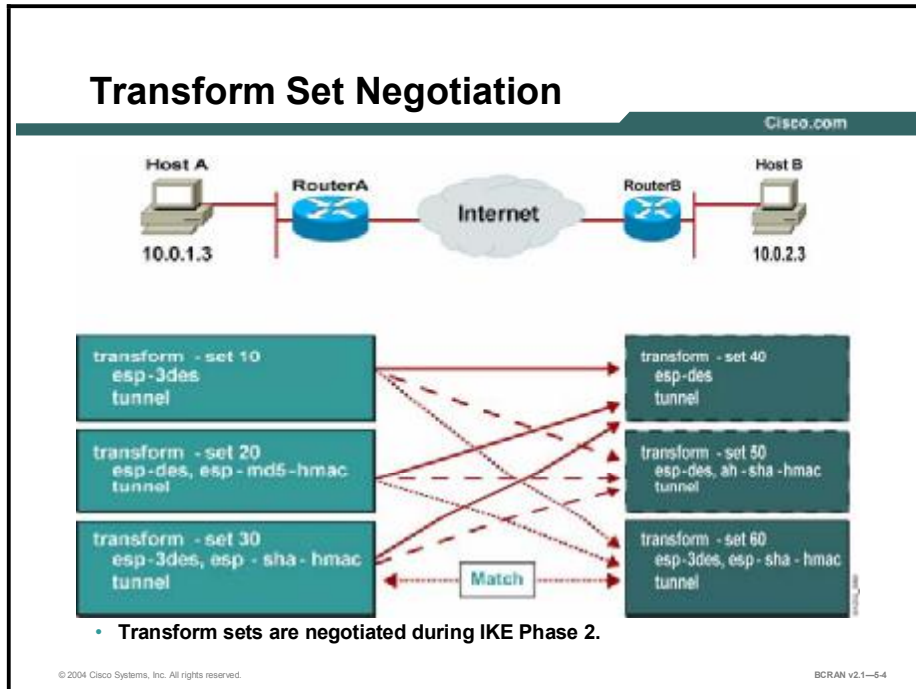
Edit Transform Sets

Use these steps if you must edit a transform set:

- Step 1** Delete the transform set from the crypto map.
- Step 2** Delete the transform set from global configuration.
- Step 3** Reenter the transform set with corrections.
- Step 4** Assign the transform set to a crypto map.
- Step 5** Clear the SA database.
- Step 6** Observe the SA negotiation and ensure that it works properly.

Set Negotiation Transformation

This topic describes the process of transform set negotiation.



Transform sets are negotiated during quick mode in IKE Phase 2 using the transform sets that you previously configured. You can configure multiple transform sets and then specify one or more of the transform sets in a crypto map entry. Configure the transforms from most to least secure, according to your policy. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows that are specified by the ACL of that crypto map entry.

During the negotiation, the peers search for a transform set that is the same at both peers, as illustrated in the figure. Each of the RouterA transform sets are compared against each of the RouterB transform sets in succession. RouterA transform sets 10, 20, and 30 are compared with RouterB transform set 40. The result is no match. All of RouterA transform sets are then compared against RouterB transform sets. Finally, RouterA transform set 30 matches RouterB transform set 60. When such a transform set match is found, it is selected and is applied to the protected traffic as part of the IPsec SAs of both peers. IPsec peers agree on one unidirectional transform proposal per SA.

Step 2: Configure Global IPSec Security Association Lifetimes

This topic describes how to configure global SAs. Both global and interface-specific SA lifetimes can be created.

Step 2—Configure Global IPSec Security Association Lifetimes

```
router(config) #
crypto ipsec security-association lifetime
{seconds seconds | kilobytes kilobytes}
```

```
RouterA (config)# crypto ipsec security - association
lifetime 86400
```

- Configures global IPSec SA lifetime values used when negotiating IPSec security associations.
- IPSec SA lifetimes are negotiated during IKE Phase 2.
- Can optionally configure interface-specific IPSec SA lifetimes in crypto maps.
- IPSec SA lifetimes in crypto maps override global IPSec SA lifetimes.

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1-5.5

The IPSec SA lifetime determines how long IPSec SAs remain valid before they are renegotiated. Cisco IOS software supports a global lifetime value that applies to all crypto maps. The global lifetime value can be overridden with a crypto map entry. You can change global IPSec SA lifetime values using the **crypto ipsec security-association lifetime** global configuration command. To reset a lifetime to the default value, use the **no** form of the command. The command syntax and parameter definitions are as follows:

```
crypto ipsec security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

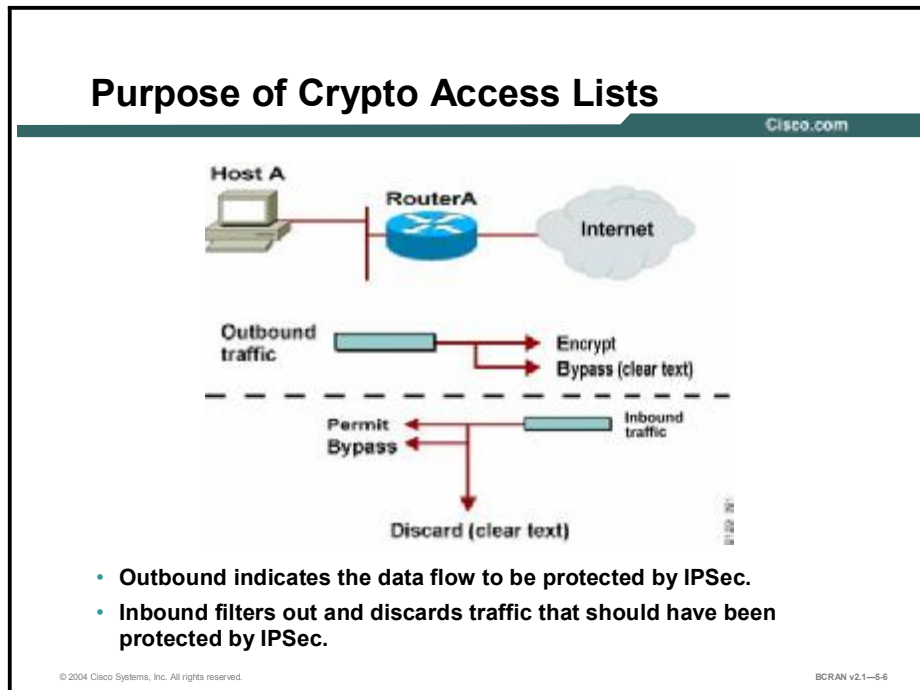
crypto ipsec security-association lifetime Command

Command	Description
seconds seconds	Specifies the number of seconds a security association will live before expiring. The default is 3600 sec (one hour).
kilobytes kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given SA before that SA expires. The default is 4,608,000 KB.

Cisco recommends that you use the default lifetime values. Individual IPSec SA lifetimes can be configured using crypto maps, which are covered later in this lesson.

Crypto Access Lists Functionality

This topic describes the purpose of crypto ACLs. Crypto ACLs are used to define which IP traffic is or is not protected by IPSec.



Crypto ACLs perform these functions:

- **Outbound:** Selects outbound traffic to be protected by IPSec. Traffic not selected is sent in clear text.
- **Inbound:** If desired, inbound access lists can be created to filter and discard traffic that should have been protected by IPSec.

Step 3: Create Crypto ACLs Using Extended Access Lists

This topic describes the process of using crypto ACLs to identify traffic flows that must be protected.

Step 3—Create Crypto ACLs using Extended Access Lists

Cisco.com

```

router(config)#
access-list access-list-number [dynamic dynamic-name
(timeout minutes )] (deny | permit) protocol source
source-wildcard destination destination-wildcard
[precedence precedence] [tos tos] [log]
    
```

```

RouterA (config)# access-list 110 permit tcp 10.0.1.0
0.0.0.255 10.0.2.0 0.0.0.255
    
```

- Define which IP traffic will be protected by crypto.
- Permit = encrypt / Deny = do not encrypt.

© 2004 Cisco Systems, Inc. All rights reserved.
BICRAN v2.1-5-7

The crypto ACLs identify the traffic flows that should be protected. Extended IP ACLs select IP traffic to encrypt by using protocol, IP address, network, subnet, and port. Although the ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs. That is, *permit* specifies that matching packets must be encrypted and *deny* specifies that matching packets must not be encrypted. Crypto ACLs behave similarly to an extended IP ACL that is applied to outbound traffic on an interface.

The command syntax and parameter definitions for the basic form of extended IP access lists are as follows:

```

access-list access-list-number { permit | deny } protocol
source
source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log]
    
```

access-list access-list-number Command

access-list access-list-number Command	Description
permit	Causes all IP traffic that matches the specified conditions to be protected by crypto, using the policy described by the corresponding crypto map entry.
deny	Instructs the router to route traffic in the clear.
source and destination	These are networks, subnets, or hosts.

Note Although the ACL syntax is unchanged, the meanings are slightly different for crypto ACLs. That is, *permit* specifies that matching packets must be encrypted and *deny* specifies that matching packets must not be encrypted.

Any unprotected inbound traffic that matches a *permit* entry in the crypto ACL for a crypto map entry that is flagged as IPsec will be dropped. This drop occurs because this traffic was expected to be protected by IPsec.

If you want certain traffic to receive one combination of IPsec protection (authentication only) and other traffic to receive a different combination (both authentication and encryption), create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries that specify different IPsec policies.

Warning Cisco recommends that you avoid using the *any* keyword to specify source or destination addresses. The *permit any any* statement is strongly discouraged because this will cause all outbound traffic to be protected and all protected traffic to be sent to the peer that is specified in the corresponding crypto map entry. Then, all inbound packets that lack IPsec protection will be silently dropped, including packets for routing protocols, NTP, echo, echo response, and so on.

Try to be as restrictive as possible when defining which packets to protect in a crypto ACL. If you must use the *any* keyword in a permit statement, you must preface that statement with a series of *deny* statements to filter out any traffic (that would otherwise fall within that permit statement) that you do not want to be protected.

Later in Step 4, you will associate a crypto ACL to a crypto map, which in turn is assigned to a specific interface.

Symmetric Peer Crypto Access Lists Configuration

This topic describes how to configure symmetric crypto ACLs for use by IPsec.

Configure Symmetric Peer Crypto Access Lists

Cisco.com

```
RouterA (config)# access - list 110 permit tcp
10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255

RouterB (config)# access - list 101 permit tcp
10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

- You must configure mirror image ACLs.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-5-8

You must configure symmetric crypto ACLs for use by IPsec. Both inbound and outbound traffic are evaluated against the same outbound IPsec ACL. The ACL criteria are applied in the forward direction to traffic exiting your router, and the reverse direction to traffic entering your router. When a router receives encrypted packets back from an IPsec peer, it uses the same ACL to determine which inbound packets to decrypt by viewing the source and destination addresses in the ACL in reverse order.

The example shown in the figure illustrates why symmetric ACLs are recommended. For site 1, IPsec protection is applied to traffic between hosts on the 10.0.1.0 network as the data exits the RouterA 0 interface enroute to site 2 hosts on the 10.0.2.0 network. For traffic from site 1 hosts on the 10.0.1.0 network to site 2 hosts on the 10.0.2.0 network, the ACL entry on RouterA is evaluated as follows:

- source = hosts on 10.0.1.0 network
- destination = hosts on 10.0.2.0 network

For incoming traffic from site 2 hosts on the 10.0.2.0 network to site 1 hosts on the 10.0.1.0 network, that same ACL entry on RouterA is evaluated as follows:

- source = hosts on 10.0.2.0 network
- destination = hosts on 10.0.1.0 network

Crypto Maps Functionality

This topic describes the purpose of crypto maps. It also examines the **crypto map** command and considers example crypto maps. Crypto map entries must be created for IPsec to set up SAs for traffic flows that must be encrypted.

Purpose of Crypto Maps

Cisco.com

Crypto maps pull together the various parts configured for IPsec, including:

- The traffic to be protected by IPsec and a set of SAs
- The local address to be used for the IPsec traffic
- The destination location of IPsec-protected traffic
- The IPsec type to be applied to this traffic
- The method of establishing SAs (manually or via RSA)
- Other parameters needed to define an IPsec SA

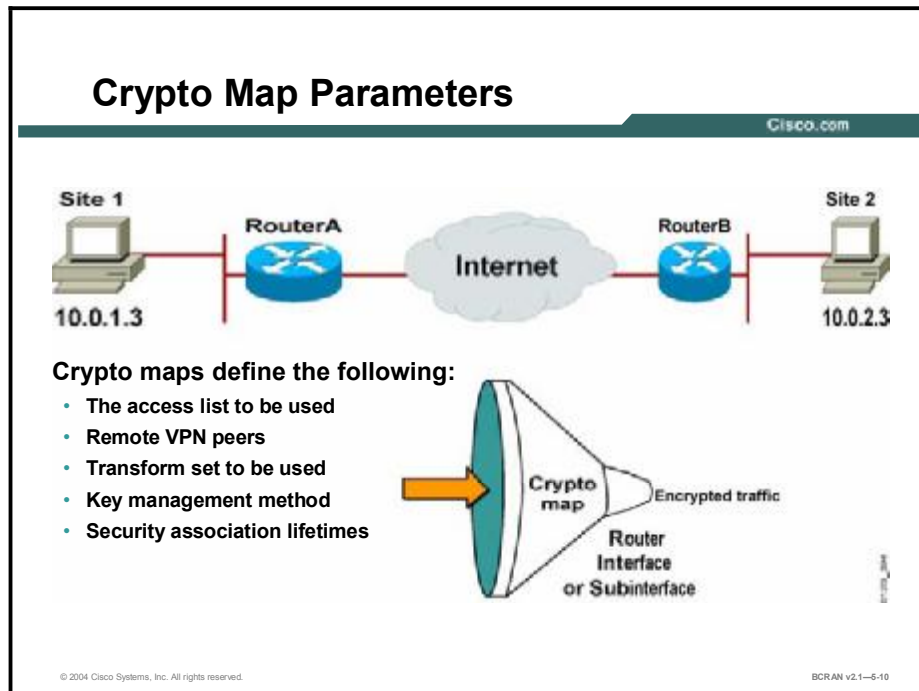
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-5.9

Crypto map entries that are created for IPsec set up SA parameters, thus tying together the various parts that are configured for IPsec, including:

- **The traffic to be protected by IPsec and a set of SAs (crypto ACL):** The access list defines the address, protocol, and port information for traffic that will be encrypted.
- **The local address to be used for the IPsec traffic:** The source address specified by the access list and the crypto map peer define the local address for IPsec traffic.
- **The destination location of IPsec-protected traffic:** The destination specified by the access list defines the identity of the remote IPsec peer.
- **The type IPsec security applied to this traffic:** The transform set applies the method of encryption and authentication.
- **The method of SA establishment:** This establishment may be completed manually (pre-shared) or through RSA.
- **Other:** Other parameters that might be necessary to define an IPsec SA.

Crypto Map Parameters

This topic describes the use of crypto maps and their parameters.



You can apply only one crypto map set to a single interface. The crypto map set can include a combination of Cisco Encryption Technology (CET) and IPSec using IKE. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces. If you create more than one crypto map entry for a given interface, use the sequence number (*seq-num*) of each map entry to rank the map entries; the lower the *seq-num*, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first.

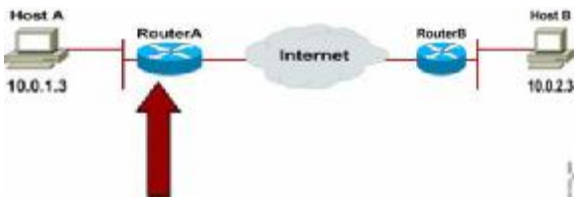
You must create multiple crypto map entries for a given interface if any of these conditions exist:

- If different data flows are to be handled by separate IPSec peers.
- If you want to apply different IPSec security to different types of traffic (to the same or separate IPSec peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case, the different types of traffic should be defined in two separate ACLs, and you must create a separate crypto map entry for each crypto ACL.
- If you are not using IKE to establish a particular set of security associations, and you want to specify multiple ACL entries, you must create separate ACLs (one per permit entry) and specify a separate crypto map entry for each ACL.

Step 4: Configure IPsec Crypto Maps

This topic describes the use of the IPsec **crypto map** command.

Step 4—Configure IPsec Crypto Maps



Cisco.com

```
router(config)#  
crypto map map-name seq-num ipsec-manual  
  
crypto map map-name-seq-num ipsec-isakmp  
[dynamic dynamic-map-name]  
  
RouterA(config)# crypto map mymap 110 ipsec-isakmp
```

- Use a different sequence number for each peer.
- Multiple peers can be specified in a single crypto map for redundancy.
- Use one crypto map per interface.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5-11

You must use the **crypto map** global configuration command to create or modify a crypto map entry and enter the crypto map configuration mode. Set the crypto map entries that reference dynamic maps to the lowest priority in a crypto map set (that is, they should have the highest sequence numbers). Use the **no** form of this command to delete a crypto map entry or set. The command syntax and parameter definitions are as follows:

```
crypto map map-name seq-num cisco  
crypto map map-name seq-num ipsec-manual  
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]  
no crypto map map-name [seq-num]
```


crypto map *map-name seq-num* Command

Command	Description
cisco	(Default value) Indicates that CET will be used instead of IPSec for protecting the traffic specified by this newly specified crypto map entry.
map-name	The name you assign to the crypto map set.
seq-num	The number you assign to the crypto map entry.
ipsec-manual	Indicates that ISAKMP will not be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	Indicates that ISAKMP will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Dynamic	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If you use this keyword, none of the crypto map configuration commands are available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.

When you enter the **config-crypto-map** command, you invoke the crypto map configuration mode with the following available commands:

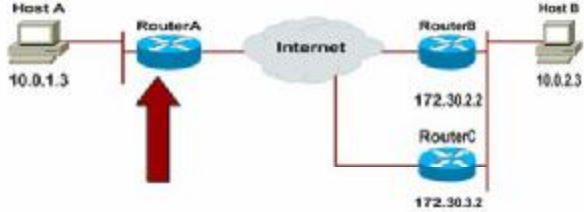
```
router(config-crypto-map)# help
  match address [access-list-id | name]
  peer [hostname | ip-address]
  transform-set [set_name(s)]
  security-association [inbound|outbound]
  set
  no
  exit
```

Crypto Map Commands Example

This topic illustrates an example of a crypto map.

Example Crypto Map Commands

Cisco.com



```
RouterA(config)# crypto map mymap 10 ipsec-isakmp
RouterA(config-crypto-map)# match address 110
RouterA(config-crypto-map)# set peer 172.30.2.2
RouterA(config-crypto-map)# set peer 172.30.3.2
RouterA(config-crypto-map)# set pfs group1
RouterA(config-crypto-map)# set transform-set mize
RouterA(config-crypto-map)# set security-association lifetime seconds 86400
```

- Multiple peers can be specified for redundancy.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-12

The figure illustrates a crypto map with two peers specified for redundancy. If the first peer cannot be contacted, the second peer is used. There is no limit to the number of redundant peers that can be configured.

The **crypto map** command is used in crypto map configuration mode with the commands shown in the following table.

config-crypto-map Command

Command	Description
set	Used with the peer , pfs , transform-set , and security-association commands.
peer [<i>hostname</i> <i>ip-address</i>]	Specifies the allowed IPSec peer by IP address or hostname.
pfs [<i>group1</i> <i>group2</i>]	Specifies Diffie-Hellman Group 1 or Group 2.
transform-set [<i>set_name(s)</i>]	Specify list of transform sets in priority order. For an ipsec-manual crypto map, you can specify only one transform set. For an ipsec-isakmp or dynamic crypto map entry, you can specify up to six transform sets.
security-association lifetime	Sets security association lifetime parameters in seconds or kilobytes.
match address [<i>access-list-id</i> <i>name</i>]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.
no	Used to delete commands entered with the set command.
exit	Exits crypto map configuration mode.

After you define crypto map entries, you can assign the crypto map set to interfaces that use the **crypto map** (interface configuration) command.

Note	ACLs for crypto map entries tagged as ipsec-manual are restricted to a single permit entry, and subsequent entries are ignored. The SAs established by that particular crypto map entry are for a single data flow only. To be able to support multiple manually established SAs for different kinds of traffic, you must define multiple crypto ACLs and then apply each one to a separate ipsec-manual crypto map entry. Each ACL should include one permit statement that defines the traffic that it must protect.
-------------	--

Step 5: Apply Crypto Maps to Interfaces

This topic describes the last step in configuring IPSec, which is to apply the crypto map set to an interface.

Step 5—Applying Crypto Maps to Interfaces

Cisco.com

```
router(config-if)#  
crypto map map-name
```

```
RouterA (config)# interface ethernet0/1  
RouterA (config-if)# crypto map mymap
```

- Apply the crypto map to outgoing interface
- Activates the IPSec policy

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5-13

Apply the crypto map to the interface of the IPSec router connected to the Internet with the **crypto map** command in interface configuration mode. Use the **no** form of the command to remove the crypto map set from the interface. The command syntax and parameter definition are as follows:

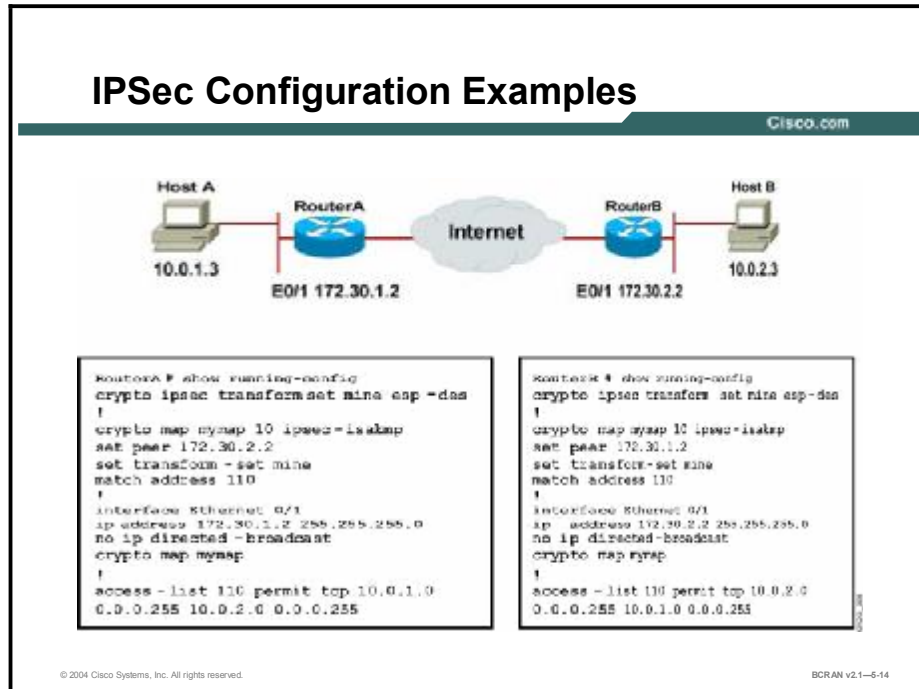
```
crypto map map-name
```

crypto map *map-name* Command

Command	Description
map-name	This is the name that identifies the crypto map set, and is the name assigned when the crypto map is created.

IPSec Configuration Examples

This topic illustrates an IPSec configuration example for two routers.



Consider the configuration example for RouterA and RouterB in the figure and as follows.

Note More complete commands relating to what has been covered so far in this lesson are shown in output.

```
RouterA# show running-config
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp key cisco1234 address 172.30.2.2
!
crypto ipsec transform-set mine esp-des
!
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.2.2
set transform-set mine
match address 110
!
interface Ethernet0/1
```

```

ip address 172.30.1.2 255.255.255.0
ip access-group 101 in
crypto map mymap
!
access-list 101 permit ahp host 172.30.2.2 host 172.30.1.2
access-list 101 permit esp host 172.30.2.2 host 172.30.1.2
access-list 101 permit udp host 172.30.2.2 host 172.30.1.2 eq
isakmp
access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0
0.0.0.255
access-list 110 deny ip any any

```

```

RouterB# show running-config
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp key cisco1234 address 172.30.1.2
!
crypto ipsec transform-set mine esp-des
!
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.1.2
set transform-set mine
match address 110
!
interface Ethernet0/1
ip address 172.30.2.2 255.255.255.0
ip access-group 101 in
crypto map mymap
!
access-list 101 permit ahp host 172.30.1.2 host 172.30.2.2
access-list 101 permit esp host 172.30.1.2 host 172.30.2.2
access-list 101 permit udp host 172.30.1.2 host 172.30.2.2 eq
isakmp
access-list 110 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0
0.0.0.255
access-list 110 deny ip any any

```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configure transform set suites with the** `crypto ipsec transform-set` **command.**
- **Configure global IPSec security association lifetimes with the** `crypto ipsec security-association lifetime` **command.**
- **Configure crypto ACLs with the** `access-list` **command.**
- **Configure crypto maps with the** `crypto map` **command.**
- **Apply the crypto maps to the terminating and originating interface with the** `interface` **and** `crypto map` **commands.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—6-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Configuring IPSec requires the user to create an IPSec list in place of an access list.
- A) true
 - B) false
- Q2) A router must have only one transform set in its running configuration in order for IPSec to function properly.
- A) true
 - B) false
- Q3) When are transform sets negotiated?
- A) on the initial router configuration
 - B) during IKE Phase 1
 - C) during IKE Phase 2
 - D) transform sets do not need to be negotiated
- Q4) Crypto SA lifetimes may be configured either globally, or per SA.
- A) true
 - B) false
- Q5) What is the function of a crypto ACL?
- A) defines the source IP address of the IPSec traffic
 - B) defines the destination IP address of the IPSec traffic
 - C) provides protocol information for traffic that will be encrypted
 - D) all of the above
- Q6) The crypto access list takes the *exact* same form as an extended access list.
- A) true
 - B) false
- Q7) Which statement correctly describes access lists that are used to define IPSec peers on routers sending and receiving to each other?
- A) They must be identical.
 - B) They must be identical, but each router can also have other access lists.
 - C) They do not need to be related.
 - D) They must be mirror images of each other, but each router can also have other access lists.

- Q8) Which of the following *cannot* be done by crypto maps?
- A) define destination traffic for IPSec
 - B) define source traffic for IPSec
 - C) define the number of IPSec conversations that a router can maintain
 - D) specify the granularity of traffic protected by SAs
- Q9) What is the number of crypto maps that can be created on an interface?
- A) 0; crypto maps are global
 - B) 1
 - C) 2
 - D) an unlimited number of crypto maps
- Q10) Which of the following commands are optional commands when you are configuring IPSec crypto maps?
- A) *sequence number*
 - B) **dynamic** *dynamic map name*
 - C) *map name*
 - D) *IPSec tuning number*
- Q11) The **crypto map peer** command may be either a hostname or an IP address.
- A) true
 - B) false
- Q12) Crypto maps must be applied to interfaces based on the map name interface number.
- A) true
 - B) false
- Q13) Based on the access lists, ping (ICMP) traffic will be allowed into RouterA Ethernet 0/1 interface from any source on the Internet.
- A) true
 - B) false

Quiz Answer Key

- Q1) B
Relates to: IPSec Configuration
- Q2) B
Relates to: Step 1: Configure Transform Set Suites
- Q3) C
Relates to: Set Negotiation Transformation
- Q4) A
Relates to: Step 2: Configure Global IPSec Security Association Lifetimes
- Q5) D
Relates to: Crypto Access Lists Functionality
- Q6) A
Relates to: Step 3: Create Crypto ACLs Using Extended Access Lists
- Q7) D
Relates to: Symmetric Peer Crypto Access Lists Configuration
- Q8) C
Relates to: Crypto Maps Functionality
- Q9) B
Relates to: Crypto Map Parameters
- Q10) B
Relates to: Step 4: Configure IPSec Crypto Maps
- Q11) A
Relates to: Crypto Map Commands Example
- Q12) A
Relates to: Step 5: Apply Crypto Maps to Interfaces
- Q13) B
Relates to: IPSec Configuration Examples

Task 4: Testing and Verifying IPsec

Overview

Cisco IOS software contains a number of **show**, **clear**, and **debug** commands that are useful for testing and verifying IPsec and ISAKMP. These commands are considered in this lesson.

Relevance

In order to implement IPsec, it is necessary to be able to test and verify that IPsec is functioning properly.

Objectives

Upon completing this lesson, you will be able to:

- List the commands to test and verify IPsec
- Describe the use of the **show crypto isakmp policy** command
- Describe the use of the **show crypto ipsec transform-set** command
- Describe the use of the **show crypto ipsec sa** command
- Describe the use of the **show crypto map** command
- Describe the use of the **clear crypto isakmp** command
- Describe the use of the **debug crypto** command
- Describe how to interpret crypto error messages for ISAKMP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Task 4: Test and Verify IPsec
- The **show crypto isakmp policy** Command
- The **show crypto ipsec transform-set** Command
- The **show crypto ipsec sa** Command
- The **show crypto map** Command
- The **clear** Commands
- The **debug crypto** Commands
- Crypto System Error Messages for ISAKMP
- Summary
- Quiz

Task 4: Test and Verify IPsec

This topic describes the commands that are used to test and verify IPsec.

Task 4—Test and Verify IPsec

Cisco.com

- Task 1 – Prepare for IKE and IPsec
- Task 2 – Configure IKE
- Task 3 – Configure IPsec
- Task 4 – Test and Verify IPsec
 - Display your configured IKE policies.
show crypto isakmp policy (**show isakmp policy** on a PIX)
 - Display your configured transform sets.
show crypto ipsec transform set
 - Display Phase I security associations.
show crypto isakmp sa (**show isakmp sa** on a PIX)
 - Display the current state of your IPsec SAs.
show crypto ipsec sa
 - Display your configured crypto maps.
show crypto map
 - Enable debug output for IPsec events.
debug crypto ipsec
 - Enable debug output for ISAKMP events.
debug crypto isakmp

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1–6.2

You can perform the following actions to test and verify that you have correctly configured the VPN using Cisco IOS software:

- Display your configured IKE policies using the **show crypto isakmp policy** command.
- Display your configured transform sets using the **show crypto ipsec transform set** command.
- Display the current state of your IPsec SAs with the **show crypto ipsec sa** command.
- View your configured crypto maps with the **show crypto map** command.
- Debug IKE and IPsec traffic through Cisco IOS software with the **debug crypto ipsec** and **debug crypto isakmp** commands.


Note The Cisco PIX IPsec troubleshooting commands are very similar to the Cisco IOS commands. Differences in the “isakmp” versus “crypto isakmp” statements are noted in the figure.

The *show crypto isakmp policy* Command

This topic illustrates an example of the **show crypto isakmp policy** command.

show crypto isakmp policy

Cisco.com



```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
 hash algorithm:        Message Digest 5
 authentication method:  sha
 Diffie-Hellman group:  #1 (768 bit)
 lifetime:               86400 seconds, no volume limit
Default protection suite
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
 hash algorithm:        Secure Hash Standard
 authentication method:  Rivest-Shamir-Adleman Signature
 Diffie-Hellman group:  #1 (768 bit)
 lifetime:               86400 seconds, no volume limit
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-53

Use the **show crypto isakmp policy** EXEC command to view the parameters for each ISAKMP policy as shown in the following example for RouterA:


```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm:  DES - Data Encryption Standard
 (56 bit keys).
 hash algorithm:        Message Digest 5
 authentication method:  Rivest-Shamir-Adleman Encryption
 Diffie-Hellman group:  #1 (768 bit)
 lifetime:               86400 seconds, no volume limit
Default protection suite
 encryption algorithm:  DES - Data Encryption Standard
 (56 bit keys).
 hash algorithm:        Secure Hash Standard
 authentication method:  Rivest-Shamir-Adleman Signature
 Diffie-Hellman group:  #1 (768 bit)
 lifetime:               86400 seconds, no volume limit
```

The *show crypto ipsec transform-set* Command

This topic illustrates an example of the `show crypto ipsec transform-set` command.

show crypto ipsec transform-set show crypto isakmp sa30

Cisco.com



```
RouterA # show crypto ipsec transform-set
Transform set mine: { esp-des }
will negotiate = { Tunnel, },
```

- View the currently defined transform sets.

```
RouterA # show crypto isakmp sa
dst          src          state  conn-id  slot
172.30.2.2   172.30.1.2   QM_IDLE  47       5
```

- Shows Phase I security associations.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.4

Use the `show crypto ipsec transform-set EXEC` command to view the configured transform sets. The command has the following syntax:

```
show crypto ipsec transform-set [tag transform-set-name]
```

show crypto ipsec transform-set Command

Command	Description
<code>tag transform-set-name</code>	(Optional) Shows only the transform sets with the specified transform-set-name

If no *transform-set-name* keyword is used, all transform sets configured at the router are displayed.


Use the `show crypto isakmp sa` command to show Phase I SAs. If the connection is working properly and an ISAKMP SA exists, it will be in its quiescent state—`QM_IDLE`—indicating that the ISAKMP SA is present but idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges.

The `show crypto ipsec sa` Command

This topic illustrates an example of the `show crypto ipsec sa` command.

show crypto ipsec sa

Cisco.com



```

RouterA# show crypto ipsec sa
interface: Ethernet0/1
  Crypto map tag: mymap, local addr: 172.30.1.2
    local ident (addr/mask/prot/port): (172.30.1.2/255.255.255.0/0)
    remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.0/0)
    current_peer: 172.30.2.2
      PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
    #send errors 0, #recv errors 0
    local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
    path mtu 1500, media mtu 1500
    current outbound spi: 8AE1C9C
    
```

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1-5.5

Use the `show crypto ipsec sa EXEC` command to view the settings used by current SAs. If no keyword is used, all security associations are displayed. The command syntax is as follows:

```
show crypto ipsec sa [map map-name | address | identity]
[detail]
```

show crypto ipsec sa Command


Command	Description
<code>map map-name</code>	(Optional) Shows any existing SAs created for the crypto map.
<code>address</code>	(Optional) Shows all the existing SAs, sorted by the destination address and then by protocol (Authentication Header [AH] or Encapsulating Security Payload [ESP]).
<code>identity</code>	(Optional) Shows only the flow information. It does not show the SA information.
<code>detail</code>	(Optional) Shows detailed error counters. (The default is the high-level send and receive error counters.)

The *show crypto map* Command

This topic illustrates an example of the **show crypto map** command.

show crypto map

Cisco.com



```
graph LR
    HA[Host A  
10.0.1.3] --- RA[Router A  
E0/1 172.30.1.2]
    RA --- Internet((Internet))
    Internet --- RB[Router B  
E0/1 172.30.2.2]
    RB --- HB[Host B  
10.0.2.3]
```

```
RouterA#show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
Peer = 172.30.2.2
Extended IP access list 102
access list 102 permit ip host 172.30.1.2 host
172.30.2.2
Current peer: 172.30.2.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ mine, }
```

- View the currently configured crypto maps.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.6

Use the **show crypto map EXEC** command to view the crypto map configuration. If no keywords are used, all crypto maps configured at the router will be displayed. The command syntax is as follows:

```
show crypto map [interface interface | tag map-name]
```

show crypto map Command

Command	Description
<i>interface interface</i>	(Optional) Shows only the crypto map set applied to the specified interface
<i>tag map-name</i>	(Optional) Shows only the crypto map set with the specified map-name.

The *clear* Commands

This topic illustrates an example of the **clear** commands for when you are changing or troubleshooting VPN tunnels.

clear Commands

Cisco.com

```
router#  
clear crypto sa  
clear crypto sa peer <IP address | peer name>  
clear crypto sa map <map name>  
clear crypto sa entry <destination address protocol spi>
```

- Clears IPsec SAs in router's database

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-7

The **clear** commands are helpful to use after altering VPN configurations. When changing transform sets and global lifetimes, the changes will not all be applied to existing IPsec connections. To ensure that these settings affect all VPN connections, the **clear** commands must be used. If a VPN device is processing a great deal of IPsec traffic that should remain uninterrupted, the **clear** commands may be applied to specific maps, entries, or peers, if specified within the command.

Note Using **clear** commands requires reestablishment of the VPN tunnel between devices and might cause inconvenience to the user.

The **clear** commands are also beneficial when troubleshooting VPN connectivity. They can show if SAs are no longer being built by peers. By comparing results of **show** commands before and after **clear** commands are used, it is often apparent that ISAKMP or IPsec SAs are not created after making a network change.

Occasionally, the Address Resolution Protocol (ARP) table will interfere with establishment or changes to IPsec tunnels and must be cleared. This ARP table interference occurs more often in PIX VPN configurations and can be remedied by clearing the ARP cache. Although not an IPsec-specific **clear** command, use the **clear arp** command to clear the ARP cache.

The *debug crypto* Commands

This topic illustrates an example of the **debug crypto** commands.

debug crypto

Cisco.com

router#
debug crypto ipsec

- Displays debug messages about all IPsec actions

router#
debug crypto isakmp

- Displays debug messages about all ISAKMP actions

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.8

Use the **debug crypto ipsec EXEC** and the **debug crypto isakmp** commands to display IPsec and ISAKMP events. The **no** form of these commands disables debugging output.

Note Because this command generates a significant amount of output for every IP packet processed, use it only when traffic on the IP network is low so that other activity on the system is not adversely affected.

The following example of ISAKMP and IPsec debugging shows normal IPsec setup messages. Note the inline comments (!).

```
RouterA# debug crypto ipsec
Crypto IPSEC debugging is on
RouterA# debug crypto isakmp
Crypto ISAKMP debugging is on
RouterA#
*Feb 29 08:08:06.556 PST: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.30.1.2, dest= 172.30.2.2,
  src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
  dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 3600s and 4608000kb,
```

spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004

! Interesting traffic from Site1 to Site2 triggers ISAKMP Main Mode.

*Feb 29 08:08:06.556 PST: ISAKMP (4): beginning Main Mode exchange
*Feb 29 08:08:06.828 PST: ISAKMP (4): processing SA payload. message ID = 0
*Feb 29 08:08:06.828 PST: ISAKMP (4): Checking ISAKMP transform 1 against priority 100 policy
*Feb 29 08:08:06.828 PST: ISAKMP: encryption DES-CBC
*Feb 29 08:08:06.828 PST: ISAKMP: hash MD5
*Feb 29 08:08:06.828 PST: ISAKMP: default group 1
*Feb 29 08:08:06.832 PST: ISAKMP: auth pre-share
*Feb 29 08:08:06.832 PST: ISAKMP (4): atts are acceptable. Next payload is 0

! The IPsec peers have found a matching ISAKMP policy

*Feb 29 08:08:06.964 PST: ISAKMP (4): SA is doing pre-shared key authentication

! Preshared key authentication is identified

*Feb 29 08:08:07.368 PST: ISAKMP (4): processing KE payload. message ID = 0
*Feb 29 08:08:07.540 PST: ISAKMP (4): processing NONCE payload. message ID = 0
*Feb 29 08:08:07.540 PST: ISAKMP (4): SKEYID state generated
*Feb 29 08:08:07.540 PST: ISAKMP (4): processing vendor id payload
*Feb 29 08:08:07.544 PST: ISAKMP (4): speaking to another IOS box!
*Feb 29 08:08:07.676 PST: ISAKMP (4): processing ID payload. message ID = 0
*Feb 29 08:08:07.676 PST: ISAKMP (4): processing HASH payload. message ID = 0
*Feb 29 08:08:07.680 PST: ISAKMP (4): SA has been authenticated with 172.30.2.2

! Main mode is complete. The peers are authenticated, and secret keys are generated. On to Quick Mode!

*Feb 29 08:08:07.680 PST: ISAKMP (4): beginning Quick Mode exchange, M-ID of -1079597279
*Feb 29 08:08:07.680 PST: IPSEC(key_engine): got a queue event...
*Feb 29 08:08:07.680 PST: IPSEC(spi_response): getting spi 3658276911d for SA

from 172.30.2.2 to 172.30.1.2 for prot 3

*Feb 29 08:08:08.424 PST: ISAKMP (4): processing SA payload. message ID = -1079597279
*Feb 29 08:08:08.424 PST: ISAKMP (4): Checking IPsec proposal 1
*Feb 29 08:08:08.424 PST: ISAKMP: transform 1, ESP_DES
*Feb 29 08:08:08.424 PST: ISAKMP: attributes in transform:
*Feb 29 08:08:08.424 PST: ISAKMP: encaps is 1
*Feb 29 08:08:08.424 PST: ISAKMP: SA life type in seconds

```

*Feb 29 08:08:08.424 PST: ISAKMP:      SA life duration (basic) of
3600
*Feb 29 08:08:08.428 PST: ISAKMP:      SA life type in kilobytes
*Feb 29 08:08:08.428 PST: ISAKMP:      SA life duration (VPI) of  0x0
0x46 0x50 0x0
*Feb 29 08:08:08.428 PST: ISAKMP:      authenticator is HMAC-MD5
*Feb 29 08:08:08.428 PST: ISAKMP (4):  atts are acceptable.
*Feb 29 08:08:08.428 PST: IPSEC(validate_proposal_request): proposal
part #1,
    (key eng. msg.) dest= 172.30.2.2, src= 172.30.1.2,
    dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Feb 29 08:08:08.432 PST: ISAKMP (4):  processing NONCE payload.
message ID = -10
79597279
*Feb 29 08:08:08.432 PST: ISAKMP (4):  processing ID payload. message
ID = -1079597279
*Feb 29 08:08:08.432 PST: ISAKMP (4):  processing ID payload. message
ID = -1079597279

! A matching IPsec policy has been negotiated and authenticated.
! Next the SAs are set up.
*Feb 29 08:08:08.436 PST: ISAKMP (4):  Creating IPsec SAs
*Feb 29 08:08:08.436 PST:      inbound SA from 172.30.2.2      to
172.30.1.2
    (proxy 10.0.2.0      to 10.0.1.0      )
*Feb 29 08:08:08.436 PST:      has spi 365827691 and conn_id 5 and
flags 4
*Feb 29 08:08:08.436 PST:      lifetime of 3600 seconds
*Feb 29 08:08:08.440 PST:      lifetime of 4608000 kilobytes
*Feb 29 08:08:08.440 PST:      outbound SA from 172.30.1.2      to
172.30.2.2
    (proxy 10.0.1.0      to 10.0.2.0      )
*Feb 29 08:08:08.440 PST:      has spi 470158437 and conn_id 6 and
flags 4
*Feb 29 08:08:08.440 PST:      lifetime of 3600 seconds
*Feb 29 08:08:08.440 PST:      lifetime of 4608000 kilobytes
*Feb 29 08:08:08.440 PST: IPSEC(key_engine): got a queue event...
*Feb 29 08:08:08.440 PST: IPSEC(initialize_sas): ,
    (key eng. msg.) dest= 172.30.1.2, src= 172.30.2.2,
    dest_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,

```

```
spi= 0x15CE166B(365827691), conn_id= 5, keysize= 0, flags= 0x4
*Feb 29 08:08:08.444 PST: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.30.1.2, dest= 172.30.2.2,
src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x1C060C65(470158437), conn_id= 6, keysize= 0, flags= 0x4
*Feb 29 08:08:08.444 PST: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.30.1.2, sa_prot= 50,
sa_spi= 0x15CE166B(365827691),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 5
*Feb 29 08:08:08.444 PST: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.30.2.2, sa_prot= 50,
sa_spi= 0x1C060C65(470158437),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 6
! IPsec SAs are set up and data can be securely exchanged.
RouterA#
```

Crypto System Error Messages for ISAKMP

This topic describes how to interpret crypto error messages for ISAKMP.

Crypto System Error Messages for ISAKMP

Cisco.com

```
%CRYPTO -6-IKMP_SA_NOT_AUTH: Cannot accept Quick Mode exchange from %15i if SA is not authenticated!
```

- ISAKMP SA with the remote peer was not authenticated.

```
%CRYPTO -6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with attribute [chars] not offered or changed
```

- ISAKMP peers failed protection suite negotiation for ISAKMP.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.9

Cisco IOS software can generate many useful system error messages for ISAKMP. Two of the error messages are as follows:

- **%CRYPTO-6-IKMP_SA_NOT_AUTH:** Cannot accept Quick Mode exchange from %15i if SA is not authenticated—The ISAKMP security association with the remote peer was not authenticated yet the peer attempted to begin a quick mode exchange. This exchange must only be done with an authenticated SA. The recommended action is to contact the remote peer administrator to resolve the improper configuration.
- **%CRYPTO-6-IKMP_SA_NOT_OFFERED:** Remote peer %15i responded with attribute [chars] not offered or changed—ISAKMP peers negotiated policy by the initiator offering a list of possible alternate protection suites. The responder responded with an ISAKMP policy that the initiator did not offer. The recommended action is to contact the remote peer administrator to resolve the improper configuration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Display your configured IKE policies using the show crypto isakmp policy command.**
- **Display your configured transform sets using the show crypto ipsec transform set command.**
- **Display the current state of your IPSec SAs with the show crypto ipsec sa command.**
- **View your configured crypto maps with the show crypto map command.**
- **Debug IKE and IPSec traffic through the Cisco IOS with the debug crypto ipsec and debug crypto isakmp commands.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—5-10

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 5-1: Configuring a Site-to-Site IPSec VPN Using Preshared Keys

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which command displays all crypto maps?
- A) **display crypto transform**
 - B) **show crypto map**
 - C) **show crypto isakmp policy**
 - D) **debug crypto isakmp**
- Q2) The **show crypto isakmp policy** command will display the hash algorithm.
- A) true
 - B) false
- Q3) If a transform set name is not specified in the **show crypto ipsec transform-set** command, what is the result?
- A) The router will not understand the command.
 - B) It will turn on crypto ipsec debugging.
 - C) Every configured transform set will be displayed.
- Q4) The state QM_IDLE on the **show crypto isakmp sa** command means the configuration is idle and the tunnel is not working.
- A) true
 - B) false
- Q5) The **show crypto ipsec sa** shows the settings used by current security associations.
- A) true
 - B) false
- Q6) The **show crypto map** command will display peer addresses.
- A) true
 - B) false
- Q7) Clearing the full security association database should be reserved for large-scale changes, or when a device is processing only a small amount of other IPsec traffic.
- A) true
 - B) false
- Q8) Debug commands are acceptable to use on a busy network.
- A) true
 - B) false

- Q9) If a remote router responds with an unoffered ISAKMP policy, the communication will continue to function normally.
- A) true
 - B) false

Quiz Answer Key

- Q1) B
Relates to: Task 4: Test and Verify IPsec
- Q2) A
Relates to: The **show crypto isakmp policy** Command
- Q3) C
Relates to: The **show crypto ipsec transform-set** Command
- Q4) B
Relates to: The **show crypto ipsec sa** Command
- Q5) A
Relates to: The **show crypto ipsec sa** Command
- Q6) A
Relates to: The **show crypto map** Command
- Q7) A
Relates to: The **clear** Commands
- Q8) B
Relates to: The **debug crypto** Commands
- Q9) B
Relates to: Crypto System Error Messages for ISAKMP

Module 6

Using ISDN and DDR to Enhance Remote Connectivity

Overview

ISDN is typically deployed to provide remote access for small office or home office. This module reviews the configuration of dial-on-demand routing (DDR) to implement ISDN dial up for remote access.

Objectives

Upon completing this module, you will be able to:

- List the steps and commands that are required to configure an ISDN connection
- List the tasks that are required to successfully configure an ISDN PRI connection
- Configure ISDN DDR using dialer maps
- Define interesting traffic with dialer and access lists
- Explain various ISDN PPP configuration options that are used with DDR
- Verify and troubleshoot ISDN environments using Cisco IOS commands

Outline

The module contains these lessons:

- Configuring ISDN BRI
- Configuring ISDN PRI
- Configuring DDR
- Verifying ISDN and DDR Configurations

Configuring ISDN BRI

Overview

To connect to an ISDN network, you must use the correct router. A BRI interface requires specific commands to enable ISDN.

Relevance

Because ISDN is still widely used for remote access and backup connectivity, it is important to know how to configure an ISDN BRI interface. This lesson covers the concepts and commands for configuring ISDN BRI.

Objectives

Upon completing this lesson, you will be able to:

- Identify the ISDN BRI services and protocols
- List the steps and commands that are required to configure an ISDN connection
- Configure the appropriate switch type with the **isdn switch-type** command
- Configure the Layer 2 B channel encapsulation method with the **encapsulation ppp** or **encapsulation hdlc** commands
- Describe the basic concepts of ISDN SPIDs
- Configure SPIDs with the **isdn spid1** and **isdn spid2** commands
- Configure advanced calling features to accept and respond to selected ISDN calls
- Configure channel rate adaption using the **speed** command available in dialer maps

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

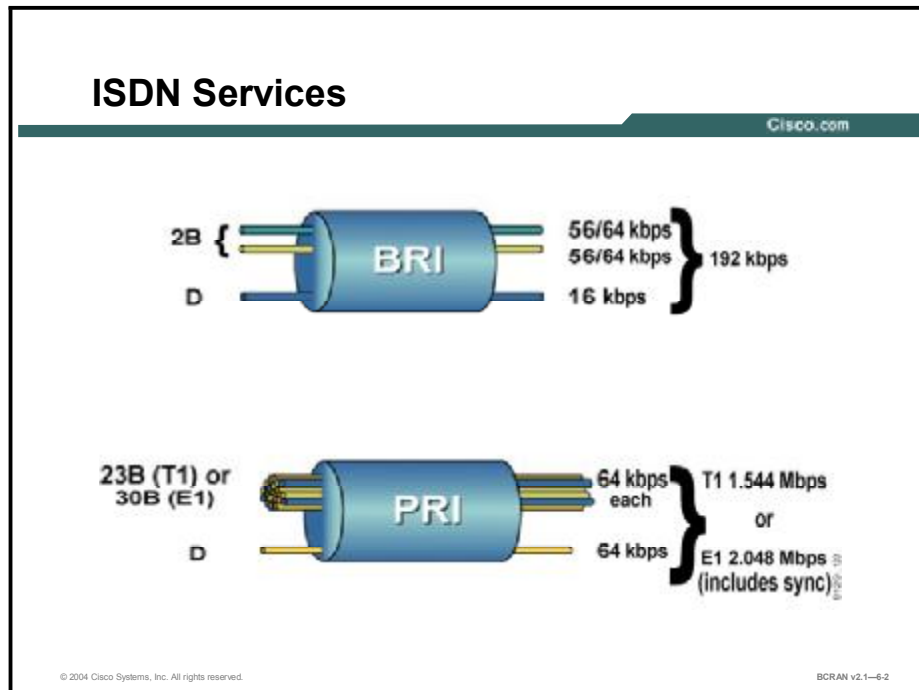
Outline

This lesson includes these topics:

- Overview
- ISDN Services
- ISDN Protocols
- ISDN Protocol Layers
- ISDN Configuration Tasks
- ISDN Configuration Commands
- ISDN Switch Types
- Interface Protocol Settings
- SPID Setting If Necessary
- Caller Identification Screening
- Configuration of Caller ID Screening
- Called-Party Number Verification
- Rate Adaption
- Summary
- Quiz

ISDN Services

This topic describes the differences between ISDN BRI and ISDN PRI. ISDN services are offered as either ISDN BRI or ISDN PRI.



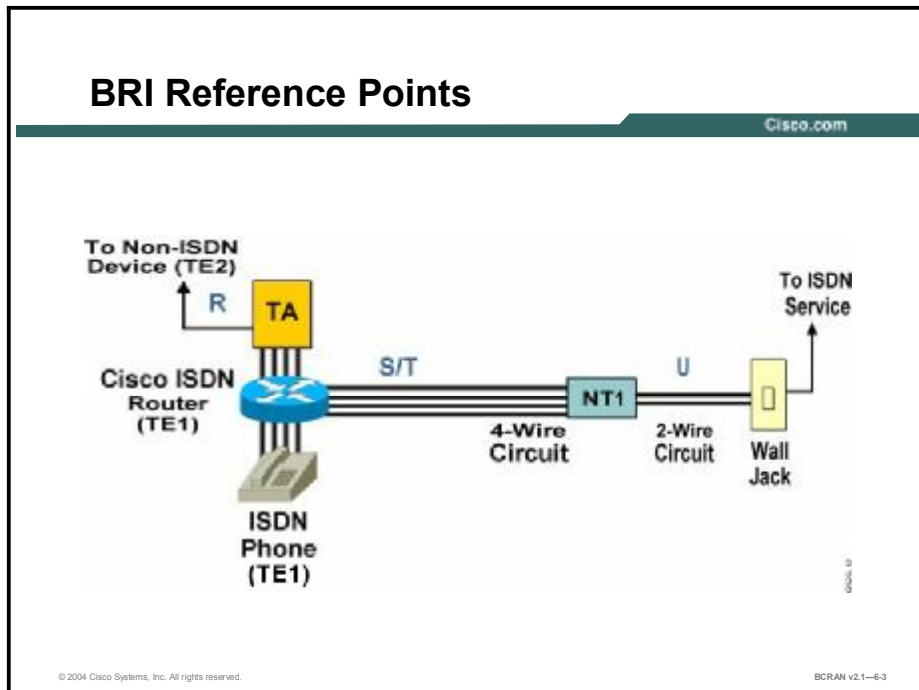
ISDN BRI specifies:

- Two 64 kbps B Channels (bearer channels) used mainly for video, data or voice
- One 16 kbps D Channel (data or delta channel) used mainly for signaling of the B Channels
- Framing and synchronization overhead at 48 kbps
- Total speed $(64 * 2) + (16 + 48) = (128 + 64) = 192$ kbps
- Intended to be used at small concentration points

Note The B channel carries the main data. The D channel carries control and signaling information.

ISDN Protocols

This topic describes the most common components and reference points of ISDN BRI. ISDN BRI includes various components and reference points.



Given all the ISDN interface abbreviations such as T, S, U, S/T, and so on, what do all of these components and reference points look like in practice?

When creating a network, connect the Network Termination 1 (NT-1) to the wall jack with a standard two-wire connector, then to the ISDN phone, terminal adapter, Cisco ISDN router, and perhaps a fax with a four-wire connector. The S/T interface is implemented using an eight-wire connector (two pairs for data transmission and two pairs for providing optional power to the NT and TE).

Because RJ-11 and RJ-45 connectors look similar, caution should be taken when connecting ISDN devices.

The S/T reference point is:

- Four-wire interface (sending [TX] and receiving [RX])
- Point-to-point and multipoint (passive bus), as shown in the figure
- Covered by International Telecommunication Union Telecommunication Standardization Sector (ITU-T) I.430 physical layer specification for BRI interfaces, and American National Standards Institute (ANSI) T1.601 standard for the United States

The S/T interface defines the interface between a TE1 or terminal adaptor (TA) and an NT. A maximum of eight devices can be daisy-chained to the S/T bus.

The U interface defines the two-wire interface between the NT-1 and the ISDN cloud. The U interface is used in the United States. Countries outside the United States use an S/T interface.

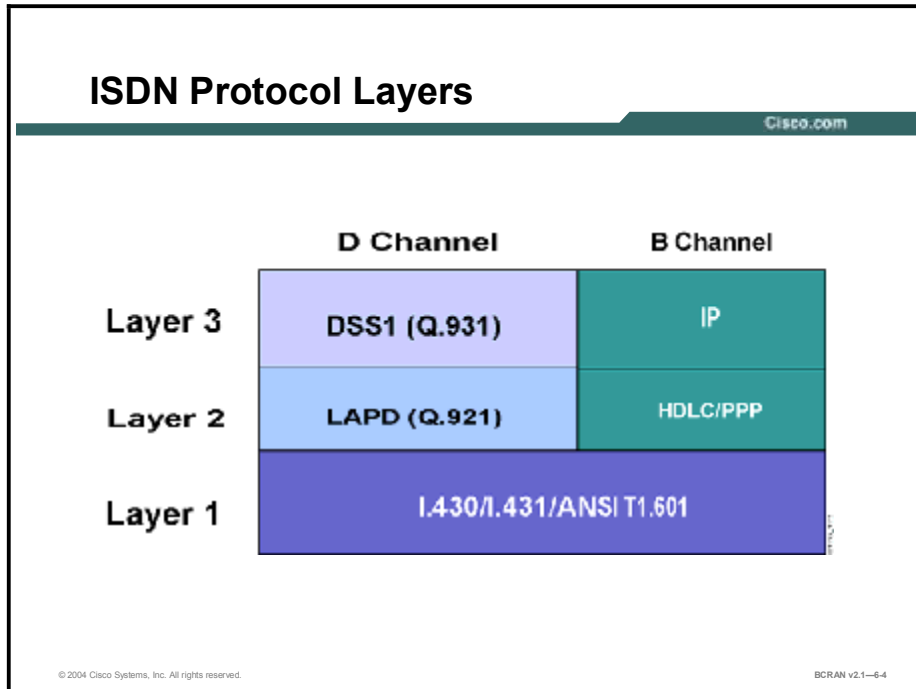
The R interface defines the interface between the TA and an attached non-ISDN device (TE2).

In North America, the NT-1 function is commonly integrated into the ISDN device (router, TA), thus permitting a direct connection from the ISDN device to the telco jack.

An NT-1 and NT-2 combination device is sometimes referred to as an NTU. In most countries, the NT-1/NT-2 combination is provided by the service provider (telco), and customer access is available only at the S/T interface.

ISDN Protocol Layers

This topic discusses ISDN protocol layers. ISDN is based on a suite of standards.



The B channel carries Layer 3 protocols for data transmission. It typically operates in either a High-Level Data Link Control (HDLC) or PPP encapsulation mode at Layer 2 to encapsulate the upper-layer protocols such as IP. Although not as common, other encapsulations such as Frame Relay can be used, depending on networking requirements.

The D channel is continuously active and works with dial-on-demand routing (DDR) to build connections over the ISDN connection. The D Channel uses Q.921 (also known as LAPD) at the Data Link Layer and Q.931 at the Network Layer. The B Channel uses PPP or HDLC at the Data Link Layer and IP, IPX, Appletalk, and so on for the Network Layer.


The ITU-T I.430 and I.431 standards define the physical layer for the BRI and PRI network interfaces, respectively. In the United States, the U and S/T interfaces are governed by the ANSI T1.601 standards and conform, where possible, to the ITU-T specifications.

ISDN Configuration Tasks

This topic describes the configuration tasks that are required to successfully configure an ISDN BRI connection. Configuring ISDN BRI requires global and interface configuration tasks.

ISDN Configuration Tasks

Cisco.com



- **Global configuration**
 - Select switch type
 - Specify traffic to trigger call
- **Interface configuration**
 - Select interface specifications
 - Configure ISDN addressing
- **Optional feature configuration**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.5

To configure an ISDN BRI interface on a router, you must use specific global and interface configuration commands.

Global configuration includes these steps:

- Step 1** Select the switch type that matches the ISDN provider switch at the central office (CO).
- Step 2** Set destination details. Indicate static routes from the router to other ISDN destinations.
- Step 3** Specify the traffic criteria that initiate an ISDN call to the appropriate destination.

Interface configuration includes these steps:

- Step 1** Select the ISDN BRI port and configure an IP address and subnet mask.

Although the interface automatically inherits the global switch-type setting, some configurations may require a specific switch type to be configured on an interface.

- Step 2** Specify the encapsulation if it is not HDLC. If PPP encapsulation is selected (typical), configure PPP including authentication, callback, and multilink options.
- Step 3** Configure ISDN addressing and any parameters supplied by the ISDN service provider.
- Step 4** Configure DDR information and calling parameters.
- Step 5** Configure optional features, including time-to-wait for the ISDN carrier to respond to the call, and seconds of idle time before the router times out and drops the call.

ISDN Configuration Commands

This topic describes the configuration commands that are required to successfully configure an ISDN BRI connection. Configuring ISDN BRI requires global and interface configuration commands.

ISDN Configuration Commands

Cisco.com

- **Global commands:**
 - isdn switch-type
- **Interface commands:**
 - ip address
 - isdn switch-type
 - encapsulation ppp
 - PPP options
(for example, Authentication, Multilink)
 - isdn spid1

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.6

At the global level, the administrator must specify the ISDN service provider CO switch type. There are several types of switches to choose from and some of these require special parameters. Because standards signaling specifics differ by region, the switch type varies according to its geographical location. For example, the DMS-100 and National-1 require a service profile identifier (SPID) to be specified. This is optional on some switches (for example, AT&T 5ESS), or may not required at all on other switches.

Although the interface configuration and selection tasks apply to all routers, this topic focuses on BRI for access routers. (PRI details for Cisco routers and access servers with T1/E1 controllers are covered in lesson two.)

Configuring the ISDN interface may include assigning the IP address, defining encapsulation, and creating ISDN service profile statements. The tasks also include a legacy method of configuring ISDN with the **dialer map** command. The **dialer map** command statically maps a remote site (usually its host name) to a destination IP address (Layer 3 address) and ISDN dial number (Layer 2 address). A more contemporary implementation includes creating dialer profiles that dynamically create these mappings. (Dialer maps are covered later in this module, and dialer profiles are covered in module 7.)

ISDN Switch Types

This topic describes the **isdn switch-type** command. Selecting the correct switch type to connect is crucial when configuring ISDN BRI.

Selecting the ISDN Switch Type

Cisco.com

```
Router(config)#isdn switch-type switch-type
```

```
Router(config-if)#isdn switch-type switch-type
```

- Specifies the type of ISDN switch with which the router communicates
- Global or interface command

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-7

Use the **isdn switch-type** command to specify the CO switch to which the router connects. For BRI ISDN service, the possible switch types and their corresponding commands are shown in the table.

isdn switch-type Commands

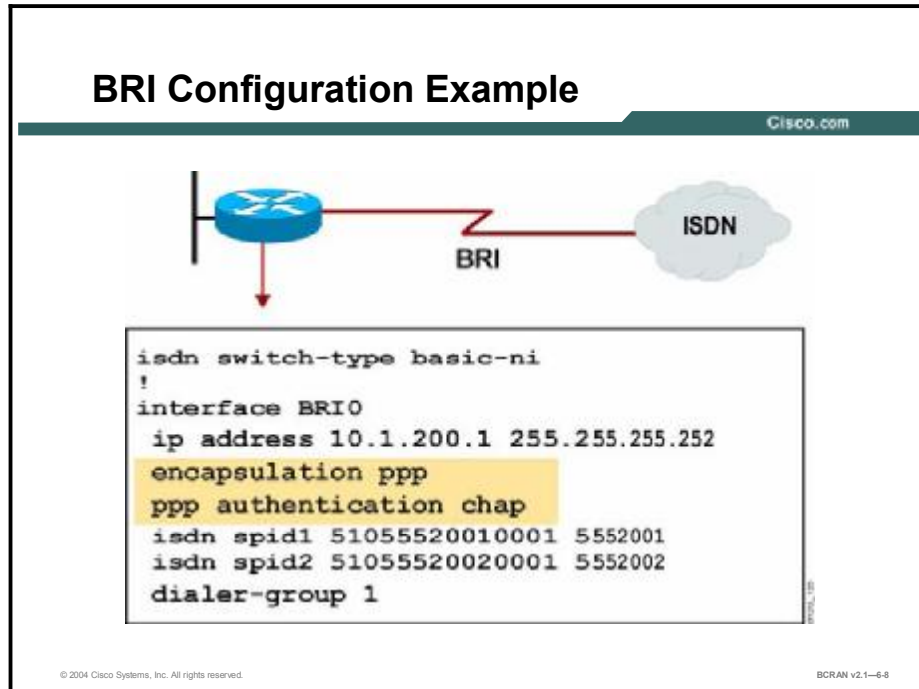
Command	Description
basic-5ess	AT&T basic rate switches (United States)
basic-dms100	NT DMS-100 (North America)
basic-ni	National ISDN-1 (North America)
basic-qsig	PINX (PBX) switches with QSIG signaling per Q.931
basic-net3	NET3 switch type for United Kingdom, Europe, Asia, and Australia
Ntt	Japanese NTT ISDN switches
none	No switch defined

Note Other switch types are available. The list of switch types can differ based on the Cisco IOS software version that is used.

When the **isdn switch-type** command is used in global configuration mode, all ISDN interfaces on the router are configured for that switch type. Beginning with Cisco IOS Release 11.3T, the **interface configuration mode** command was introduced to allow different interfaces to be configured with different switch types. If the command is used in interface configuration mode, only the interface that is configured assumes that switch type. The interface setting always overrides the global setting.

Interface Protocol Settings

This topic describes the **encapsulation ppp** and **encapsulation hdlc** commands. You may have to configure the Layer 2 B channel encapsulation protocol and authentication when configuring ISDN BRI.



The **interface bri** *interface-number* command designates the interface that is used for ISDN on a router acting as a TE1 device.

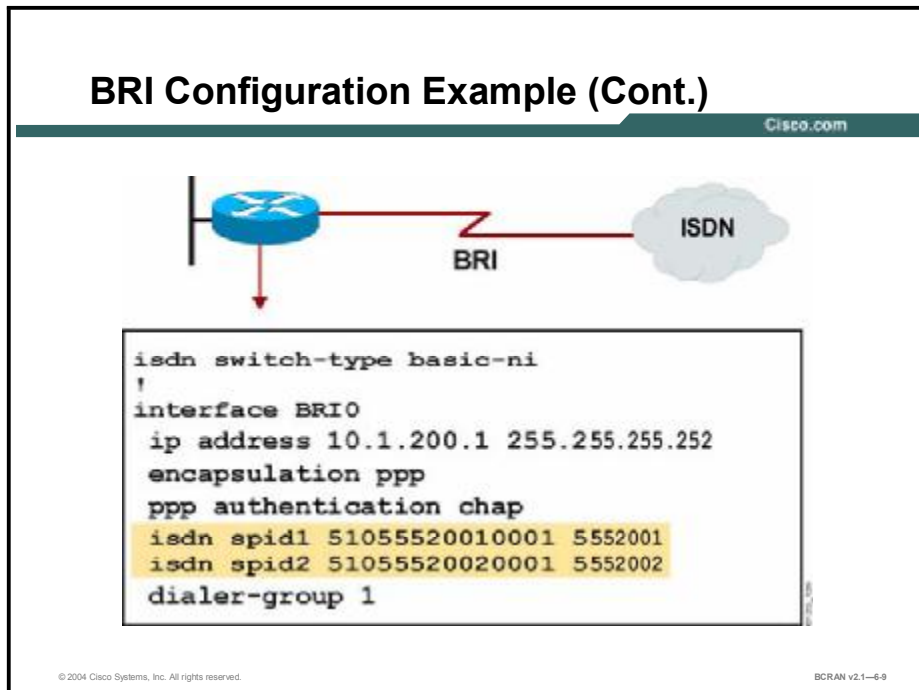
A router without a native BRI interface is a TE2 device. It must connect to an external ISDN TA via a serial interface. On a TE2 router, the **interface serial** *interface-number* command must be used.

The default encapsulation on a BRI interface is HDLC. The **encapsulation ppp** command changes the encapsulation on the ISDN interface. Although HDLC encapsulation offers a simpler configuration, it lacks much of the functionality provided by PPP. Some of the functionality that is lacking includes link control protocol (LCP) options such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication, as well as multilink capability. Authentication is typically a requirement in networks of today, particularly if calls are to be received from multiple dialup sources. Otherwise, calling line identification (CLID) can be used with HDLC encapsulation to identify callers, providing that the service provider sends this information.

To revert from PPP encapsulation to the default, use the **encapsulation hdlc** command. Other encapsulation options for BRI interfaces may include Link Access Procedure, Balanced (LAPB) and Frame Relay.

SPID Setting If Necessary

This topic describes ISDN SPIDs and the `isdn spid1` and `isdn spid2` commands. Depending on the switch type, you may have to configure SPIDs.



Several ISDN service providers use CO switches that require dial-in numbers called SPIDs. The SPIDs are used to authenticate call requests that are within contract specifications. These switches include National ISDN and DMS-100 ISDN switches, as well as the AT&T 5ESS multipoint switch. SPIDs are used only in the United States and are typically not required for ISDN data communications applications. The service provider supplies the local SPID numbers. If uncertain, contact the service provider to determine if the SPIDs must be configured on your access routers.

Use the `isdn spid1` and `isdn spid2` commands to access the ISDN network when your router makes its call to the local ISDN exchange.

The `isdn spid1` command syntax is shown in the figure for the first BRI 64-kbps channel. The field for *ldn*, if required, matches the number provided by the `dialer map` command.

The commands for **isdn spid1** and **isdn spid2** are listed in the following table.

isdn spid1 and isdn spid2 Commands

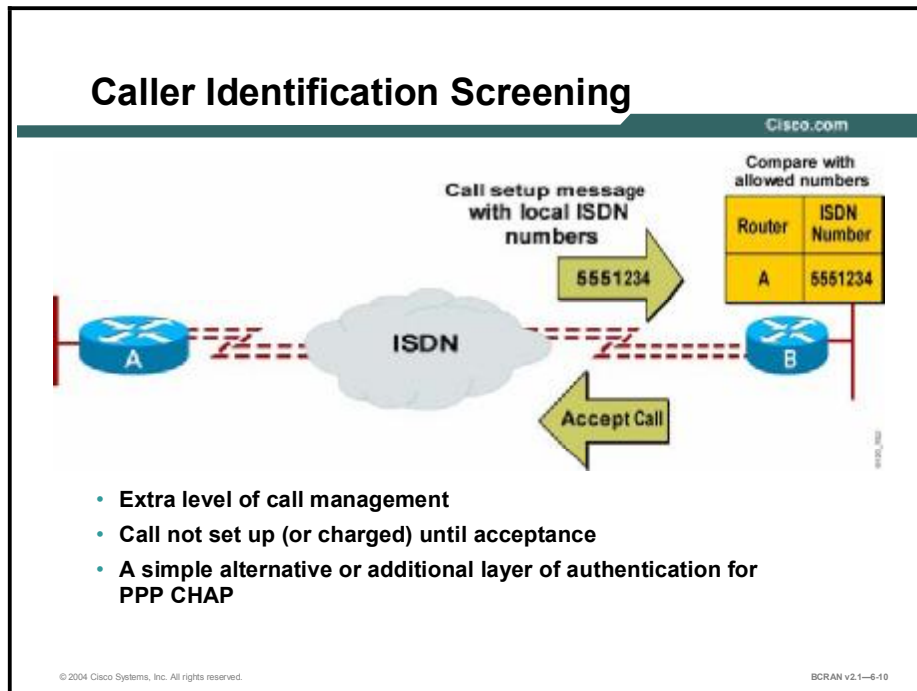
Command	Description
<i>spid-number</i>	Number identifying the service to which you have subscribed. This value is usually a ten-digit telephone number followed by more digits. The ISDN service provider assigns this value.
<i>ldn</i>	(Optional) Seven-digit local directory number assigned by the ISDN service provider.

Note If you want the SPID to be automatically detected, you can specify 0 for the *spid-number* argument. You can also use the interface command **isdn autodetect** for SPID and switch type detection. This command is available in IOS Release 12.0(3)T and later.

The *ldn* parameter allows you to associate up to three local directory numbers with each SPID. This number must match the called-party information coming in from the ISDN switch in order to use both B channels on most switches.

Caller Identification Screening

This topic describes the basic features of calling line identification (CLID).



CLID (also known as caller ID) adds a level of security between ISDN connections by screening incoming ISDN calls based on the setup request. The calling number in the call setup request message supplied by the local service provider is verified against a table of allowed numbers configured in the router.

This feature prevents charges for calls from unauthorized numbers. However, in some situations, there are charges for call setup attempts, even if the call does not pass caller ID screening.

The figure shows the router, the medium, and the connection to the ISDN cloud. The upper arrow displays the number of the calling party (RouterA). The calling party number comes from the network, not from the router that initiated the call.

The table at the right of the figure contains the allowed numbers that are configured on RouterB. Call verification using this table provides extra security. Call acceptance does not occur until the router has verified the calling number.

CLID is not universally available. Not all service providers have the calling party number contained in the call setup request. In addition, CLID screening records the number exactly as it was sent, with or without an area code prefix, which can cause errors.

Configuration of Caller ID Screening

This topic describes the commands that are required to enable CLID.

Configuring CLID Screening

Cisco.com

```
Router(config-if)#isdn caller number
```

- Enables CLID screening

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6-11

Use the **isdn caller number** command to configure ISDN CLID. This command configures the router to accept calls from the specified telephone number. More than one caller number can be assigned to an interface.

The telephone number can be up to 25 characters in length. As part of this number, you can enter an *x* in any position to stand for any number (a “wildcard”).

For example, **isdn caller 55666612xx** would accept calls from any number beginning with 55666612 followed by any other number in the last two positions.

Called-Party Number Verification

This topic describes the commands that are required to enable called-party number verification. Called-party number verification is used to ensure that the correct device answers an incoming call.

Configuring Called Party Number Verification

Cisco.com

```
Router (config-if)#isdn answer1 [called-party-number]
```

or

```
Router (config-if)#isdn answer2 [called-party-number]
```

- Sets the number to allow the interface to respond

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-12

When multiple devices and a router share the same ISDN local loop, you can ensure that the correct device answers an incoming call. This guarantee is accomplished by configuring the router to verify the called-party number. However, the ISDN switch must support the delivery of called-party numbers.

The **isdn answer1** interface configuration command verifies a called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the ISDN switch supplies the number. Use the **isdn answer2** interface command to verify an additional called-party number or subaddress number. To remove a verification request, use the **no** form of the command.

All calls are processed or accepted if you do not specify the **isdn answer1** or **isdn answer2** commands. If you specify one of these commands, the router must verify the incoming called-party number before processing or accepting the call. Devices on multipoint ISDN connections are typically assigned a specific subaddress. The **isdn answer1** command can also verify the incoming call based on the specific subaddress.

You can configure just the called-party number or just the subaddress, in which case only that part will be verified.

The table describes the arguments for the **isdn answer 1** command.

```
isdn answer1 [called-party-number] [:subaddress]
```

isdn answer1 Command

Command	Description
<i>called-party-number</i>	Number supplied in the call setup request.
:	(Optional) Identifies the number that follows as a subaddress. Use the colon (:) when you configure both the called-party number and the subaddress, or when you configure only the subaddress.
<i>subaddress</i>	(Optional) Subaddress number used for ISDN multipoint connections.


Some service providers require that both **isdn answer1** and **isdn answer2** parameters be specified.

Rate Adaption

This topic describes rate adaption. Rate adaption allows the ISDN channel to adjust to a lower speed if requested in the call setup.

BRI Rate Adaption Configuration Example

Cisco.com



```
isdn switch-type basic-ni
!
interface BRI0
 ip address 10.1.200.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 dialer map ip 10.1.200.2 name RouterB 5551212 speed 56
 dialer-group 1
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-13

If requested in the call setup by the access router, rate adaption allows the ISDN channel to adjust to a lower speed. The speed may be designated in a **dialer map** statement using the optional parameter of **speed 56** or **speed 64** on the router that is placing the call.

Use rate adaption for cases where the destination does not use the default DS-0 of 64 kbps. The alternative speed used in most of North America is 56 kbps.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **ISDN BRI: total speed is 64 kbps x 2 (B channels) + 16 kbps (D channel) + 48 kbps (framing and synchronization) = 192 kbps.**
- **In most countries, customer access to BRI is available at the S/T interface.**
- **Enabling ISDN BRI requires global configuration and interface configuration commands.**
- **A switch type can be configured in global configuration or in interface configuration mode.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-14

Summary (Cont.)

Cisco.com

- **BRI supports HDLC encapsulation and 64 kbps by default.**
- **PPP encapsulation is more advantageous because of its LCP options such as PAP, CHAP, Multilink.**
- **Some ISDN switches require the configuration of SPID numbers.**
- **BRI supports CLID and called-party number verification.**
- **Use rate adaption for 56 kbps.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the data rate of one ISDN B channel?
- A) 48 kbps
 - B) 56 kbps
 - C) 64 kbps
 - D) 128 kbps
- Q2) Which ISDN channel is always active and in communication with the ISDN switch while using the Q.931 signaling protocol?
- A) A
 - B) B
 - C) C
 - D) D
- Q3) Which ISDN channel carries network layer protocols for data transmission?
- A) A
 - B) B
 - C) C
 - D) D
- Q4) Which type of configuration task category does configuring ISDN addressing fall into?
- A) global
 - B) interface
 - C) standard
 - D) primary
- Q5) Which configuration task category level applies to specifying the ISDN service provider CO switch type?
- A) global
 - B) interface
 - C) standard
 - D) primary

- Q6) Which Cisco router global command is used to specify the CO switch to which the router connects?
- A) **isdn router-type**
 - B) **isdn switch-type**
 - C) **isdn hub-type**
 - D) **isdn bridge-type**
- Q7) Which Cisco router command designates the interface that is used for ISDN on a router acting as a TE1 device?
- A) **interface serial *interface-number***
 - B) **interface Ethernet *interface-number***
 - C) **interface bri *interface-number***
 - D) **interface ISDN *interface-number***
- Q8) The dial-in numbers that an ISDN service provider CO site switch might require are known as _____?
- A) service provider identifiers (SPIDs)
 - B) service profile identifiers (SPIDs)
 - C) service profile interface devices (SPIDs)
 - D) service provider interface devices (SPIDs)
- Q9) Which Cisco router command is used to configure ISDN CLID screening?
- A) **caller ID**
 - B) **isdn caller**
 - C) **ID caller**
 - D) **ID caller**
- Q10) Rate adaption allows the ISDN channel to adjust to which of the following:
- A) lower speed
 - B) higher speed
 - C) speed of 128 kbps
 - D) speed of 256 kbps

Quiz Answer Key

- Q1) C
Relates to: ISDN Services
- Q2) D
Relates to: ISDN Protocols
- Q3) B
Relates to: ISDN Protocol Layers
- Q4) B
Relates to: ISDN Configuration Tasks
- Q5) A
Relates to: ISDN Configuration Commands
- Q6) B
Relates to: ISDN Switch Types
- Q7) C
Relates to: Interface Protocol Settings
- Q8) B
Relates to: SPID Setting If Necessary
- Q9) B
Relates to: Configuration of Caller ID Screening
- Q10) A
Relates to: Rate Adaption

Configuring ISDN PRI

Overview

ISDN BRI is typically used for remote access at small branch sites with lower bandwidth requirements. Primary Rate Interface (PRI) is typically used by larger central sites with higher bandwidth requirements to aggregate multiple remote BRIs. Internet service providers (ISPs) also use ISDN PRI to support combined large numbers of analog modem and ISDN BRI calls.

Relevance

This lesson provides an overview of concepts and configuration of ISDN PRI.

Objectives

Upon completing this lesson, you will be able to:

- List the tasks required to successfully configure an ISDN PRI connection
- Configure the appropriate switch type with the **isdn switch-type** command
- List and explain the commands that are required to configure an ISDN T1 or E1 controller
- List and explain the commands that are required to configure the ISDN PRI channels and D channel

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

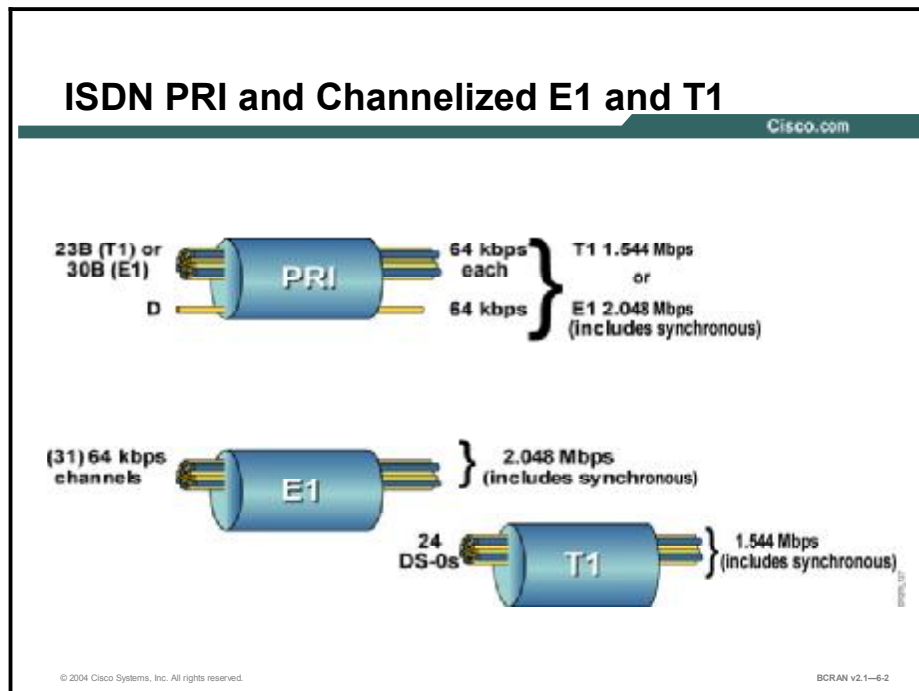
Outline

This lesson includes these topics:

- Overview
- ISDN Services
- PRI Reference Points
- Configuration Tasks for PRI
- ISDN PRI Configuration
- T1 and E1 Controller Parameters
- Additional ISDN PRI Configuration Parameters
- PRI Configuration Example
- Summary
- Quiz

ISDN Services

This topic describes the services of the ISDN PRI. ISDN services are offered as either ISDN BRI or ISDN PRI.



In the figure, the ISDN PRI specifies:

- 23 B (U.S. T1) or 30 B (European E1) channels at 64 kbps each
- 1 D channel at 64 kbps
- Framing and synchronization at 8 kbps (T1), or 64 kbps (E1)
- Total speed 1.544 Mbps (T1), or 2.048 Mbps (E1)

Because an ISDN BRI comprises two B channels and one D channel, it is often referred to as “2B+D.” Likewise, a U.S. T1 PRI is commonly referred to as “23B+D,” and a European E1 PRI as “30B+D.”

In Europe the D channel is carried in timeslot 16. In the United States it is in timeslot 24.

Note In an E1 PRI there are actually 32 channels: 30 B, 1 D, and 1 synchronization channel.

The table below displays the relationships between the DS level, speed, “T” designations, and number of channels.

North American Digital Hierarchy

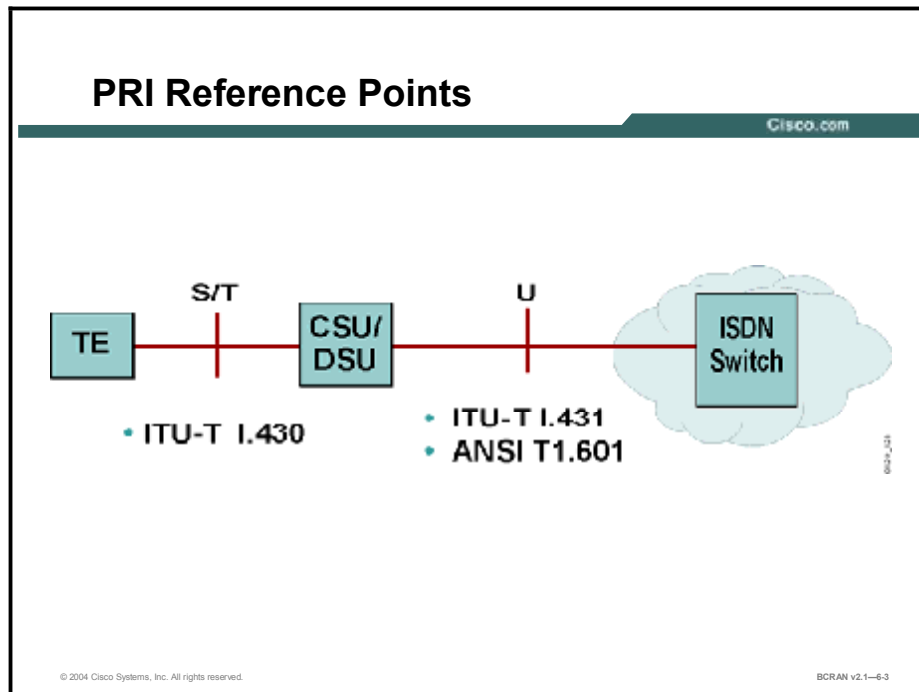
Digital Signal Level	Speed	“T” Designation	Channels or DS-0s
DS-0	64 kbps	–	1
DS-1	1.544 Mbps	T1	24
DS-3	44.736 Mbps	T3	672

In some cases, a DS-0 can carry only 56 kbps, usually because of legacy telco equipment or a signaling method called robbed-bit signaling (RBS).

In Europe, the equivalent of a T1 facility is an E1 facility.

PRI Reference Points

This topic describes the most common components and reference points of ISDN PRI.



Depending on country implementation, either the ANSI T1.601 or ITU-T I.431 standard governs the physical layer of the PRI interface.

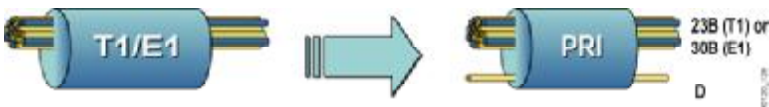
PRI technology is simpler than BRI. The wiring is not multipoint because there is only the straight connection between the CSU/DSU and the PRI interface. (Multipoint refers to the ability to have multiple ISDN devices connected to the network, all of which have access to the ISDN network.) Arbitration at Layer 1 and Layer 2 allows multiple devices that need to share the ISDN network to access the network without collisions or interruptions. PRI does not require this arbitration because there are no multiple devices.

Configuration Tasks for PRI

This topic describes the configuration tasks that are required to successfully configure an ISDN PRI connection.

Configuration Tasks for PRI

Cisco.com



- **Select the PRI switch type**
- **Specify T1/E1 controller, framing, and line coding for the facility**
- **Set PRI group timeslots for T1/E1 and indicate the speed used**
- **Specify the interface on the router that you will configure for DDR**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.4

Use the PRI configuration task steps listed in the figure, in addition to the DDR-derived commands covered earlier in BRI configurations, to enable a PRI connection.

Complete the following configuration tasks:

1. Specify the ISDN switch type used by the service provider for this PRI connection.
2. Specify the T1/E1 controller, framing type, and line coding for the service provider facility.
3. Set a PRI group timeslot for the T1/E1 facility and indicate the speed used.
4. Identify the interface used to configure DDR for the PRI.

ISDN PRI Configuration

This topic describes the **isdn switch-type** command. Configuring ISDN PRI requires global and interface configuration commands. Selecting the correct switch type to connect is critical when configuring ISDN PRI.

ISDN PRI Configuration

Cisco.com


```
Router(config)#isdn switch-type switch-type
```

- Configures the ISDN PRI switch type


```
Router(config)#controller {t1 | e1}
                        {slot/port | unit-number}
```

- Configures the ISDN PRI controller

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6-5

Use the **isdn switch-type** command to specify the CO PRI switch to which the router connects. With Cisco IOS Release 11.3(3)T or later, this command is also available as a controller command to allow different switch types to be supported on different controllers. If configured as a global command, the specified switch type applies to all controllers, unless a switch type is specifically configured on an individual controller.

An incompatible switch selection configuration can result in failure to make ISDN calls. After changing the switch type, you must reload the router to make the new configuration effective.

Telco **isdn switch-type** commands are shown in the table below.

isdn switch-type Command

Command	Description
primary-4ess	AT&T Primary-4ESS switches (United States)
primary-5ess	AT&T Primary -5ESS switches (United States)
primary-dms100	NT DMS-100 switches (North America)
primary-ni	National ISDN switch type
primary-ntt	NTT ISDN PRI switches (Japan)
primary-net5	European and Australian ISDN PRI switches
primary-qsig	Q Signaling (QSIG) per Q.931
None	No switch defined

Unlike BRI operation, ISDN PRIs do not use SPIDs. Therefore, there is no requirement to configure SPIDs, regardless of the ISDN switch type used by the PRI.

Use the **controller {t1 | e1} slot/port** command in global configuration mode to identify the controller to be configured. Use a single *unit-number* to identify the AS5000 Series controller. These commands are shown in the table below.

controller {t1 | e1} Command

Command	Description
t1	Specifies the controller interface for North America and Japan
e1	Specifies the controller interface for Europe and most other countries
<i>slot/port or unit number</i>	Specifies the physical slot/port location or unit number of the controller

T1 and E1 Controller Parameters

This topic describes the commands that are required to configure an ISDN T1 or E1 controller. In ISDN PRI, a T1 or E1 controller must first be configured to communicate with the service provider.

T1 and E1 Controller Parameters

Cisco.com

```
Router (config-controller)#framing
{sf | esf | crc4 | no-crc4}
```

- Selects the framing type on the controller

```
Router (config-controller)#linecode
(ami | b8zs | hdb3)
```

- Selects the line-code type on the controller

```
Router (config-controller)#clock source
[line [primary | secondary] | internal]
```

- Specifies the T1 clock source

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-66

Use the **framing** controller configuration command to select the frame type used by the PRI service provider. The table shows framing commands that you can use.

framing Command

Command	Description
sf	Super Frame. Use for some older T1 configurations.
esf	Extended Super Frame. Use for T1 PRI configurations.
crc4 or no-crc4	Cyclic redundancy check 4. Use for E1 PRI configurations.

Without a sufficient number of ones in the digital bit stream, the switches and multiplexers in a WAN can lose their synchronization for transmitting signals. Use the **linecode** command to identify the physical layer signaling method to satisfy the “ones” density requirement on the digital facility of the provider.

The table shows line code commands that you can use.

linecode Command

Command	Description
ami	Alternate mark inversion. Use for T1 configurations.
b8zs	Binary 8-zero substitution. Use for T1 PRI configurations.
hdb3	High density binary 3. Use for E1 PRI configurations.

Binary 8-zero substitution (B8ZS) accommodates the ones density requirements for T1 carrier facilities using special binary signals that are encoded over the digital transmission link. It allows 64 kbps (clear channel) for ISDN channels.

Settings for these two Cisco IOS software controller commands on the router must match the framing and line-code types used at the T1/E1 WAN CO switch of the provider.

Use the **clock source {line | internal}** command to configure the T1 and E1 clock source on Cisco routers. T1 configurations typically require **framing esf** and **linecode b8zs**. E1 configurations typically require **framing crc4** and **linecode hdb3**.

Additional ISDN PRI Configuration Parameters

This topic describes the commands that are required to configure the ISDN PRI channels and D channel. After the T1 or E1 controller is configured, the PRI channels and the corresponding D channel interface must be configured.

Additional ISDN PRI Configuration Parameters

Cisco.com

`Router(config-controller)#pri-group [timeslots range]`

- Specifies ISDN PRI on the T1 or E1 controller
- Specifies timeslots (channels) used by PRI

`Router(config)#interface serial {slot/port | unit:}{23 | 15}`

- Specifies the serial interface for the PRI D channel

`Router(config-if)#isdn incoming-voice modem`

- Switches incoming analog calls to internal modems

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.7

The **pri-group** command configures the specified interface for PRI operation and specifies which fixed timeslots (channels) are allocated on the digital facility of the provider.

pri-group Command

Command	Description
<code>timeslots range</code>	The range of timeslots allocated to this PRI. For T1, use values in the range of 1 to 24, and for E1, use values from 1 to 31. The speed of the PRI is the aggregate of the channels assigned.

Example 1: If using all 30 B channels on an E1 PRI (30B+D), specify **pri-group 1-31**.

Example 2: If allocated only the first eight B channels (512-kbps total data bandwidth) for a T1 PRI (23B+D), then specify **pri-group 1-8,24**. Note that the D channel must be specified.

Note When provisioning a PRI line with less than 24 time slots (or 30 for E1), include the D channel for signaling.

Specification of the PRI group automatically creates the corresponding serial interface for the D channel: **interface serial** *{slot/port | unit}*:**{23 | 15}**. This interface is used to configure the PRI D channel. The table shows the interface serial commands that you can use.

interface serial Command

Command	Description
<i>slot/port</i>	The slot/port of the channelized controller
<i>unit</i>	The unit number of the channelized controller on a Cisco 4000 or AS5000 Series router
23	A T1 interface that designates channelized DS-0s 0 to 22 as the B channels, and DS-0 23 as the D channel
15	An E1 interface that designates 30 B channels and timeslot 16 as the D channel

Note In an E1 or T1 facility, the channels start numbering at 1 (1 to 31 for E1 and 1 to 24 for T1). Serial interfaces in the Cisco router start numbering at 0. Therefore, channel 16, the E1 signaling channel, is serial port subinterface 15. Channel 24, the T1 signaling channel, is serial subinterface 23.


The **isdn incoming-voice modem** command allows incoming analog calls to be switched to internal modems. Software examines the bearer capability fields of the D channel data and determines whether a call is a normal ISDN call or an analog call being carried on an ISDN B channel. If it is an analog call, it is switched to internal modems. This command is only available for access servers with the capability for internal modems.

PRI Configuration Example

The following topic highlights a sample ISDN PRI configuration.

PRI Configuration Example

Cisco.com



```
isdn switch-type primary-5ess
!
controller t1 0/0
 pri-group timeslots 1-24
 framing esf
 linecode b8zs
 clock source line
!
interface serial 0/0:23
 ip address 192.168.11.2 255.255.255.0
 isdn incoming-voice modem
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-8

The table describes the commands in the figure.

PRI Configuration Commands

Command	Description
isdn switch-type primary-5ess	Selects a switch type of AT&T 5ESS
controller t1 0/0	Selects the T1 controller 0/0
pri-group timeslots 1-24	Establishes the interface port to function as PRI with 24 timeslots (including D channel) designated to operate at a speed of 64 kbps
framing esf	Selects Extended Superframe (ESF) framing, a T1 configuration feature
linecode b8zs	Selects line code B8ZS for T1
clock source line	Specifies the T1 line as the clock source for the router
interface serial 0/0:23	Identifies the D channel on serial interface 0/0

Note Static mapping and DDR commands are also used for configuring PRI. Although they are also required for ISDN operation, these commands are omitted from this example.

The **controller t1 0/0** command configures the T1 controller. In the example, the switch type selected is an AT&T model. This example is accurate for some operations in the United States.

For an E1 example, the timeslot argument for the **pri-group** command would be **1-31** rather than **1-24** as shown for a T1 example, and the interface command would be **0/0:15** instead of **0/0:23**.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- ISDN PRI is typically used to aggregate multiple BRIs or for higher-bandwidth requirements.
- ISDN PRI (T1) total speed is 64 kbps x 23 (B channels) + 64 kbps (D channel) + 8 kbps (framing and synchronization) = 1.544 Mbps.
- ISDN PRI (E1) total speed is 64 kbps x 30 (B channels) + 64 kbps (D channel) + 64 kbps (framing and synchronization) = 2.048 Mbps.
- ISDN PRI requires that a T1 (or E1) controller be configured.
- A T1 controller configuration must include the framing type and line coding.

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-9

Summary (Cont.)

Cisco.com

- Like ISDN BRI, a PRI switch type must also be configured.
- ISDN PRI does not require SPIDs.
- The ISDN PRI D and B channels are configured separately from the controller, using the interface serial command.
- The pri-group command configures the specified interface for PRI operation and the number of fixed timeslots that are allocated on the provider digital facility.

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-10

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) When you are configuring PRI on a Cisco router, where does the information for the correct PRI switch type, T1 or E1 controller, framing type, and line coding come from?
- A) service provider facility
 - B) client facility
 - C) company human resources department
 - D) local electronic retail store
- Q2) Which Cisco router command is used to specify the CO PRI switch to which the router connects?
- A) **isdn switch-type**
 - B) **isdn router-type**
 - C) **isdn hub-type**
 - D) **switch isdn-type**
- Q3) Which framing controller configuration command code parameter is used to select the frame type used by the PRI service provider for Extended Super Frame?
- A) **sf**
 - B) **esf**
 - C) **crc4**
 - D) **esc4**
- Q4) Which Cisco router command configures the specified interface for PRI operation and specifies the number of fixed timeslots that are allocated on the digital facility of the provider?
- A) **BRI group**
 - B) **SER group**
 - C) **PRI group**
 - D) **Eth group**
- Q5) Which command would be used to configure a European ISDN PRI switch type?
- A) **isdn switch-type primary-4ess**
 - B) **isdn switch-type primary-net5**
 - C) **isdn switch-type primary-5ess**
 - D) **isdn switch-type primary-dms100**

Quiz Answer Key

Q1) A

Relates to: Configuration Tasks for PRI

Q2) A

Relates to: ISDN PRI Configuration

Q3) B

Relates to: T1 and E1 Controller Parameters

Q4) C

Relates to: Additional ISDN PRI Configuration Parameters

Q5) B

Relates to: PRI Configuration Example

Configuring DDR

Overview

DDR enables routers to connect on an as-needed basis. They typically connect long enough to exchange information and then disconnect. This results in significant cost savings for the enterprise.

Relevance

ISDN connects and disconnects faster than plain old telephone service (POTS), and has greater throughput. For these reasons, DDR is most often used with ISDN. This lesson provides an overview of ISDN DDR.

Objectives

Upon completing this lesson, you will be able to:

- Explain the logic flow when defining interesting traffic
- List the steps that are required to configure DDR
- Define and configure interesting traffic on selected interfaces
- Configure access lists to provide more granular control when defining interesting traffic
- Apply dialer lists to ISDN BRI interfaces
- Configure dialer maps to specify how to reach a remote destination
- Configure a simple ISDN network
- Define interesting traffic with dialer and access lists

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

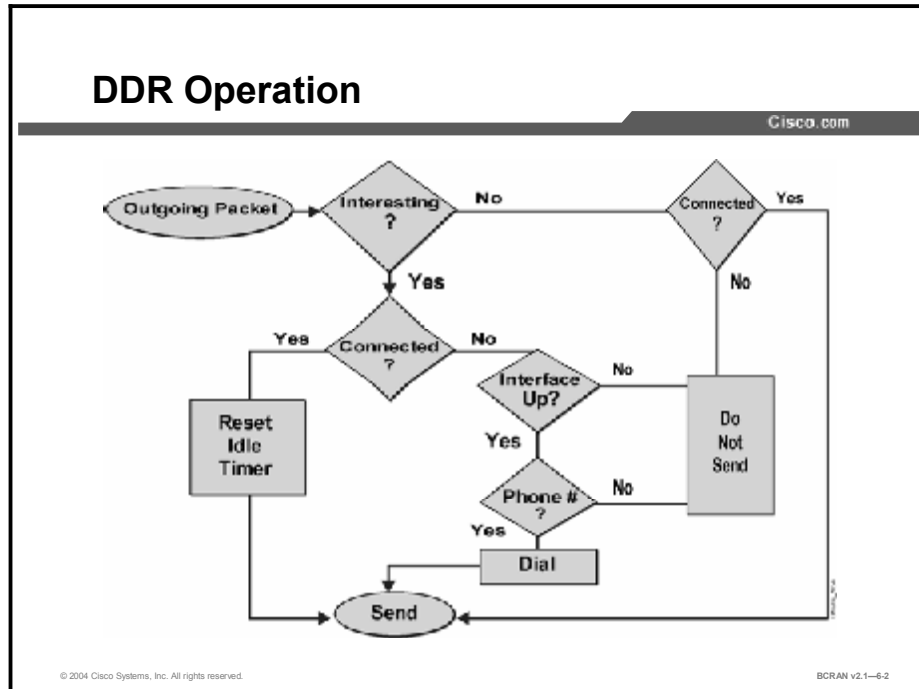
Outline

This lesson includes these topics:

- Overview
- DDR Operation
- DDR and ISDN Usage
- DDR Configuration Tasks
- Interesting Traffic for DDR
- Access Lists for DDR
- Destination Parameters for DDR
- Configuration of a Simple ISDN Call
- Configuration Example: RouterA
- Configuration Example: RouterB
- Access List for DDR Example
- Summary
- Quiz

DDR Operation

This topic describes the ISDN DDR process and explains the logic flow when defining interesting traffic. DDR routing enables predefined interesting traffic to initiate a call across the ISDN WAN connection.



Cisco implements DDR from the perspective of the outgoing data from the router.

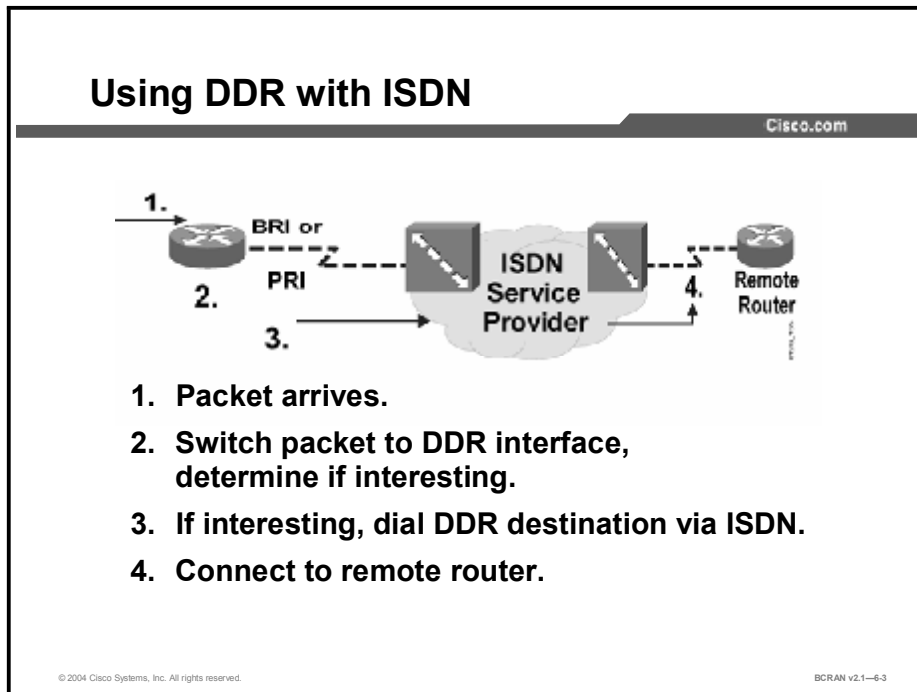
With DDR, all traffic that is destined to the dialer interface is classified as either “interesting” or “uninteresting,” based on the dialer list. If the traffic is interesting (permitted by the dialer list), then the router connects to the remote router if not currently connected. If the traffic is uninteresting (denied by the dialer list) and there is no connection, then it does not dial the remote router, thereby saving costs.

The dialer idle timer is used to reset the connection if no interesting traffic for the destination arrives within the configured timer interval.

Note When a connection is made, all traffic uses the link (unless denied by another access list applied to the interface). For example, if the dialer list is configured to allow only ping (Internet Control Message Protocol [ICMP]) traffic, a user could send a ping to bring up the connection and then start a Telnet session on the open DDR interface.

DDR and ISDN Usage

This topic describes the sequence of events that triggers an ISDN DDR call. ISDN is commonly configured with DDR



Access routers use DDR to connect to remote routers. The access router will initiate a connection only when it detects “interesting traffic” that is bound for a remote site. Dialer lists specify interesting traffic. You can place a BRI interface in a dial group, which is linked to a dialer list that specifies interesting traffic. You can use multiple dialer list entries to identify traffic that is interesting and destined for other DDR destination routers, based on various protocols. Access lists can also be used to refine the designation of interesting packets that will initiate DDR calls.

Routing updates may cause ISDN calls to remote routers. This could dramatically increase service charges from the ISDN service provider. For this reason, it is usually best to use static and default routes to reach destination networks.

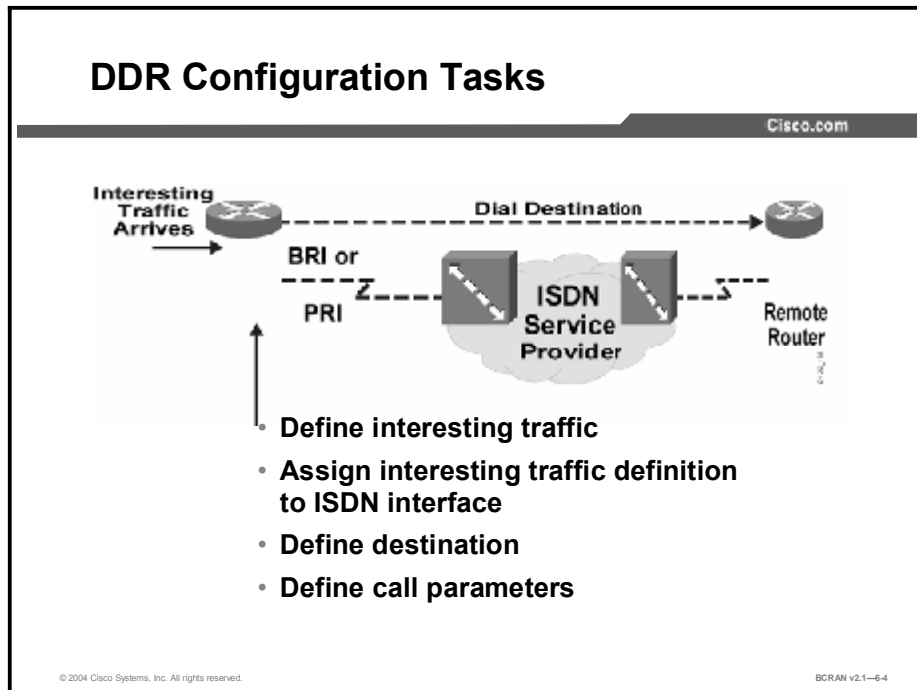
Note Some dynamic routing protocols, like Open Shortest Path First (OSPF), support features specifically designed to work over DDR connections. In addition, Cisco IOS software supports a feature called Snapshot Routing. This feature permits the use of distance-vector routing protocols over DDR links while minimizing routing and service advertisement updates, thus saving link charges. Further information on these features can be located at <http://www.cisco.com>.

DDR commands map a host ID and dialer string to initiate the setup of an ISDN call for interesting traffic. The router then makes an outgoing call from its BRI interface through the ISDN NT-1. If using an external TA, it must support V.25bis dialing. Calling details for these devices come from **dialer** commands.

An idle timer starts when no more interesting traffic is transmitted over the ISDN call. The timer is reset if an interesting packet is received before the Idle-Timeout value is reached. If no interesting packets are received when the Idle-Timeout expires, the call disconnects.

DDR Configuration Tasks

This topic describes the tasks that are required to configure DDR. Several tasks are required to configure ISDN with DDR.



To configure DDR, you must complete these tasks:

1. Define what constitutes interesting traffic by using the **dialer-list** command.
2. Assign this interesting traffic definition to an interface using the **dialer-group** command.
3. Define the destination IP address, host name, telephone number to dial, and optional call parameters using the **dialer map** command.
4. Define call parameters using the following commands:
 - **dialer idle-timeout** *seconds*: Specifies the time that the line can remain idle without receiving interesting traffic before it is disconnected. Default time is 120 seconds.
 - **dialer fast-idle** *seconds*: Specifies the time that a line for which there is contention (another call is waiting to use line) can remain idle before the current call is disconnected, to allow the competing call to be placed. Default time is 20 seconds.
 - **dialer load-threshold** *load* [**outbound** | **inbound** | **either**]: Specifies the interface load at which time the dialer initiates another call to the destination. This command is used with Bandwidth on Demand (BoD) or Multilink PPP (MLP).

Definitions of the arguments and options for the **dialer load-threshold** *load* [**outbound** | **inbound** | **either**] command are displayed in the table.

dialer load-threshold Command

Command	Description
<i>load</i>	A number from 1 to 255, with 255 equal to 100 percent load and 128 equal to 50 percent load
outbound	Calculates the load on outbound data only (the default)
inbound	Calculates the load on inbound data only
either	Calculates the load on the maximum of the outbound or inbound data

Note For more information, refer to the "Cisco Access Dial Configuration Cookbook" at <http://www.cisco.com/>

Interesting Traffic for DDR

This topic describes how to configure interesting traffic and apply it to an ISDN interface. With ISDN DDR, an interface is activated when it sees interesting traffic that it must forward.

Defining Interesting Traffic

Cisco.com

```
Router(config)#dialer-list dialer-group-number
protocol protocol-name {permit | deny |list
access-list-number}
```

- Defines interesting packets for DDR
- Associated with the dialer group assigned to the interface

```
Router(config-if)#dialer-group group-number
```

- Assigns an interface to the dialer access group specified in the dialer-list command

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.5

The **dialer-list** command is used to configure dial-on-demand calls that will initiate a connection. The simple form of the command specifies whether a whole protocol suite, such as IP or Internetwork Packet Exchange (IPX), will be permitted or denied to trigger a call. The more complex form references an access list that allows finer control of the interesting traffic definition for a given protocol. A dialer list can contain multiple entries to define multiple protocol types as interesting.

The **dialer-group** interface command applies the dialer list specifications to an interface. Only one dialer list can be applied to an interface at a time.

The **dialer-list** and **dialer-group** command syntax is described in the table.

dialer-list and dialer-group Commands

Command	Description
dialer-list <i>dialer-group-number</i> protocol <i>protocol-name</i> { permit deny list <i>access-list-number</i> <i>access-group</i> }	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and access list.
<i>dialer-group-number</i>	Number of a dialer access group identified in any dialer-group interface configuration command.
<i>protocol-name</i>	One of the following protocol keywords: appletalk , bridge , clns , clns_es , clns_is , decnet , decnet_router-L1 , decnet_router-L2 , decnet_node , ip , ipx , vines , or xns .
dialer-group <i>group-number</i>	Configures an interface to belong to a specific dialer group. The dialer group points to a dialer list.
<i>group-number</i>	Number of the dialer access group to which the specific interface belongs. This access group is defined with the dialer-list command, which specifies interesting traffic that initiates a DDR call. Acceptable values are nonzero, positive integers from 1 to 10.

Access Lists for DDR

This topic describes how to define ISDN DDR interesting traffic by referencing an access list. Interesting traffic can be specifically defined with an access list.

Using Access Lists for DDR

Cisco.com

```
Router(config)#access-list access-list-number {permit|deny}
  {protocol | protocol-keyword }
  {source source-wildcard | any}
  {destination destination-wildcard | any}
  [protocol-specific-options] [log]
```

- Gives tighter control over “interesting” traffic and uses standard or extended access lists

```
Router(config)#dialer-list dialer-group protocol protocol-name list access-list-number
```

- Associates an access list with a dialer access group

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.6

When linked to a dialer list, access lists give strict control over which packets are considered interesting. The **access-list** command specifies the interesting traffic that initiates a DDR call. Both standard and extended access lists are supported, which enables the identification of interesting traffic based on simple destination addresses, or based on both source and destination addresses, and upper layer protocols.

An extended access list is displayed in the figure shown, providing more control over the protocol, source address, and destination address in determining interesting packets.

Note Not all command parameters are displayed for the **access-list** command. Refer to the Cisco Documentation CD-ROM or <http://www.cisco.com> for the complete syntax.

The **dialer-list** command is used in conjunction with the access list. This command associates the access list with the dialer access group.

The following is a sample configuration:

```
interface BRI0
dialer-group 1

access-list 101 deny igmp 0.0.0.0 any any
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
```

Destination Parameters for DDR

This topic describes how to identify a remote destination with the **dialer map** command. When interesting traffic has been detected, the interface is activated and initiates a call to the remote ISDN destination, which is identified by a dialer map.

Defining Destination Parameters

Cisco.com

```
Router(config-if)# dialer map protocol next-hop-address  
[name hostname] [speed 56|64] [broadcast]  
[modem-script modem-regexp]  
[system-script system-regexp]  
[dial-string[:isdn-subaddress]]
```

- Maps an IP network layer address to a remote phone number
- Defines the method of reaching a remote ISDN destination

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-67

When interesting traffic has been identified for the ISDN interface, the router initiates a DDR call, if the call is not already connected. The router uses the information that is configured in the **dialer map** command to determine dialing parameters to the destination router, such as the telephone number to dial. The **dialer map** command binds the next-hop protocol address to a telephone number, or *dial-string*, for a particular destination.

A dialer map is similar in concept to an Address Resolution Protocol (ARP) entry for a LAN that binds an IP address to a MAC address, or a Frame Relay map that binds a next-hop protocol address to a data-link connection identifier (DLCI). Each dialer map associates a destination or next-hop Layer 3 network address to a destination Layer 2 address.

The **dialer map** command options are described in the table.

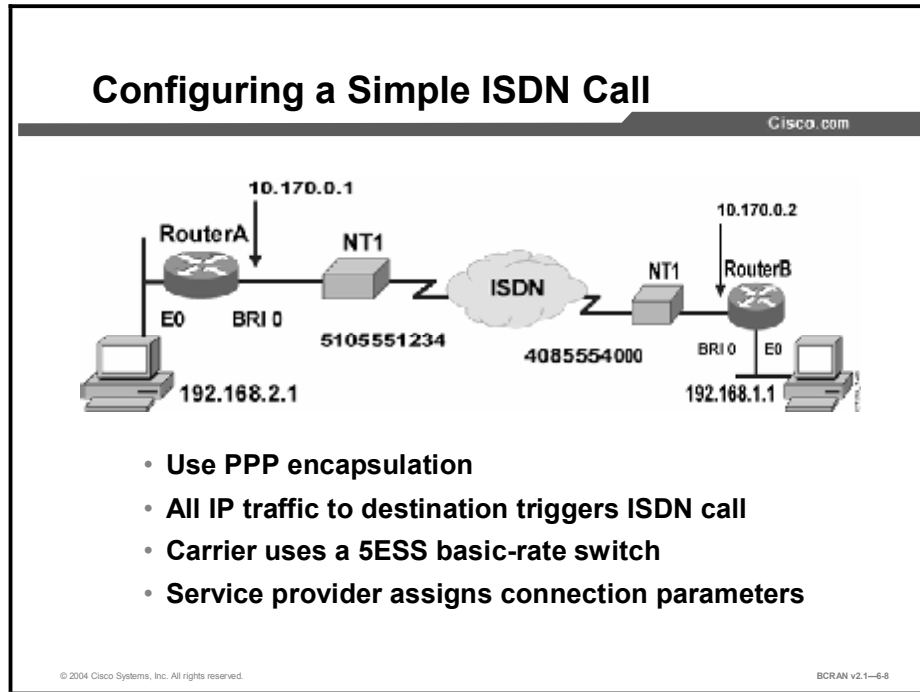
dialer map Commands

Command	Description
dialer map <i>protocol next-hop-address</i> [name <i>hostname</i>] [speed 56 64] [broadcast] [<i>dial-string</i> [: <i>isdn-subaddress</i>]]	Configures a serial interface or ISDN interface to call one or multiple sites. <ul style="list-style-type: none">■ name parameter refers to the name of the remote system■ speed parameter is the line speed to use in kilobits per second■ broadcast parameter indicates that broadcasts should be forwarded to this address■ <i>dial-string</i>[:<i>isdn-subaddress</i>] is the number to dial to reach the destination and the optional ISDN subaddress
[modem-script <i>modem-regexp</i>]	(Optional) Indicates the modem script to use for the connection (for asynchronous interfaces). Create <i>modem-regexp</i> using a chat script.
[system-script <i>system-regexp</i>]	(Optional) Indicates the system script to use for the connection (for asynchronous interfaces). Create <i>system-regexp</i> using a chat script.

Note The **dialer map** command has many other optional parameters available. For a complete description of the command and its parameters, refer to the documentation CD-ROM or <http://www.cisco.com>.

Configuration of a Simple ISDN Call

This topic describes a simple ISDN BRI connection with DDR-enabled configuration.



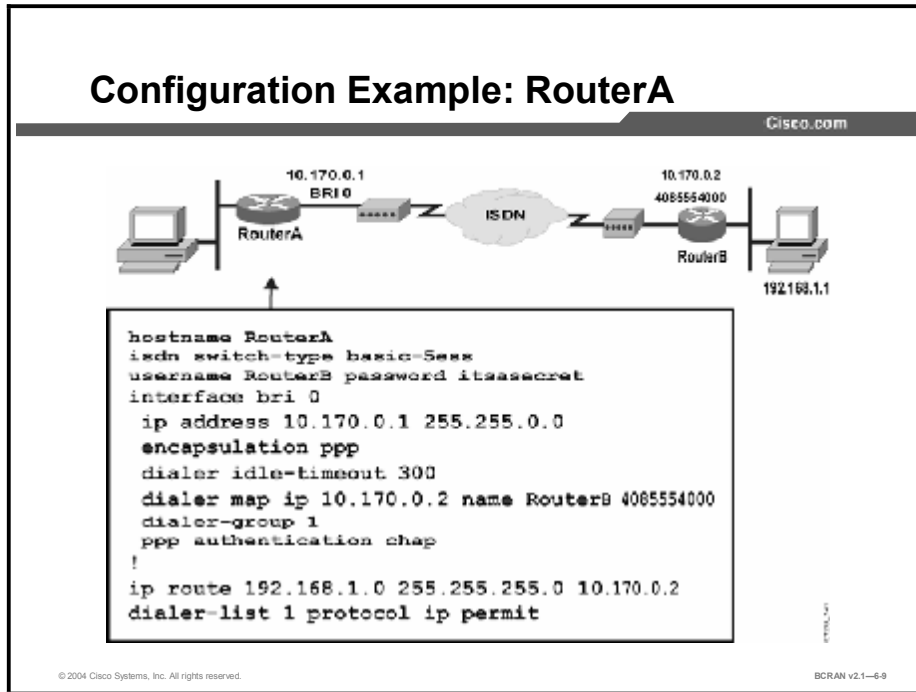
The figure displays an example of how you can combine the commands described in the previous lessons to set up ISDN and initiate DDR.

DDR is configured to connect RouterA to RouterB. Interesting traffic is defined as any IP traffic that will initiate a DDR call to RouterB. Similar to a telephone call, the number dialed is for the remote ISDN device. The ISDN service provider supplies this number.

As shown in the figure, traffic is routed to the LAN. Before a connection can be made, you must configure Challenge Handshake Authentication Protocol (CHAP) authentication, a dialer map, and static routes of how to reach the RouterB 192.68.1.0 network.

Configuration Example: RouterA

This topic describes a sample ISDN BRI and DDR configuration for RouterA.



The configuration in the figure is for legacy DDR, which uses dialer maps.

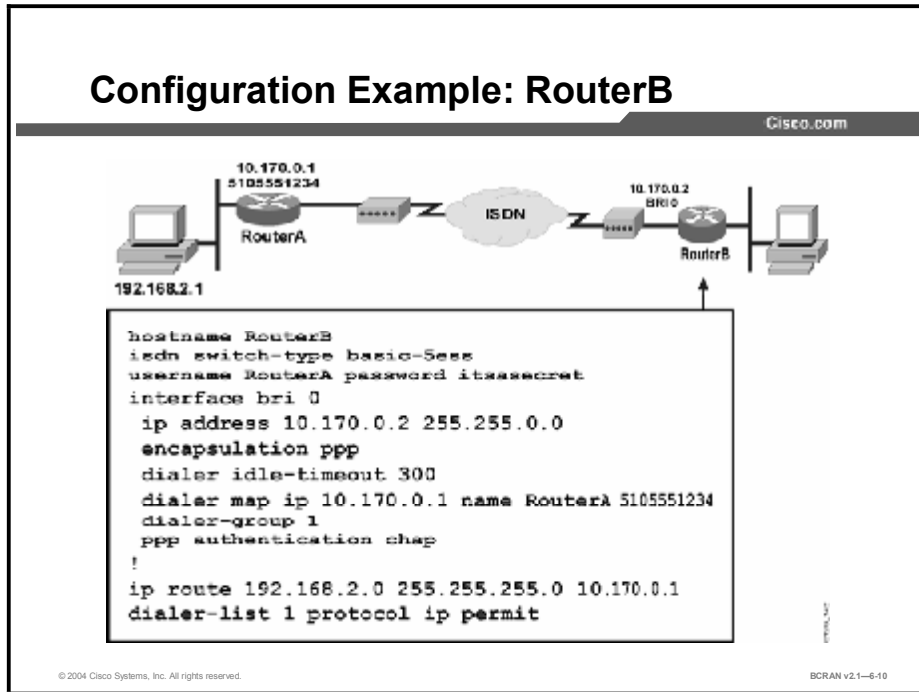
The table describes the commands that are used in the configuration.

BRI and DDR RouterA Configuration Commands

Command	Description
isdn switch-type	Selects the AT&T 5ESS switch as the central office (CO) ISDN switch type for this interface.
username rtb password itsasecret	Sets up a CHAP username and password for the remote router.
interface bri 0	Enters BRI 0 configuration mode.
ip address 10.170.0.1 255.255.0.0	Specifies the BRI 0 IP address and subnet mask.
encapsulation ppp	Sets up PPP encapsulation for BRI 0.
dialer idle-timeout 300	Specifies the number of seconds of idle time before the router drops the ISDN call (300 sec = 5 min).
dialer map	Establishes how to call the next-hop router.
ip	Specifies the name of the protocol that is used by this map.
10.170.0.2	Specifies the IP address for the next-hop router BRI interface.
RouterB	Specifies the CHAP identification name for the remote router.
4085554000	Specifies the telephone number that is used to reach the BRI interface on the remote router for this DDR destination.
dialer-group 1	Associates the BRI 0 interface with dialer list 1.
ppp authentication chap	Sets up CHAP PPP authentication for BRI 0.
ip route....	Configures a static route to the subnet on the remote router.
dialer-list 1 protocol ip permit	Associates permitted IP traffic with dialer group 1. The router will start an ISDN call for IP traffic only.

Configuration Example: RouterB

This topic describes a sample ISDN BRI and DDR configuration for RouterB.



This figure displays the configuration of RouterB. This configuration is also for legacy DDR.

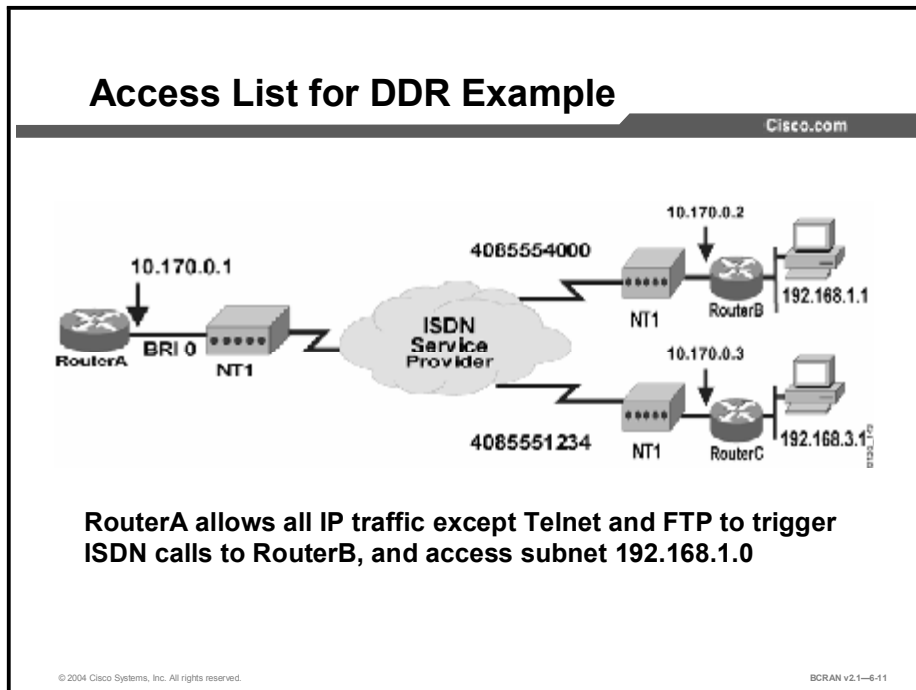
The table describes the commands that are used in the configuration.

BRI and DDR RouterB Configuration Commands

Command	Description
isdn switch-type	Selects the ISDN switch type for this interface.
username rta password itsasecret	Sets up the CHAP username and password for the remote router.
interface bri0	Enters BRI 0 configuration mode.
ip address 10.170.0.2 255.255.0.0	Specifies the BRI 0 IP address and net mask.
encapsulation ppp	Sets up PPP encapsulation for BRI 0.
dialer idle-timeout 300	Specifies the number of seconds of idle time before the router drops the ISDN call (300 sec = 5 min).
dialer map	Establishes how to call the next-hop router.
ip	Specifies the name of the protocol that is used by this map.
10.170.0.1	Specifies the IP address for the next-hop router BRI interface.
RouterA	Specifies the CHAP identification name for the remote router.
5105551234	Specifies the telephone number that is used to reach the remote router for this DDR destination.
dialer-group 1	Associates the BRI 0 interface with dialer list 1.
ppp authentication chap	Sets up CHAP PPP authentication for BRI 0.
ip route....	Configures a static route to the subnet on the remote router.
dialer-list 1 protocol ip permit	Associates permitted IP traffic with dialer group 1. The router will start an ISDN call for IP traffic only.

Access List for DDR Example

This topic describes a simple ISDN BRI connection that uses a DDR configuration. Interesting traffic is more specifically defined with an access list.



This figure displays how to combine DDR commands with an extended access list to trigger an ISDN call. The configuration uses many of the same commands for configuring a simple ISDN call. Through dialer lists, access lists are applied to a dialer group to trigger call setup.

DDR is configured on RouterA to connect with RouterB for all IP traffic except Telnet and the FTP. The details about what is interesting to DDR are defined in an access list.

The service provider offering the ISDN service uses a Northern Telecom DMS-100 switch. Therefore, the configuration requires that the service profile identifiers (SPIDs) be specified. The service provider supplies other details to use when you are configuring the router for ISDN.

It is more common in networks to reference an access list in the dialer list because it offers more granular control over the protocols, users, and destinations that trigger a call. The previous example permitted any IP packet to trigger the call. It is likely that noncritical packets will activate the line unnecessarily, thereby resulting in an inflated line.

Access List for DDR Example: RouterA

Cisco.com



```

hostname RouterA
isdn switch-type basic-dms100
username RouterB password itsasecret
username RouterC password itsasecret
interface bri 0
 ip address 10.170.0.1 255.255.0.0
 encapsulation ppp
 dialer idle-timeout 300
 dialer map ip 10.170.0.2 name RouterB 4085554000
 dialer map ip 10.170.0.3 name RouterC 4085551234
 dialer-group 2
 ppp authentication chap
(continued on next figure)

```

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-12

This figure displays the configuration of RouterA from the previous figure. This configuration is for legacy DDR and uses dialer maps and extended access lists. The table describes the commands that are used in the configuration.

Access List Configuration Commands

Command	Description
isdn switch-type	Selects the ISDN switch type for this interface.
username RouterB password itsasecret	Sets up the CHAP username and password for the remote router in the local user database.
interface bri0	Enters BRI 0 configuration mode, and sets up DDR and ISDN functions.
ip address 10.170.0.1 255.255.0.0	Specifies the BRI 0 IP address and net mask.
encapsulation ppp	Sets up PPP encapsulation for BRI 0.
dialer idle-timeout 300	Specifies the number of seconds of idle time (300 sec = 5 min) before the router drops the ISDN call.
dialer map	Establishes the IP address and ISDN number to call the next-hop routers.
dialer-group 2	Associates the BRI 0 interface with dialer list 2.
ppp authentication chap	Sets up CHAP PPP authentication for BRI 0.

Access List for DDR Example: RouterA (Cont.)

Cisco.com



```
ip route 192.168.1.0 255.255.255.0 10.170.0.2
ip route 192.168.3.0 255.255.255.0 10.170.0.3
access-list 101 deny tcp any any eq ftp
access-list 101 deny tcp any any eq telnet
access-list 101 permit ip any any
dialer-list 2 protocol ip list 101
```

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-13

This figure shows the continuation of the configuration of RouterA. This simple example shows how access lists are linked to dialer lists and dialer groups to determine interesting traffic that triggers DDR calls. Either simple or extended access lists can be linked with dialer lists and dialer groups to identify interesting traffic, thus creating a powerful set of tools to control dialup costs.

The table describes the commands that are used in the configuration.

Access List Configuration Example Commands

Command	Description
ip route ...	Configures static routes to subnets on remote router Ethernet interfaces.
access-list 101 deny ...	Defines extended TCP access list entries to prevent FTP and Telnet packets from triggering calls.
access-list 101 permit ...	Defines entry in the extended access list to permit remaining IP traffic to trigger ISDN calls.
dialer-list 2 protocol ip list 101	Sets up control for automatic DDR dialing. Assigns access list 101 to dialer list 2, which is assigned to the BRI 0 interface by the dialer-group command statement. Only IP will trigger DDR calls with this configuration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **ISDN DDR enables routers to connect on an as-needed basis and therefore can result in significant cost savings.**
- **The global configuration dialer-list command is used to define interesting traffic.**
- **Access lists can also be used with dialer lists to provide more granular control.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-14

Summary (Cont.)

Cisco.com

- **The interface configuration dialer-group command is used to apply a dialer list to an ISDN BRI interface.**
- **The interface configuration dialer map command is used to specify how to connect to a remote site.**
- **Call parameters which can be specified include dialer idle-timeout, dialer fast-idle, and dialer load-threshold.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What type of traffic is passed on to the router in DDR?
- A) uninteresting traffic
 - B) uninvited traffic
 - C) invited traffic
 - D) interesting traffic
- Q2) A DDR-configured Cisco access router initiates a connection to a remote router _____?
- A) as soon as the connection is broken
 - B) when it detects “interesting traffic” bound for a remote site
 - C) when the network administrator issues a **no shutdown** command on the Ethernet interface
 - D) when the network administrator issues a **shutdown** command on the Ethernet interface
- Q3) Which Cisco router command defines what constitutes interesting traffic?
- A) **dialer-group**
 - B) **dialer-map**
 - C) **dialer-list**
 - D) **dialer-interesting**
- Q4) Which Cisco router command applies the dialer list specifications to an interface?
- A) **dialer-group**
 - B) **dialer-map**
 - C) **dialer-list**
 - D) **dialer-interesting**
- Q5) Which Cisco router command specifies source, destination, and protocols that define interesting traffic that will initiate a DDR call?
- A) **dialer-group**
 - B) **dialer-map**
 - C) **dialer-list**
 - D) **access-list**

- Q6) Which Cisco router command identifies destination router information, such as the telephone number to dial?
- A) **dialer-group**
 - B) **dialer-map**
 - C) **dialer-list**
 - D) **dialer-access-list**
- Q7) Which Cisco router command feature associates permitted IP traffic with dialer group 1?
- A) **dialer-group 1**
 - B) **dialer map**
 - C) **dialer-list 1 protocol ip permit**
 - D) **dialer idle-timeout 1**
- Q8) Which Cisco router command configures static routes to subnets on remote router Ethernet interfaces?
- A) **access-list 101 permit**
 - B) **access-list 101 deny**
 - C) **ip route**
 - D) **dialer list 2 protocol ip list 101**

Quiz Answer Key

- Q1) A
Relates to: DDR Operation
- Q2) B
Relates to: DDR and ISDN Usage
- Q3) C
Relates to: DDR Configuration Tasks
- Q4) A
Relates to: Interesting Traffic for DDR
- Q5) D
Relates to: Access Lists for DDR
- Q6) B
Relates to: Destination Parameters for DDR
- Q7) C
Relates to: Configuration Example: RouterB
- Q8) C
Relates to: Access List for DDR Example

Verifying ISDN and DDR Configurations

Overview

ISDN still serves as a viable technology in many parts of the world. It is commonly used in a WAN environment as a backup technology for Frame Relay. ISDN is also used for small office, home office (SOHO) connectivity in areas where a digital subscriber line (DSL) or cable modem technology is not available. This lesson provides an overview of various commands to verify ISDN and dial-on-demand routing (DDR) connectivity.

Relevance

Implementing and troubleshooting ISDN is a necessary skill for network engineers.

Objectives

Upon completing this lesson, you will be able to:

- Monitor ISDN connections
- Verify and troubleshoot ISDN environments using **debug** commands
- Monitor the ISDN BRI D channel
- Monitor the ISDN BRI B channels
- Monitor PPP on an ISDN BRI connection
- Test an ISDN and DDR connection

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

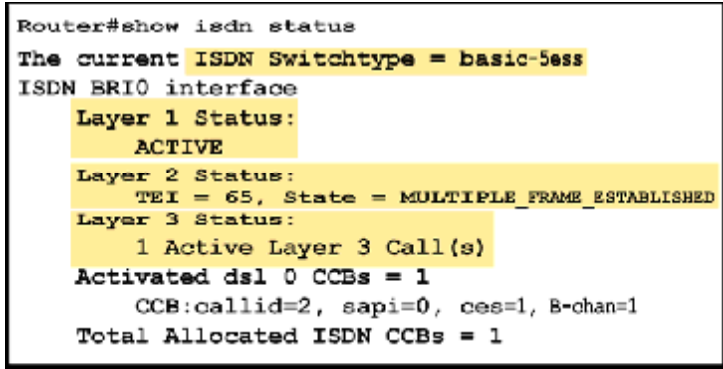
Outline

This lesson includes these topics:

- Overview
- ISDN BRI Monitoring
- ISDN Layer 2 **debug** Commands
- ISDN Layer 3 **debug** Commands
- ISDN BRI D Channel Monitoring
- ISDN BRI B Channel Monitoring
- PPP on BRI Monitoring
- DDR Configuration Test
- Summary
- Quiz

ISDN BRI Monitoring

This topic describes the **show isdn status** command, which is useful when monitoring and troubleshooting Layer 1 and Layer 2 of an ISDN BRI configuration. Various commands are required to monitor and troubleshoot ISDN BRI and DDR connections.



```
Router#show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 65, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
1 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 1
CCB:callid=2, sapi=0, ces=1, B-chan=1
Total Allocated ISDN CCBs = 1
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-2

Use the **show isdn status** command to display a status summary of each of the three ISDN layers. The command is very useful to determine if Layer 1 and Layer 2 are active and are properly communicating with the telco ISDN switch. After this has been verified, you can proceed on to higher-level troubleshooting issues such as dialer interfaces, interesting traffic definitions, PPP negotiation, and authentication failures.

The output displayed in the figure is an example of a properly functioning BRI circuit. In this example, the correct switch type has been configured and Layer 1 is ACTIVE. The command also reports that Layer 2 has been successfully negotiated because it is displaying the TEI and the MULTIPLE_FRAME_ESTABLISHED state. Finally, the output reports that the ISDN Layer 3 (end-to-end) is ready to make or receive calls.

The following tables show status messages for the Layer 1 and 2 states, as well as troubleshooting tips.

Layer 1 Status Messages

Status	Description
ACTIVE	There is physical connectivity with the telco ISDN switch.
DEACTIVATED	There is no physical connectivity with the telco ISDN switch. Check the following: <ul style="list-style-type: none"> ■ BRI not shut down (no shutdown) - Is interface up/up? ■ Check cabling ■ External NT-1 required and not connected or operational? ■ Service from telco down
GOINGDOWN, INIT, TESTING, RESET, DELETED (sic), SHUTDOWN, ACTIVATING ACTIVE_ErrorInd	Most of the Layer 1 states are temporary. Use the clear interface bri number command to clear them. If those states persist for extended periods, contact the telco for further troubleshooting.

Layer 2 Status Messages

Status	Description
TEI = #	Valid TEI number range is 64 to 126.
MULTIPLE_FRAME_ESTABLISHED	Indicates there is data-link connectivity to the telco ISDN switch. This is the state that you should see under normal operations. Any other state usually indicates a problem on the circuit.
Layer 2 is NOT Activated	Layer 2 is down. Use the debug q.921 command to help troubleshoot.
TEI_ASSIGNED	Indicates that the router has lost connectivity to the switch. Check the following: <ul style="list-style-type: none"> ■ Verify configured switch-type setting ■ Verify SPID settings, if required ■ Verify with service provider the correct values
TEI_UNASSIGNED, ASSIGN_AWAITING_TEI, ESTABLISH_AWAITING_TEI, AWAITING_ESTABLISHMENT, AWAITING_RELEASE, TIMER_RECOVERY	Most of these Layer 2 states are temporary. Use the clear interface bri number command to reestablish connectivity. If those states persist for extended periods, use the debug isdn q921 command for further troubleshooting.

ISDN Layer 2 *debug* Commands

This topic describes the **debug isdn q921** command, which is useful when monitoring and troubleshooting Layer 2 of an ISDN BRI configuration.

ISDN Layer 2 debug Commands

Cisco.com

```
Router#debug isdn q921
```

- Shows data-link layer messages (Layer 2) on the D channel between the access router and the ISDN switch

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6-3

To monitor Layer 2 problems, use the **debug isdn q921 EXEC** command. The command displays real-time data-link layer (Layer 2) access procedures that are taking place at the access router on the D channel (LAPD) of its ISDN interface. This command is useful when you want to observe signaling events between the access router and the ISDN switch.

ISDN Layer 3 *debug* Commands

This topic describes the **debug isdn q931** command, which is useful when monitoring and troubleshooting Layer 3 of an ISDN BRI configuration.

ISDN Layer 3 debug Commands

Cisco.com

```
Router#debug isdn q931
```

- Shows call setup and teardown of ISDN network connections (Layer 3) between the access router and the ISDN switch

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.4

To display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network, use the **debug isdn q931 EXEC** command. The router tracks activities that occur on the user side only, not the network side of the network connection.

The **debug isdn** output for q921 and q931 is limited to commands and responses exchanged during peer-to-peer communication carried over the D channel. This debug information does not include data transmitted over the B channels that are also part of the router ISDN interface.

Multiple debug commands can be entered concurrently. Results will display in real time as they occur, so output may be intermingled.

ISDN BRI D Channel Monitoring

This topic describes the **show interface** command, which is useful when monitoring an ISDN BRI D channel configuration.

ISDN BRI D Channel Monitoring

Cisco.com

```
Branch#show interface bri 0
BRI0 is up, line protocol is up (spoofing)
Hardware is BRI
Internet address is 10.155.0.1/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set
Last input 00:00:04, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/255 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
580 packets input, 3651 bytes, 0 no buffer
Received 223 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
580 packets output, 3697 bytes, 0 underruns
0 output errors, 0 collisions, 5 interface resets
0 output buffer failures, 0 output buffers swapped out
3 carrier transitions
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-6.5

Use the **show interfaces bri** privileged EXEC command without arguments to display information about the BRI interface D channel only.

Command syntax:

```
show interfaces bri number[:bchannel] | [first] [last]
```

The arguments for the **show interfaces bri** command are shown in the following table.

show interfaces bri Command

Command	Description
<i>Number</i>	Interface number.
<i>:bchannel</i>	(Optional) Colon (:) followed by a specific B channel number.
<i>first</i>	(Optional) Specifies the first of the B channels; the value can be either 1 or 2 for BRI.
<i>last</i>	(Optional) Specifies the last of the B channels; the value can only be 2 for a BRI.

The **show interfaces bri** command displays the first B channel on the BRI. The alternate value for this field is **2**, which displays information about the second B channel. To display both B channels (first and last), enter **show interfaces bri number 1 2**.

If the router is an older platform and is a TE2 (non-native BRI with an external terminal adapter), use the **show interfaces serial** command.

Note that in the figure, **line protocol is up (spoofing)**. This does not mean that the B channel is active, but that it is pretending, or spoofing, to be up. This is required because routes known through this interface would otherwise be removed from the routing table. This permits packets to be forwarded to the interface. Whether or not the packets trigger the link depends on the dialer list that is configured for the interface.

The number of resets is not important for ISDN connections.

ISDN BRI B Channel Monitoring

This topic describes the **show interface** command, which is useful when monitoring an ISDN BRI B channel configuration.

ISDN BRI B Channel Monitoring

Cisco.com

```
BranchF#sh int bri 0 1 2
BR10:1 is up, line protocol is up
Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queuing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    82 packets input, 2044 bytes, 0 no buffer
    Received 82 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 short
    82 packets output, 2838 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    5 carrier transitions
(output omitted)
```

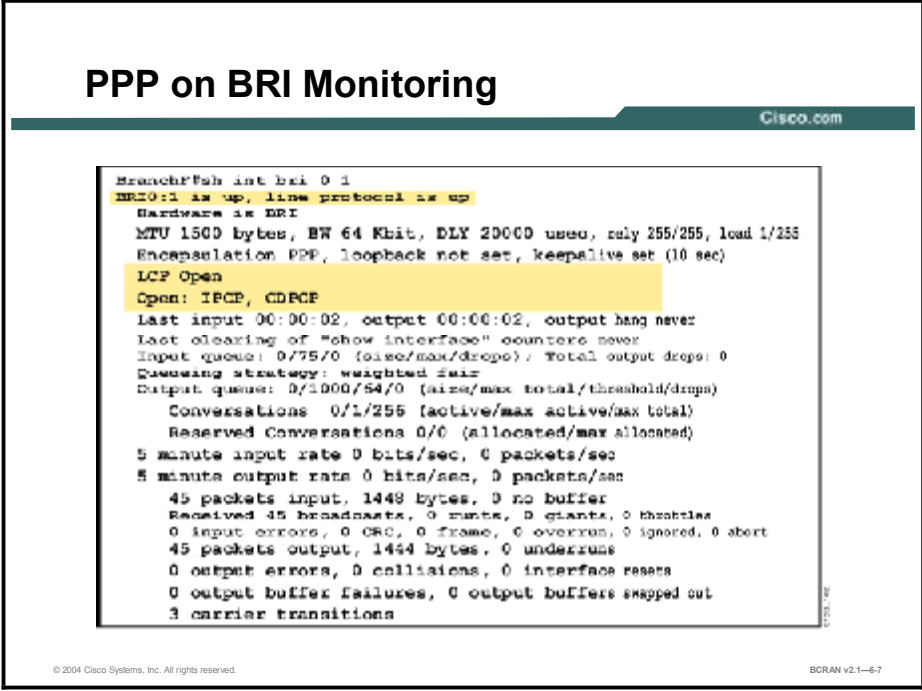
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.6

Use the **show interfaces bri *number* 1 2** (or **sh int**) command to display information about the B1 and B2 channels. If the command is entered without the parameters 1 and 2, only D channel status is shown.

For information about the DDR configuration or functions used by ISDN, use the **show dialer** and **debug dialer** commands.

PPP on BRI Monitoring

This topic describes the **show interface** command, which is useful when monitoring an ISDN BRI PPP configuration.



```
Branch#sh int bri 0/1
BRI0/1 is up, line protocol is up
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 used, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCE
Last input 00:00:02, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/255 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
45 packets input, 1448 bytes, 0 no buffer
Received 45 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
45 packets output, 1444 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
3 carrier transitions
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6-7

After you have configured for ISDN connectivity, you can check the interface to see evidence of your configuration and some of the resulting call setup details. If your router acts as a TE1 (has a native BRI), use the **show interfaces bri EXEC** command to monitor the interface and optionally, the individual B channels for the BRI interface.

The command displays information on the encapsulation and channel status for LCP and Network Control Protocol (NCP), including the protocols that can transmit over the link. The figure displays output for the first B channel of the BRI. It shows that the interface is configured for PPP encapsulation, that LCP is **Open** (currently active), and that NCP is **Open** and has negotiated the protocols IP and Cisco Discovery Protocol (CDP) on the link.

DDR Configuration Test

This topic describes the **debug dialer** command and other commands, which are useful when troubleshooting a DDR configuration.

DDR Configuration Test

Cisco.com

```
BranchF#debug dialer
BranchF#ping 10.115.0.135

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.115.0.135, timeout is 2 seconds:

BRIO: Dialing cause ip (s=10.155.0.1, d=10.115.0.135)
BRIO: Attempting to dial 6000
%LINK-3-UPDOWN: Interface BRI0:2, changed state to up
dialer Protocol up for BR0:2.
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed state to
up!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/34/36 ms
BranchF#
BRIO: rotary group to 6000 overloaded (1)
BRIO: Attempting to dial 6000
%ISDN-6-CONNECT: Interface BRI0:2 is now connected to 6000 CentralF
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-6.8

The **debug dialer** command displays debugging information about the packets received on a dialer interface. Some of the information indicates whether the multilink is up after authentication.

The **debug dialer** command also shows when overload occurs.

The **isdn test call interface** and **isdn disconnect interface** commands are useful when testing an ISDN and DDR configuration.

DDR Configuration Test (Cont.)

Cisco.com

```
Router#isdn test call interdice interface-number dialing-  
string [64]
```

```
Branch#isdn call interface bri 0 5552001
```

- Used to test your DDR configuration

```
Router#isdn disconnect interface interface-type interface-  
number {b1 | b2 | all}
```

```
Branch#isdn call interface bri 0 5552001
```

- Disconnects any data calls placed manually or caused by DDR

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6.9

The **isdn test call interface** command can be used to test the DDR configuration. Introduced in Cisco IOS software Release 12.0(3)T, this command can also be used to verify the dialing string and speed without having to know the IP address of the remote router or without configuring a dialer map or string.

Use the **isdn disconnect interface** command to disconnect any ongoing data calls placed manually or caused by DDR.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The show isdn status command can display a status summary of each of the three ISDN layers.**
- **The debug isdn q921 and debug isdn q931 commands display Layer 2 and Layer 3 debugging information.**
- **The show interface bri command can be used to display PPP, B channel, and D channel information.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—6-10

Summary (Cont.)

Cisco.com

- **The debug dialer command displays debugging information about the packets received on a dialer interface.**
- **To test your DDR connection, use the isdn call interface command.**
- **To disconnect a call, use the isdn disconnect interface command.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—6-11

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 6-1: Using ISDN and DDR to Enhance Remote Connectivity

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which Cisco router command is used to display data-link layer (Layer 2) access procedures that are taking place at the access router on the D channel (LAPD) of its ISDN interface?
- A) **debug isdn q921**
 - B) **debug isdn q931**
 - C) **debug isdn q920**
 - D) **debug isdn q941**
- Q2) Which Cisco router command is used to display network layer (Layer 3) access procedures that are taking place at the access router on the D channel (LAPD) of its ISDN interface?
- A) **debug isdn q921**
 - B) **debug isdn q931**
 - C) **debug isdn q941**
 - D) **debug isdn q951**
- Q3) Which Cisco router command is used to display information about the BRI interface D channel only?
- A) **show interface serial 0/0**
 - B) **show interface Ethernet 0/0**
 - C) **show interface bri 0 1**
 - D) **show interface bri 0**
- Q4) Which Cisco router command is used to display information about the channel?
- A) **show interface serial 0/0**
 - B) **show interface Ethernet 0/0**
 - C) **show interface bri 0 1**
 - D) **show interface bri 0 2**
- Q5) After you have configured for ISDN connectivity, you can check the interface to see evidence of your configuration.
- A) true
 - B) false

- Q6) The **isdn call interface** command can be used to verify the _____.
- A) IP address and speed
 - B) dialing string and IP address
 - C) dialing string and speed
 - D) connection

Quiz Answer Key

- Q1) A
Relates to: ISDN Layer 2 **debug** Commands
- Q2) B
Relates to: ISDN Layer 3 **debug** Commands
- Q3) D
Relates to: ISDN BRI D Channel Monitoring
- Q4) D
Relates to: ISDN BRI B Channel Monitoring
- Q5) A
Relates to: PPP on BRI Monitoring
- Q6) C
Relates to: DDR Configuration Test

Module 7

Using DDR Enhancements

Overview

This module introduces the configuration of dialer profiles and rotary groups.

Objectives

Upon completing this module, you will be able to:

- Select appropriate dialup capabilities to place a call
- Configure rotary groups and dialer profiles
- Verify proper configuration and troubleshoot any incorrect configuration to properly initiate a call
- Configure and test the use of both ISDN B channels by calling the central and branch sites from the SOHO site.

Outline

The module contains these lessons:

- Describing the Dialer Profile
- Configuring Dialer Profiles
- Verifying and Troubleshooting a Dialer Profile Configuration

Describing the Dialer Profile

Overview

This lesson contains an overview of dialer profiles, which provide improvements over dialer maps by separating the logical dialing configuration from the physical interfaces.

Relevance

To establish a dialup connection, there must be an understanding of the technology and components required, and how to configure them. This lesson provides an overview of dialer profile features and concepts.

Objectives

Upon completing this lesson, you will be able to:

- Describe the purpose of a dialer profile
- List the four elements of a dialer profile
- Describe the use of dialer map classes

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

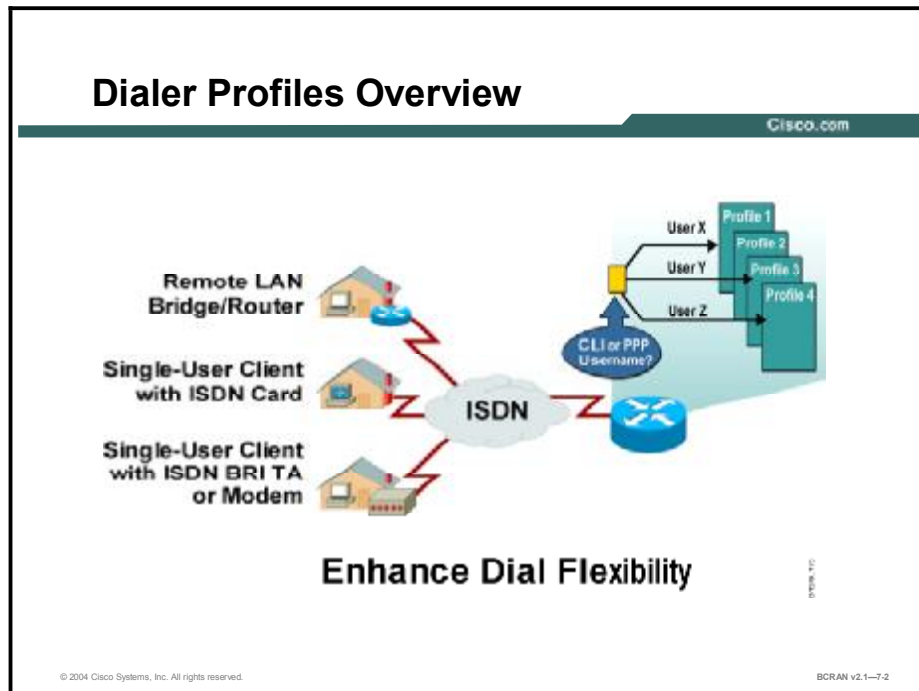
Outline

This lesson includes these topics:

- Overview
- Dialer Profile
- Dialer Profile Features
- Dialer Profile Elements
- Dialer Map Classes
- Summary
- Quiz

Dialer Profile

This topic identifies the basic concepts of a dialer profile.



Dialer profiles separate the logical configuration from the interface receiving or making calls. Profiles can turn features on or off, and can define encapsulation, access control lists, and minimum or maximum calls.

With dialer profiles, the logical and physical configurations are dynamically bound to each other on a per-call basis, which allows physical interfaces to dynamically take on different characteristics based on incoming or outgoing call requirements.

Legacy dial-on-demand routing (DDR), although useful in many scenarios, is restrictive in instances where it is desired to differentiate per user by defining different characteristics to different users. This cannot be accomplished with legacy DDR.

Dialer profiles were designed as a new DDR model to allow a user access to a specific profile. The profile would determine the characteristics of a particular user, and would be dynamically bound to a physical interface for incoming or outgoing DDR calls.

Note Dialer profiles support PPP, High-Level Data Link Control (HDLC), Frame Relay, or X.25 encapsulation for inbound or outbound dialing. PPP encapsulation is the recommended choice, and the discussion here will focus on PPP.

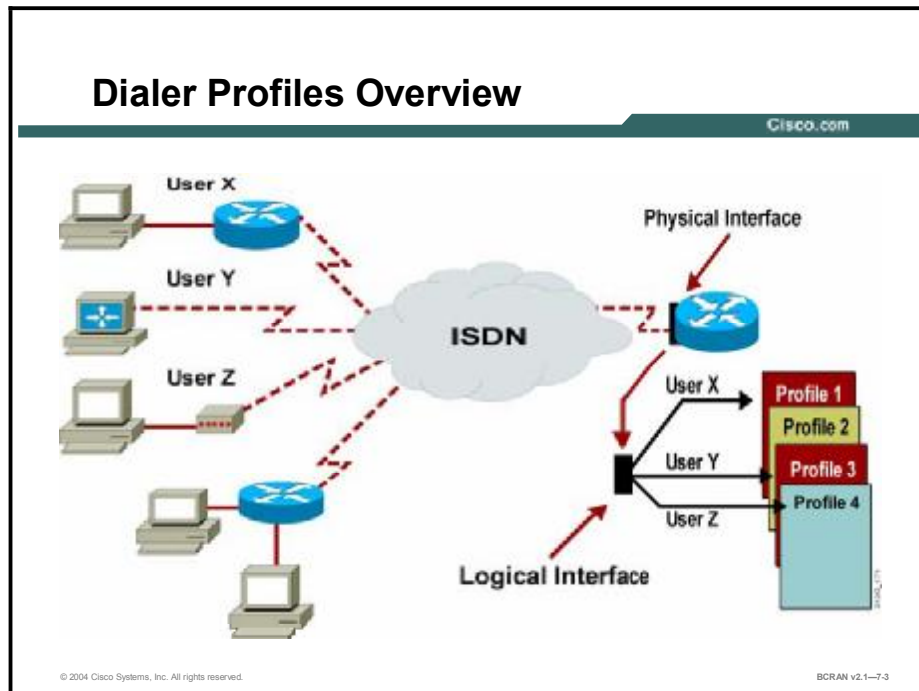
The advantages of dialer profiles over legacy DDR include:

- There is no requirement for a Layer 3- to Layer 2-map and the added complexities of managing multiple maps. Unlike legacy DDR, the dialer profile is a point-to-point interface.
- Dialer profiles allow you to configure different members of a physical interface with different Layer 3 network addresses.
- Dialer profiles allow physical interfaces to take on different characteristics that are based on incoming or outgoing call requirements.
- Dialer profiles allow a backup interface to be nondedicated and useable when the primary interface is operational.
- A DDR interface allows you to control the number of minimum and maximum connections.

Note Prior to using dialer profiles, the ISDN bearer (B) channels on a BRI or PRI inherited the same physical interface configuration. When used as a backup interface, all B channels were down and unusable until the interface came out of backup mode. Dialer profiles solved this issue.

Dialer Profile Features

This topic describes the different features of dialer profiles.



Dialer profiles were first introduced in Cisco IOS Software Release 11.2. They help users design and deploy complex and scalable circuit-switched internetworks by implementing a new DDR model in Cisco routers and access servers. Dialer profiles separate the logical portion of DDR (that is, the network layer, encapsulation, and dialer parameters) from the physical interface that places or receives calls.

Dialer profiles address several dialup issues:

- **One configured interface per ISDN interface:** Before dialer profiles, all ISDN B channels inherited the configuration of the physical interface.
- **Dialer map complexity:** Before dialer profiles, one dialer map was required per dialer per protocol, making multiprotocol configurations very complex.
- **Limited dial backup:** When a BRI or PRI is used to back up an interface, all the B channels are down and the entire interface is idle. None of the B channels could be used until the interface came out of backup mode. In addition, in a packet-switching environment with many virtual circuits that may need to be backed up individually, the one-to-one relationship between interfaces and backup interfaces would not scale well.

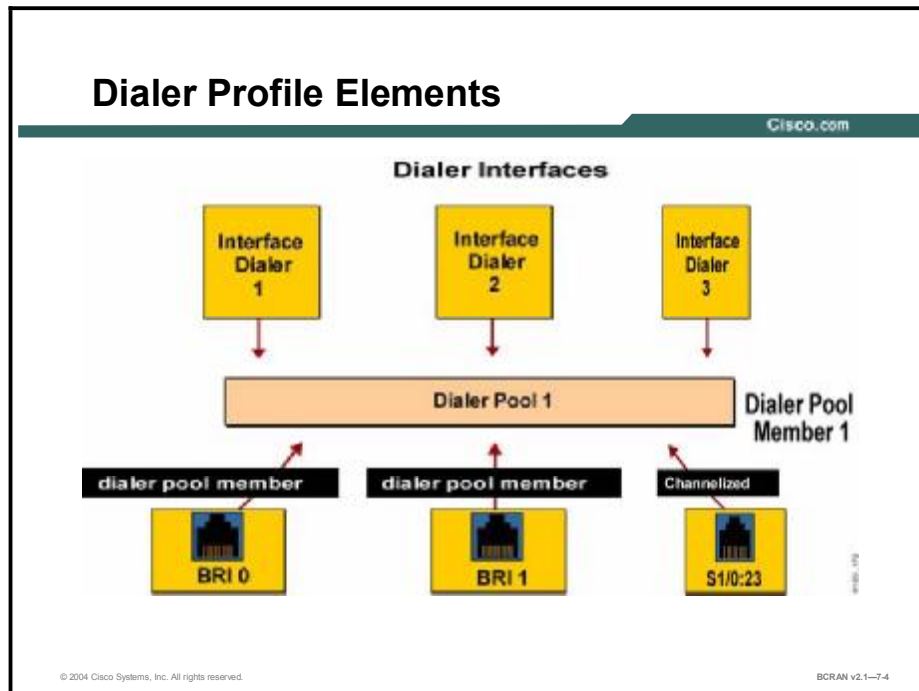
Dialer profiles let you create different configurations for each call on an ISDN interface, providing these configuration advantages:

- **Different IP subnets:** You can configure each call on the ISDN interface with different IP subnets.
- **Different encapsulations:** You can use different encapsulations of each call on the ISDN interface. However, only PPP and HDLC encapsulation are now supported.
- **Different DDR parameters:** You can set different DDR parameters for each call on the ISDN interface.
- **Multiple dialer pools:** You can eliminate the waste of ISDN B channels by letting ISDN BRI interfaces belong to multiple dialer pools.

Note Because of changes that were made to dialer profiles, it is recommended that Cisco IOS Software Release 12.1 or later be used.

Dialer Profile Elements

This topic describes the elements that make up a dialer profile.



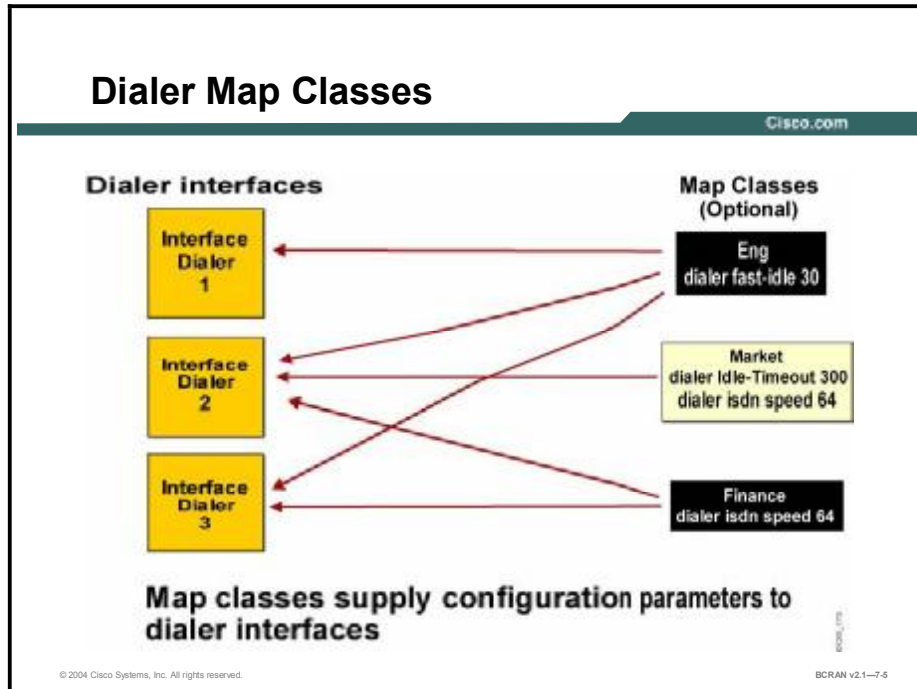
A dialer profile consists of these elements:

- **Dialer interface:** A logical entity that uses a per-destination dialer profile.
 - All configuration settings specific to the destination go into the dialer interface configuration. Multiple dialer maps can be specified for the same dialer interface. A dialer map can be associated with different per-call parameters that are defined with each dialer map class.
 - The dialer interface is configured with the IP address of the destination network, encapsulation type, PPP authentication type, dialer remote name (for PPP Challenge Handshake Authentication Protocol [CHAP]), dialer string or dialer map, dialer pool number, dialer group number, dialer list number, Multilink PPP (MLP), and optional dialer Idle-Timeout and dialer inband entries.
- **Map class:** An optional element that defines specific characteristics for a call to a specified dial string.
- **Dialer pool:** Each dialer interface references a dialer pool, which is a group of one or more physical interfaces associated with a dialer profile.
- **Physical interfaces:** Interfaces in a dialer pool are configured for encapsulation parameters and to identify the dialer pools of which the interface is a member.
 - **Channelized T1:** Access link operating at 1.544 Mbps that is subdivided into 24 channels (23 B channels and 1 data (D) channel) of 64 kbps each. The individual channels or groups of channels connect to different destinations. It supports DDR, Frame Relay, and X.25, and is also called fractional T1.

Note Dialer profiles support PPP or HDLC encapsulation, PPP authentication (Password Authentication Protocol [PAP] or CHAP), and MLP.

Dialer Map Classes

This topic describes dialer map classes.



Map classes are optional. They are used to specify different characteristics for different types of calls on a per-destination basis.

In the figure shown, three map classes are used with the dialer interfaces. The telephone number being called determines which map class to use. A different map class might be used if a different number is called.

The same map class can be used for multiple dialer interfaces. The configuration parameters of a map class are specific to one or more destinations.

As an example, the map class for one destination might specify an ISDN speed of 64 kbps, while a map class for a different destination might specify an ISDN semipermanent connection. The dialer map class can also contain optional dialer timing parameters including **dialer fast-idle**, **dialer idle-timeout**, and **dialer wait-for-carrier-time**.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

Dialer profile elements include:

- Dialer interface
- Dialer pool
- Physical interfaces
- Optional dialer map-class

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-7-6

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which Cisco router feature was designed as a new DDR model to allow a user access to a specific profile?
- A) dialer calls
 - B) dialer maps
 - C) dialer profiles
 - D) dialer groups
- Q2) Which Cisco router feature separates the logical portion of DDR (for example, the network layer, encapsulation, and dialer parameters) from the physical interface that places or receives calls?
- A) dialer groups
 - B) dialer calls
 - C) dialer maps
 - D) dialer profiles
- Q3) Which element of the dialer profile is a logical entity that uses a per-destination dialer profile?
- A) a dialer interface
 - B) the dialer map class
 - C) a dialer pool
 - D) physical interfaces
- Q4) Which optional Cisco dialer map router feature is used to specify different characteristics for different types of calls on a per-destination basis?
- A) map rooms
 - B) map profiles
 - C) map classes
 - D) map calls

Quiz Answer Key

- Q1) C
Relates to: Dialer Profile
- Q2) D
Relates to: Dialer Profile Features
- Q3) A
Relates to: Dialer Profile Elements
- Q4) C
Relates to: Dialer Map Classes

Configuring Dialer Profiles

Overview

This lesson covers dialer profile configuration and how it relates the logical configuration to the physical interface.

Relevance

To establish dialup connections using dialer profiles, you must understand the steps to configure a dialer profile.

Objectives

Upon completing this lesson, you will be able to:

- Configure physical interfaces to operate with dialer profiles
- Create multiple dialer profiles
- Configure dialer interfaces to be used in a dialer profile
- Customize a dialer profile for the dialup connection

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

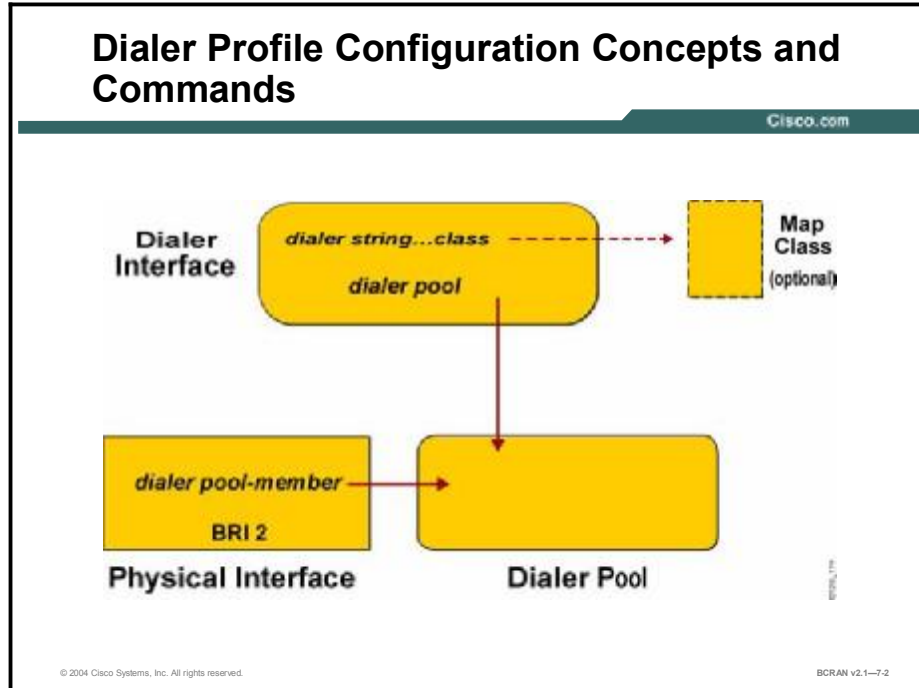
Outline

This lesson includes these topics:

- Overview
- Dialer Profile Configuration Concepts and Commands
- Typical Dialer Profile Application
- Configuration of Dialer Interfaces
- Configuration of Physical Interfaces
- Dialer Profiles Configuration Example
- Summary
- Quiz

Dialer Profile Configuration Concepts and Commands

This topic describes the basic configuration steps for a dialer profile.



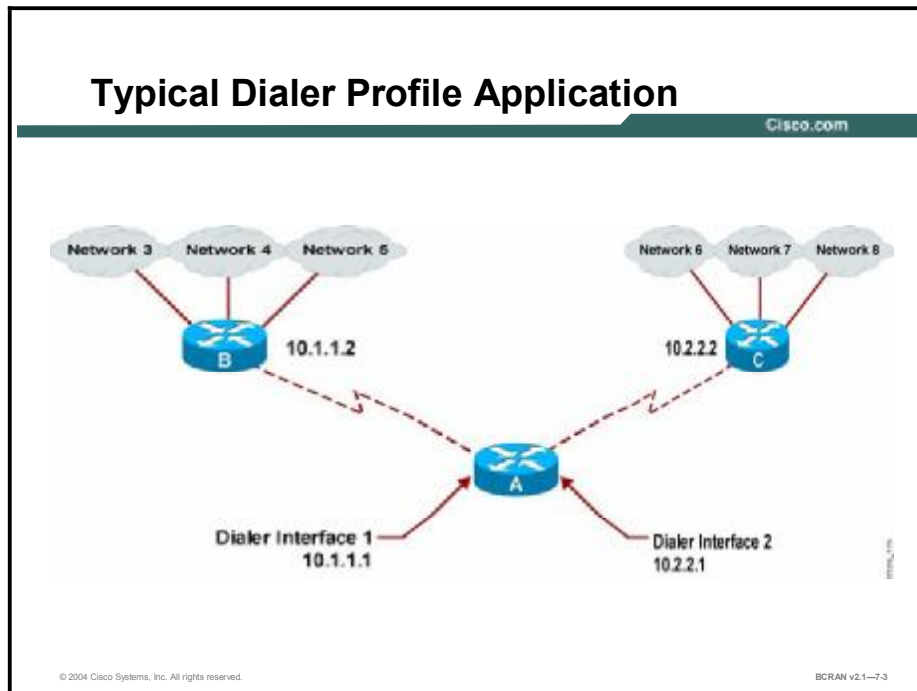
The configuration commands that create the relationships between the elements of a dialer profile are displayed in the figure. The commands and the configuration mode in which they are used are described in the following table.

Dialer Profile Configuration Commands

Command	Description
dialer string number class map class-name	A dialer interface command that specifies the telephone number of the destination. The use of the optional keyword class , followed by the map class name, points to a specific map class and uses the configuration commands of that map class in the call.
dialer pool number	A dialer interface command that specifies the pool of physical interfaces available to reach the destination subnetwork. A number between 1 and 255 identifies the pool.
dialer pool- member number	An interface configuration command that associates and places a physical interface in a specifically numbered pool. A physical interface can belong to multiple dialer pools. Contention for a specific physical interface is resolved with a configured priority, which is optional.
Note	When you use the dialer pool command to configure a dialer interface, you create a dialer profile. You must use the dialer string command to allow the router to dial out.

Typical Dialer Profile Application

This topic describes an example of a dialer profile application.



The configuration displayed in this figure provides an example of a typical application of dialer profiles. Network Router A has dialer interface 1 for DDR with subnetwork 10.1.1.0, and dialer interface 2 for DDR with subnetwork 10.2.2.0.

Calls destined for subnetwork 10.1.1.0, and any of the networks reachable through it (networks 3, 4, and 5), use dialer interface 1.

Calls destined for subnetwork 10.2.2.0, and any of the networks reachable through it (networks 6, 7, and 8), use dialer interface 2.

Configuration of Dialer Interfaces

This topic describes the configuration of multiple dialer profiles.

Configuration of Dialer Interfaces

Cisco.com

```
interface dialer1
 ip address 10.1.1.1
 255.255.255.0
 encapsulation ppp
 dialer remote-name smalluser
 dialer string 5554540
 dialer pool 0
 dialer-group 1
 ppp authentication chap
 ppp multilink
 !
interface dialer2
 ip address 10.2.2.1
 255.255.255.0
 encapsulation ppp
 dialer remote-name mediumuser
 dialer string 5551234 class Eng
 dialer load-threshold 50 either
 dialer pool 1
 dialer-group 1
 ppp multilink
 (cont.)
```

```
interface dialer3
 ip address 10.3.3.1 255.255.255.0
 encapsulation ppp
 dialer remote-name poweruser
 dialer string 415555321 class Eng
 dialer hold-queue 10
 dialer idle-timeout 9999
 dialer pool 2
 dialer-group 1
 ppp multilink
 !
map-class dialer Eng
 dialer ixm speed 56

dialer-list 1 protocol IP permit
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-7.4

To configure dialer profiles, perform these tasks:

1. Configure one or more dialer interfaces.
2. Configure a dialer string and optionally a dialer map class to specify different characteristics on a per-call basis.
3. Configure the physical interfaces and attach them to a dialer pool.

Any number of dialer interfaces can be configured on a router. Each dialer interface is the complete configuration for a destination. The **interface dialer** global command creates a dialer interface and enters interface configuration mode.

The figure displays dialer profiles that are created using the commands listed in the table.

interface dialer Command

Command	Description
ip address address mask	Specifies the IP address and mask of the destination network.
dialer remote-name name	Specifies the remote router name, which is passed for CHAP authentication.
dialer string string class map class-name	Defines the destination of the router telephone number, and supports optional map classes. Map classes are covered in the next table.
dialer load-threshold load [outbound inbound either]	Specifies at what traffic load additional links will be brought up for MLP. Valid values are 1 to 255. Optionally, you may specify which direction of traffic is used to calculate the actual load. If you want the links to remain in a MLP bundle indefinitely, use a very high dialer Idle-Timeout value (9999, for example) instead of a dialer load-threshold.
dialer hold-queue number-of-packets	Specifies the length of the queue for packets that are waiting for the line to come up. Valid values are from 0 to 100.
dialer pool number	Binds a dialer interface to a dialer pool configured with the dialer remote-name command that gives the CHAP username for a remote user. Valid values are from 1 to 255.
dialer-group group-number	Specifies a dialer list that defines “interesting” packets to trigger a call for DDR. The dialer-list command can reference access lists to more specifically define “interesting” packets. Valid values are from 1 to 10.
ppp multilink	Specifies that this dialer interface uses MLP. This command is placed on the physical interface for incoming calls, in the dialer profile for outgoing calls, and on both the interface and dialer profile when incoming and outgoing calls are expected.
dialer-list group-number	Associates a DDR dialer list for dialing by protocol or by a combination of protocols and a previously defined access-list.

After the interface is configured, an optional dialer map class can be defined. Use the **map-class dialer class-name** command to specify a map class and enter the map class configuration mode. In the figure, the dialer “interface dialer3” is associated with map class “Eng.” Any dialer associated with this map class will set the ISDN line speed to 56 kbps. You can set the speed to 56 kbps, but 64 kbps is the default value.

The following table shows other **map-class** commands that are available in map class configuration mode.

map-class Commands

Command	Description
dialer isdn [speed 56 spc]	Specifies the ISDN line speed. The default is 64 kbps; therefore, the parameter is used only with 56-kbps line speed. [spc] is used for specifying that an ISDN semipermanent connection will be used for calls associated with this map.
dialer idle-timeout seconds	Specifies the idle timer values to use for the call. This timer disconnects the call if there has been no data for the specified time. Defaults to 120 seconds.
dialer fast-idle seconds	Specifies the fast-idle timer value to use for a call. This timer specifies a quick disconnect time if there is another call waiting for the same interface and the interface is idle. The waiting call will not have to wait for the idle timer to expire. Defaults to 20 seconds.
dialer wait-for-carrier-time seconds	Specifies the Carrier Detect (CD) time value to use for the call. The call is abandoned if no carrier is detected within the time value specified.

Configuration of Physical Interfaces

This topic describes the steps that are needed to configure the physical interfaces used by the dialer profiles.

Configuration of Physical Interfaces

Cisco.com

```
interface bri0/0
encapsulation ppp
dialer pool-member 0 priority 100
ppp authentication chap
ppp multilink
!
interface bri0/1
encapsulation ppp
dialer pool-member 1 priority 150
ppp authentication chap
ppp multilink
!
interface S1/0:23
encapsulation ppp
dialer pool-member 0 priority 200
dialer pool-member 1 priority 200
dialer pool-member 2 priority 200
ppp authentication chap
ppp multilink
```

dialer pool 0
BR0/0 (priority 100)
S1/0:23 (priority 200)

dialer pool 1
BR0/1 (priority 150)
S1/0:23 (priority 200)

dialer pool 2
S1/0:23 (priority 200)

***The higher the priority number assigned, the higher the priority given.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-7-5

Use the **dialer pool-member** command to assign a physical interface to a dialer pool. An interface can be assigned to multiple dialer pools by using this command to specify several dialer pool numbers. A combination of synchronous, serial, BRI, or PRI interfaces can be assigned with dialer pools.

Use the **priority** option of this command to set the interface priority within a dialer pool. The **priority** keyword is used only when dialing out.

The following table shows the arguments that are used with the **dialer pool-member** command.

dialer pool-member Command

Command	Description
<i>number</i>	Specifies the dialer pool number. This is a decimal value from 1 to 255.
<i>priority priority number</i>	Sets the priority of the physical interface within the dialer pool. This is a decimal value from 1 (lowest) to 255 (highest). Interfaces with the highest priority number are selected first when dialing out. Use this to determine which interfaces are used the most, or which are reserved for special pool uses.
<i>min-link minimum</i>	Sets the minimum number of ISDN B channels on an interface reserved for this dialer pool. This is a number from 1 to 255 (used for dialer backup).
<i>max-link maximum</i>	Sets the maximum number of ISDN B channels on an interface that can be used for this dialer pool. This is a number from 1 to 255.

Note The optional **min-link** and **max-link** apply to ISDN interfaces only. The **max-link** defaults to 255, and the **min-link** defaults to 0. A reserved channel is inactive until it is used by the specified interface.

Dialer Profiles Configuration Example

This topic describes an example configuration of two dialer profiles.

Dialer Profiles Configuration Example

Cisco.com

```
interface dialer0
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name RouterA
 dialer pool 1
 dialer string 5551212
 dialer-group 1
 ppp multilink
!
interface dialer1
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name RouterB
 dialer pool 1
 dialer string 5551234
 dialer-group 1
 ppp multilink (cont.)
```

```
interface bri0
 encapsulation ppp
 dialer pool-member 1
 ppp authentication chap
 ppp multilink
!
interface serial0
 ip unnumbered loopback0
 backup interface dialer0
 backup delay 5 10
!
interface serial1
 ip unnumbered loopback0
 backup interface dialer1
 backup delay 5 10
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-7-6

The dialer interfaces are visible to the upper-layer protocols only, not to the physical interfaces making up the dialing pool. Because one dialer interface maps to one destination, addressing, access lists, and static routes can be specified on a per-destination basis, regardless of which interface actually carries out the call.

Dialer commands can be configured under the dialer interface directly. The same command may appear more than once, possibly with different parameters. The order of precedence is as follows (from highest to lowest):

- Map class parameters
- Interface parameters

Note Refer to the “Configuring Dialer Interfaces” figure earlier in this lesson for examples of the use and syntax for the **map-class** command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Dialer profiles allow logical and physical configurations to be dynamically bound to each other on a per-call basis.**
- **Basic configuration of an interface dialer includes dialer string, dialer pool, dialer-group, encapsulation, and logical address.**
- **Physical interfaces are assigned via the dialer pool-member command.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-7.7

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which interface configuration command associates and places a physical interface in a specifically numbered pool?
- A) **dialer pool-member *number***
 - B) **dialer pool *number***
 - C) **dialer string *number class map class-name***
 - D) **dialer interface**
- Q2) Which dialer interface command specifies the phone number of the destination?
- A) **dialer interface**
 - B) **dialer string *number class map class-name***
 - C) **dialer pool *number***
 - D) **dialer pool-member *number***
- Q3) Which Cisco router global command creates a dialer interface and enters interface configuration mode?
- A) **interface caller**
 - B) **interface group**
 - C) **interface dialer**
 - D) **interface port**
- Q4) Which Cisco router command is used to assign a physical interface to a dialer pool?
- A) **dialer pool-member**
 - B) **pool-dialer member**
 - C) **dialer member-pool**
 - D) **pool member-dial**
- Q5) At which Cisco router configuration level are dialer profile commands configured?
- A) under the serial interface directly
 - B) under the dialer interface directly
 - C) under the Ethernet interface directly
 - D) under the BRI interface directly

Quiz Answer Key

- Q1) A
Relates to: Dialer Profile Configuration Concepts and Commands
- Q2) B
Relates to: Typical Dialer Profile Application
- Q3) C
Relates to: Configuration of Dialer Interfaces
- Q4) A
Relates to: Configuration of Physical Interfaces
- Q5) B
Relates to: Dialer Profiles Configuration Example

Verifying and Troubleshooting a Dialer Profile Configuration

Overview

This lesson covers the commands that are used to verify and troubleshoot a dialer profile configuration.

Relevance

To verify and troubleshoot the operation of a dialup connection using dialer profiles, you must understand the **show** and **debug** commands.

Objectives

Upon completing this lesson, you will be able to:

- Describe the output from the **show dialer** command
- Describe the output from the **show interfaces dialer** command
- Describe the output from the **debug dialer** command
- Troubleshoot unsuccessful outgoing calls
- Troubleshoot unsuccessful incoming calls

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Verification of Dialer Profiles
- Outbound Dialing Issues
- Outbound Binding Issues
- Examples
- Inbound Call Issues
- Disconnect Issues
- Summary
- Quiz

Verification of Dialer Profiles

This topic describes the show dialer interface and the **show dialer interface** commands.

```
Verification of Dialer Profiles
Cisco.com

NASM#show dialer interface bri0
BR10 - dialer type = ISDN

Dial String      Successes      Failures      Last called   Last status
5553972          6              0             19 secs      Successful
0 incoming call(s) have been screened.
BRIC: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip [s=10.1.1.8, d=10.1.1.11]

Interface bound to profile Dialer0

Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5553972 (myatml)

BRIC: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

The **show dialer interface bri number** command displays information in the same format as the legacy DDR statistics on incoming and outgoing calls.

In the figure, the message “Dialer state is data link layer up” suggests that the dialer came up properly.

If the message “physical layer up” is displayed, it means that the line protocol came up but the Network Control Protocol (NCP) did not.

In the figure, “Dial reason” refers to the source and destination addresses of the packet that initiated the dialing.

Verification of Dialer Profiles (Cont.)

Cisco.com

```
Router# show interfaces dialer1
Dialer1 is up, line protocol is up
Hardware is Unknown
Internet address is 1.1.1.1/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set
DTR is pulsed for 1 seconds on reset
Interface is bound to BRI0:1
Last input 00:00:38, output never, output hang never
Last clearing of "show interface" counters 00:05:36

< Output Omitted >

Bound to:
BRI0:1 is up, line protocol is up
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive not set
Interface is bound to Dialer1 (Encapsulation PPP)

< Output Omitted >
```

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-7-3

The **show interface dialer** command displays information on incoming and outgoing calls.

In the figure, the messages “Dialer1 is up, line protocol is up” and “BRI0:1 is up, line protocol is up” suggest that the dialer came up properly.

The message “Interface is bound to BRI0:1” informs you that this dialer is bound to the 1 B channel.

You also know that BRI0:1 is active and that the PPP encapsulation has been applied by the dialer interface.

Outbound Dialing Issues

This topic describes the use of the **debug dialer** command.

Outbound Dialing Issues: Dialing Never Occurs

Cisco.com

```
Router# debug dialer
Router#
Router# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
*Mar 1 00:24:47.242: BR0 DDR: rotor dialout [priority]
*Mar 1 00:24:47.250: BR0 DDR: Dialing cause ip (s=192.168.1.1, d=10.1.1.1)
*Mar 1 00:24:47.250: BR0 DDR: Attempting to dial 5551111
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-7.4

As is the case with legacy DDR, the most appropriate command for debugging dialer profile problems is **debug dialer**. In the case of a successful call, the debug will not indicate any more than the logged messages already have indicated. In the case of a failure, there are a number of problems that can be the cause.

Enable **debug dialer** and generate interesting traffic to the peer. The router should attempt to dial. In the figure, dialing is attempted but never occurs.

The following is an example output:

```
Router# debug dialer
Router# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
*Oct 1 00:24:47.242: BR0 DDR: rotor dialout [priority]
*Oct 1 00:24:47.250: BR0 DDR: Dialing cause ip (s=192.168.1.1,
d=10.1.1.1)
*Oct 1 00:24:47.250: BR0 DDR: Attempting to dial 5551111
```

Verify if **debug dialer** generates any debug output. If there is no debug dialer output, it is most likely because the IP packet being sent is not routed to the dialer interface, or binding fails.

Outbound Binding Issues

This topic describes troubleshooting for unsuccessful outgoing calls.

Outbound Binding Issues: Dialing Never Occurs

Cisco.com

```
Router# *Mar 1 07:20:45.676: Di15: Cannot place call, no dialer pool set
```

- **Configure the dialer pool command on the dialer interface.**

```
Router# *Mar 1 11:54:14.937: Di15: No free dialer - starting fast idle timer
```

- **Enter the dialer pool-member command on the physical interface to associate it to the dialer pool.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—7.5

If the dialer profile is not associated with a dialer pool, **debug dialer** will indicate the following for an outbound call:

```
*Mar 1 07:20:45.676: Di15: Cannot place call, no dialer pool set
```

The solution is to configure the **dialer pool** command on the dialer interface.

If the physical interface is not associated with any pool, the debug message on the calling router will be the same as in the case where physical interfaces are no longer available, causing the fast idle timer to trigger:

```
*Mar 1 11:54:14.937: Di15: No free dialer - starting fast idle timer
```

The solution is to enter the **dialer pool-member** command on the physical interface to associate it to a dialer pool.

After you have verified that the dialer pool configuration is correct, perform the following tasks:

- Verify that IP is configured on the dialer interface. You should either have an IP address on the interface or **ip unnumbered** *type number* (where *type number* is another interface on which the router has an assigned IP address) or **ip address negotiated**.
- Check whether the command **ip routing** is configured. When you look at your configuration using the **show running-config** command, you should not see the command **no ip routing** configured.
- Ensure that there is a static route pointing at the dialer interface. The following example is a static route for 172.22.53.0/24 with next-hop dialer 1:

```
Router(config)#ip route 172.22.53.0 255.255.255.0 dialer 1
```

- Verify that the dialer interface is not in shutdown state. Use the **show interface dialer interface** command to verify that the interface is up/up or check to see if **no shutdown** exists under the dialer interface configuration.

Examples

This topic describes examples of troubleshooting when dialing does not occur.

Examples

Cisco.com

- **No dialer-group configured on the dialer interface**

No dialer-group defined

- **Dialer-list does not exist**

dialer-list 1 not defined

- **No physical interface available to make the call**

No free dialer

- **No dialer-string configured on the dialer interface**

Cannot place call, no dialer string set

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—7-6

Another scenario occurs when there is **debug** output, but there is no “Attempting to Dial” message generated. In this case, there is probably an IP packet routed to the interface, but the router discards it and does not initiate the call for some reason. Look at the **debug dialer** output to find out why the call attempt is not made.

The following are examples of output generated by the **debug dialer** command. The examples focus on specific problems followed by possible solutions.

Example 1

```
*Mar 1 00:07:22.255: Di1 DDR: ip (s=10.1.0.1,
d=192.168.201.1),
100 bytes, outgoing uninteresting (no dialer-group defined).
```

There is no dialer-group configured on the dialer interface. Add a dialer-group as in this example:

```
interface Dialer1
dialer-group 1
```

Example 2

```
*Mar 1 00:08:24.919: Di1 DDR: ip (s=10.1.0.1,
d=192.168.201.1),
    100 bytes, outgoing uninteresting (dialer-list 1 not
defined).
```

There is a dialer group statement on the dialer interface, but the dialer list referred to does not exist. Configure the dialer list as in this example:

```
dialer-list group-number protocol ip permit
```

Note The value for *group-number* of the **dialer-group** command must match *dialer-group-number* of the **dialer-list** command. For example, the number 1 in dialer-group 1 matches dialer-list 1.

Example 3

```
*Mar 1 00:25:32.551: Di1 DDR: ip (s=10.1.0.1,
d=192.168.201.1),
    100 bytes, outgoing interesting (ip PERMIT)
*Mar 1 00:25:32.555: Di1 DDR: No free dialer - starting fast
idle timer.
```

In this case, the outgoing packet is considered interesting enough to bring up the link, but there is no physical interface available to place the call. Make sure that **dialer pool-member number** is configured in the physical interface and **dialer pool number** is configured in the dialer interface. For example:

```
interface BRI0
    dialer pool-member 1
!
interface Dialer1
    dialer pool 1
```

Also, verify that the physical interface is not in shutdown state. Use the **no shutdown** command on the physical interface.

Example 4

```
*Mar 1 00:37:24.235: Di1 DDR: ip (s=10.1.0.1,
d=192.168.201.1),
    100 bytes, outgoing interesting (ip PERMIT)
*Mar 1 00:37:24.239: Di1 DDR: Cannot place call, no dialer
string set.
```

In this case, no **dialer string dial-string** is configured on the dialer interface. The router wants to place a call but does not know the number to call. Define a dialer string:

```
interface Dialer1
    dialer string 8134
```

Inbound Call Issues

This topic describes troubleshooting for unsuccessful incoming calls.

Inbound Call Issues

Cisco.com

- Check configured dialer pool on dialer interface.
- Check authentication on the physical interface.
- Check remote dialer name on the dialer interface.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—7.7

When incoming calls fail to connect with a dialer profile, there may be a problem with binding the physical interface to the dialer interface for that call. Verify that the router meets one of the conditions for binding.

Follow these steps:

Step 1 If the dialer profile is not associated with a dialer pool, **debug dialer** will indicate the following for an inbound call:

```
*Mar 1 11:51:24.873: BRI0:1: Authenticated host Branch with no matching dialer profile
```

Solution: Configure the **dialer pool** command on the dialer interface.

Step 2 There are four attempts to bind. Assuming that you have more than one dialer profile, the calling line identification (CLID) and dialed number identification service (DNIS) bind attempt fails, and PPP authentication is not configured (preempting the possibility of the fourth test), then the following **debug dialer** message will be generated on the called router:

```
*Mar 1 11:59:36.521: ISDN BR0:1: Incoming call rejected, unbindable
```

Solution: Configure **ppp authentication chap | pap [callin]** on the physical interface.

Step 3 If PPP authentication is enabled on the physical interface, then the fourth attempt to bind will proceed. The router will use the authenticated username in an attempt to bind to one of the dialer interfaces in the dialer pool. If that attempt fails, you will see the following debug output on the called router.

```
*Mar 1 12:03:32.227: BRI0:1: Authenticated host Branch with no  
matching dialer profile
```

Solution: Configure the **dialer remote-name** command on the dialer interface. The name specified must exactly match the username provided by the remote router for authentication. In this example, the authenticated username is “Branch.”

Disconnect Issues

This topic describes troubleshooting for calls that are unexpectedly disconnected.

Disconnect Issues

Cisco.com

- Check dialer Idle-Timeout values.
- Check interesting traffic definition (ACL).

```
router#debug dialer packet
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-7.8

A common problem affecting dialup links is unexpected call drops. Dialer drops are calls that are disconnected prematurely, or calls that never disconnect. There are many reasons for this, including hardware failures and telco issues. However, one of the most common causes for unexpected call drops is the expiration of the Idle-Timeout.

Another common Idle-Timeout problem occurs when the link does not disconnect because the Idle-Timeout never expires. This situation can result in high toll charges for connections that are charged, based on the time that the call is connected.

If the call disconnects unexpectedly, or the call never disconnects, check the dialer Idle-Timeout and interesting traffic definition. Use the **debug dialer packet** command to see if a particular packet is interesting or not. For example:

```
Apr 26 01:57:24.483: Di1 DDR: ip (s=192.168.1.1, d=224.0.0.5),  
64 bytes,  
    outgoing uninteresting (list 101)  
Apr 26 01:57:26.225: Di1 DDR: ip (s=192.168.1.1, d=10.1.1.1),  
100 bytes,  
    outgoing interesting (list 101)
```

In the last example, Open Shortest Path First (OSPF) hellos are uninteresting per access-list 101, while the second packet is interesting per access-list 101.

Adjust the **dialer idle-timeout** in the dialer interface configuration. The default is 120 seconds, but you may wish to raise or lower this value depending on your needs.

Change the interesting traffic definition (configured with the **dialer-list** command). If the call disconnects prematurely, you may wish to define the interesting traffic more loosely. If the call never disconnects, change your interesting traffic definition to be more restrictive. For example, you can define routing protocol traffic as uninteresting. The following is a sample interesting traffic definition:

```
access-list 101 remark Interesting traffic for dialer-list 1
access-list 101 deny ospf any any
!--- mark OSPF as uninteresting. This will prevent OSPF hellos
!--- from keeping the link up.
access-list 101 deny udp any any eq ntp
!--- Define ntp traffic as NOT interesting.
!--- This will prevent periodic ntp traffic from keeping the
!--- link up indefinitely.
access-list 101 permit ip any any
!--- All other IP traffic is interesting. Change this
!--- depending on your traffic needs.
dialer-list 1 protocol ip list 101
```

The following symptoms may indicate issues related to the Idle-Timeout:

- Calls get disconnected every 120 seconds after the connection is established.
This disconnection is normally due to the default Idle-Timeout of 120 seconds being enabled, while the interesting traffic definition is either not defined or is not applied to the interface. Although the **dialer in-band** command enables a default Idle-Timeout of 120 seconds on the interface, this value does not appear in the **show running-configuration** output. Because the default Idle-Timeout is not visible, a 120-second disconnect is often misdiagnosed.
- Calls get disconnected every *x* minutes after the connection is established.
This disconnection occurs because the Idle-Timeout is being configured (using the **dialer idle-timeout** command), while the interesting traffic definition is either not defined or is not applied to the interface.
- Calls disconnect prematurely. This problem is probably due to a low dialer Idle-Timeout value, or a restrictive interesting traffic definition.
- Calls do not disconnect. This problem is probably caused by a high dialer Idle-Timeout value, combined with a loose interesting traffic definition.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The show dialer and show interface dialer commands are useful when verifying proper operation of a dialer profile.**
- **The debug dialer command is useful when troubleshooting dialer profile functionality.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—7-9

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 7-1: Using Dialer Profiles to Enhance DDR

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which Cisco router command displays information on incoming and outgoing calls?
- A) **show interface dialer**
 - B) **show dialer ver**
 - C) **show dialer mem**
 - D) **show dialer calls**
- Q2) What is the most appropriate command for debugging dialer profile problems?
- A) **show dialer**
 - B) **debug dialer**
 - C) **show calls**
 - D) **debug calls**
- Q3) When debug dialer output indicates that the dialer profile is not associated with a dialer pool, which of the following is the most appropriate solution?
- A) enter the **dialer pool-member** command on the physical interface to associate it with a dialer pool
 - B) configure the **dialer call** command on the dialer interface
 - C) configure the **dialer pool** command on the dialer interface
 - D) configure the **dialer group** command on the dialer interface
- Q4) When you have a problem or error message such as “no dialer group configured on the dialer interface,” what is most likely the problem?
- A) No dialer string is set.
 - B) There is no free dialer.
 - C) No dialer group has been defined.
 - D) There is no dialer list.
- Q5) How many attempts are made to bind the physical interface with the dialer interface for that call?
- A) 2
 - B) 3
 - C) 4
 - D) 5

- Q6) A common issue affecting dialup links is unexpected call drops. Which command is most appropriate to use to see if a particular packet is interesting or not when calls are disconnected prematurely (or when they never disconnect)?
- A) **debug dialer packet**
 - B) **show run**
 - C) **erase start**
 - D) **reload**

Quiz Answer Key

- Q1) A
Relates to: Verification of Dialer Profiles
- Q2) B
Relates to: Outbound Dialing Issues
- Q3) C
Relates to: Outbound Binding Issues
- Q4) C
Relates to: Examples
- Q5) C
Relates to: Inbound Call Issues
- Q6) A
Relates to: Disconnect Issues

Configuring Frame Relay with Traffic Shaping

Overview

This module reviews Frame Relay operation and configuration. It also covers traffic shaping. You will learn how to configure Frame Relay traffic shaping (FRTS) on a Cisco router.

Objectives

Upon completing this module, you will be able to:

- Configure Frame Relay so that two sites can exchange data
- Configure the subinterfaces on each virtual interface to solve a reachability problem caused by split horizon
- Configure FRTS
- Verify proper configuration and troubleshoot an incorrect configuration so data travels as intended across the Frame Relay link

Outline

The module contains these lessons:

- Reviewing Frame Relay
- Configuring Frame Relay
- Verifying Frame Relay Configuration
- Configuring Frame Relay Subinterfaces
- Identifying Frame Relay Traffic Shaping Features
- Configuring Frame Relay Traffic Shaping

Reviewing Frame Relay

Overview

This lesson provides an overview of Frame Relay features and operation.

Relevance

To establish a Frame Relay connection, there must be an understanding of the technology and components required, and how to configure them.

Objectives

Upon completing this lesson, you will be able to:

- Describe the basic features of Frame Relay
- Describe how Frame Relay connections operate over VCs
- Explain the function of the LMI and how it operates

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

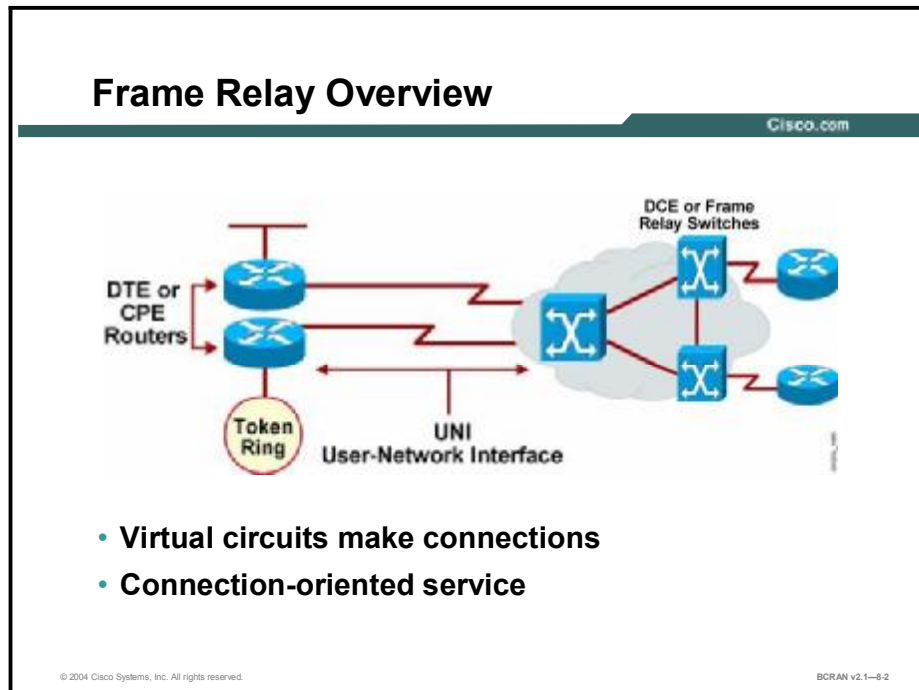
Outline

This lesson includes these topics:

- Overview
- Frame Relay Overview
- Frame Relay Operation
- Frame Relay Signaling
- Summary
- Quiz

Frame Relay Overview

This topic provides an overview of Frame Relay concepts and features. Frame Relay is an important and popular WAN connection standard.



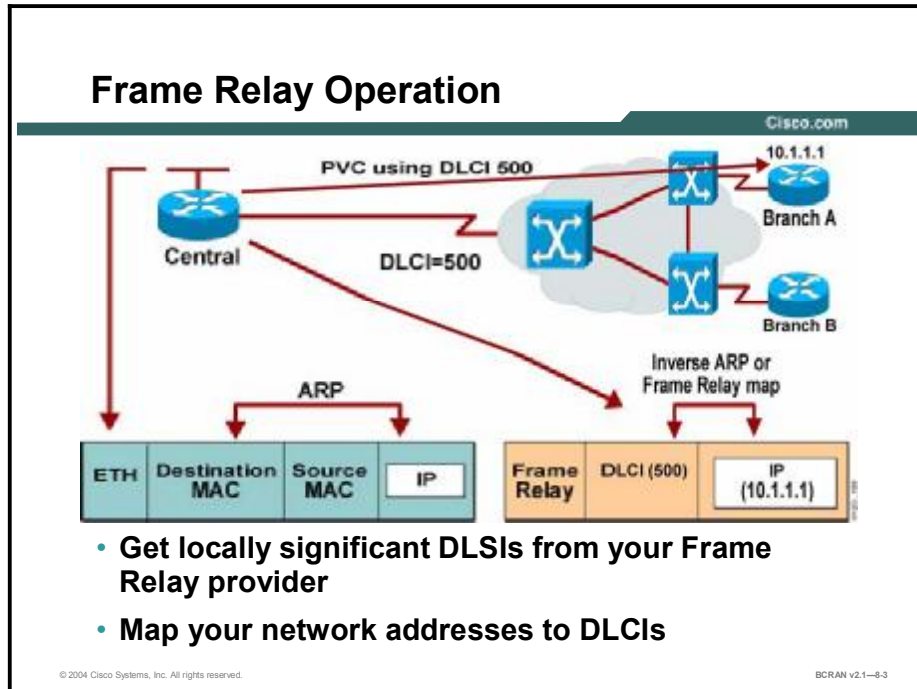
Frame Relay is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and American National Standards Institute (ANSI) standard. Frame Relay defines the process for sending data over a public data network (PDN). As a next-generation protocol to X.25, it is a connection-oriented data-link technology that is streamlined to provide high performance and efficiency. Frame Relay relies on upper-layer protocols for error correction and more dependable fiber and digital networks.

The connection between the customer and the service provider is known as the User-Network Interface (UNI). The Network-to-Network Interface (NNI) is used to describe how different Frame Relay service provider networks connect to each other. ATM is the technology commonly used within the network of the service provider to carry Frame Relay data. However, regardless of the technology that is used inside the cloud, the connection between the customer and the Frame Relay service provider is still Frame Relay.

Note that Frame Relay defines the interconnection process between the customer premises equipment (CPE, also known as DTE), such as a router, and the local access switching equipment of the service provider (known as DCE). Frame Relay does not define how the data is transmitted within the Frame Relay cloud of the service provider.

Frame Relay Operation

This topic describes the operation of Frame Relay. Frame Relay connections operate over virtual circuits (VCs). Each VC is identified by a data-link connection identifier (DLCI) that is mapped to an IP address.



Frame Relay provides a means for statistically multiplexing many logical data conversations—or VCs—over a single physical transmission link. Frame Relay assigns connection identifiers to each pair of DTE devices. The switching equipment of the service provider constructs a table that maps connection identifiers to outbound ports. When a frame is received, the switching device analyzes the connection identifier and delivers the frame to the preestablished, associated outbound port. The association of a connection identifier to an outbound port is established when the VC is created, and occurs before any data is transferred across the link.

Frame Relay networks are known as nonbroadcast multiaccess (NBMA) networks. Multiaccess means that a customer with a single connection to the Frame Relay network (cloud) has the ability to communicate with any other customer remote network. This communication remains as long as the customer is connected to the same Frame Relay network of the provider. A single connection to a Frame Relay network of the provider is likely to be much less expensive than separate leased lines to each remote site, particularly where long distances exist between sites.

The service provider must set up a VC between these sites within the Frame Relay network so that any two sites that are connected to the same Frame Relay network are able to communicate. Service providers typically charge for each VC. With a full-mesh topology, this could be expensive, depending upon the number of circuits needed. Many enterprises use hub-and-spoke topology, with VCs between a central site and each of the branch offices. In this configuration, the traffic must pass through the central site in order for two branch offices to reach each other.

The VCs can be either permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). PVCs are permanently established connections that are used when there is frequent and consistent data transfer between DTE devices across a Frame Relay network.

Based on specifications from ANSI T1.617, ITU-T Q.933 (Layer 3), and Q.922 (Layer 2), Frame Relay now supports SVCs. SVCs are temporary connections used when there is only sporadic data transfer between DTE devices across a Frame Relay network. Because they are temporary, SVC connections require call setup and termination for each connection. Cisco IOS Software Release 11.2 and later support Frame Relay SVCs. You must determine whether your carrier supports SVCs before implementing them.

Note Frame Relay SVCs are not covered in this course.

Data-Link Connection Identifier

Frame Relay uses a DLCI to identify the logical VC between the CPE and the Frame Relay switch. The Frame Relay switch maps the DLCIs between each pair of routers to create a PVC. DLCIs have local significance because the identifier references the point between the local router and the Frame Relay switch to which it is connected. Although some Frame Relay service providers use globally significant DLCIs, this is not the norm. Your Frame Relay provider sets up the DLCI numbers to be used by the routers for establishing PVCs.

Some Frame Relay providers allow their customers to choose their DLCI numbers, within a specific range, usually between 16 and 1007. DLCIs 0 through 15, and DLCIs 1008 through 1023 are reserved for special purposes: DLCI 1019 and DLCI 1020 are reserved for multicasts, DLCI 1023 is reserved for Cisco LMI, and DLCI 0 is reserved for ANSI and Q933A LMI types.

DLCI-to-Address Mappings

To pass data over the Frame Relay circuit, you must associate each local DLCI with a destination address. This association, or mapping, tells the router which DLCI to use when packets are destined for the remote address. For example, referring to the figure, an administrator would map the IP address of the destination Frame Relay interface (10.1.1.1) to DLCI 500, which is the PVC to that remote router. Any routes that point to 10.1.1.1 as the next-hop IP address will use this mapping that the PVC identified as DLCI 500, and forward packets to the remote site.

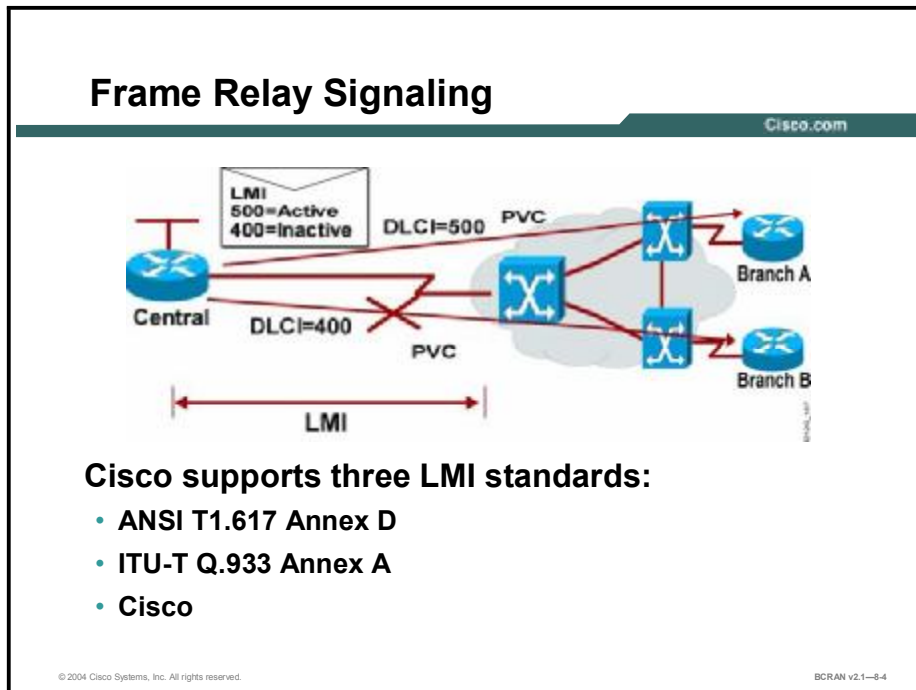
On Cisco routers, the address mapping can be either configured manually or dynamically assigned. With dynamic address mapping, Frame Relay Inverse Address Resolution Protocol (Inverse ARP) is used to dynamically discover the protocol address of the remote device associated with a given PVC. During initial link establishment, the router sends an Inverse ARP packet out each active DLCI and requests the next-hop protocol addresses from the device at the other end of the connection. The remote device responds with the protocol addresses associated with that PVC. The router then updates its mapping table and uses the information to forward packets on the correct route.

When packets are sent across the network, the intermediate switches look up the DLCI in the map table and perform the following

- If the DLCI is defined on the link, the switch forwards packets toward their destination.
- If the DLCI is not defined on the link, the switch discards the frame.

Frame Relay Signaling

This topic describes the function of the Local Management Interface (LMI) and how it operates. Routers and Frame Relay switches communicate using an LMI signaling standard.



Local Management Interface

LMI is a signaling standard between the CPE device and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices. LMI supports the following items:

- A keepalive mechanism, which verifies that data is flowing
- A multicast mechanism, which provides the DTE with its local DLCI
- Multicast addressing, which gives DLCIs global rather than local significance in Frame Relay networks
- A status mechanism, which provides an ongoing status on the DLCIs known to the switch

Although LMI is configurable, beginning in Cisco IOS software Release 11.2, the Cisco router attempts to autosense the LMI type that the Frame Relay switch is using by sending one or more full status requests to the Frame Relay switch. The Frame Relay switch responds with one or more LMI types. The router configures itself with the last LMI type received.

Cisco routers support three LMI types:

- **Cisco:** Cisco LMI type defined jointly by the “Gang of Four” (Cisco, StrataCom, Northern Telecom, and Digital Equipment Corporation)
- **ANSI:** ANSI T1.617 Annex D
- **Q933a:** ITU-T Q.933 Annex A

If LMI autosensing does not take place, then the administrator setting up a connection to a Frame Relay network must choose the appropriate LMI from the three supported types to ensure proper Frame Relay operation.

When an Inverse ARP request is made, the router updates its map table with one of three possible PVC connection states:

- **Active state:** Indicates that the connection is active and that routers can exchange data
- **Inactive state:** Indicates that the local connection to the Frame Relay switch is working, but the remote router connection to the Frame Relay switch is not working
- **Deleted state:** Indicates that no LMI is being received from the Frame Relay switch, the DLCI has been removed from the Frame Relay switch, or there is no service between the CPE router and Frame Relay switch

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Frame Relay is a standard that defines the process for sending data over a public data network.**
- **Frame Relay connections operate over virtual circuits.**
- **LMI is a signaling standard between the CPE device and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—8-5

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) The connection between the customer site and the service provider network is known as the _____.
- A) Network-to-Network Interface
 - B) user-network interface
 - C) serial interface
 - D) network to user interface
- Q2) Frame Relay provides connections between sites using a VC that is identified by its _____.
- A) IP address
 - B) network address
 - C) DLCI
 - D) PVC
- Q3) Which DLCI does the Frame Relay LMI type “Cisco” use for communication?
- A) 15
 - B) 1023
 - C) 0
 - D) 16

Quiz Answer Key

Q1) B

Relates to: Frame Relay Overview

Q2) C

Relates to: Frame Relay Operation

Q3) B

Relates to: Frame Relay Signaling

Configuring Frame Relay

Overview

This lesson illustrates how to configure Frame Relay on a serial interface.

Relevance

It is important to know how to configure a Frame Relay connection because it is the most popular WAN connectivity solution. This lesson covers the concepts and commands for configuring Frame Relay.

Objectives

Upon completing this lesson, you will be able to:

- List the steps and commands that are required to configure a basic Frame Relay connection
- Explain how DLCI numbers are dynamically mapped to IP addresses
- Describe how DLCI numbers are statically mapped to IP addresses
- Identify the significance of DLCI numbers
- Explain the function of a hub-and-spoke topology
- List the commands that are required to configure a hub-and-spoke topology
- Explain why static DLCI maps should be configured to reach the hub site and the other spoke sites
- Configure a Frame Relay map

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

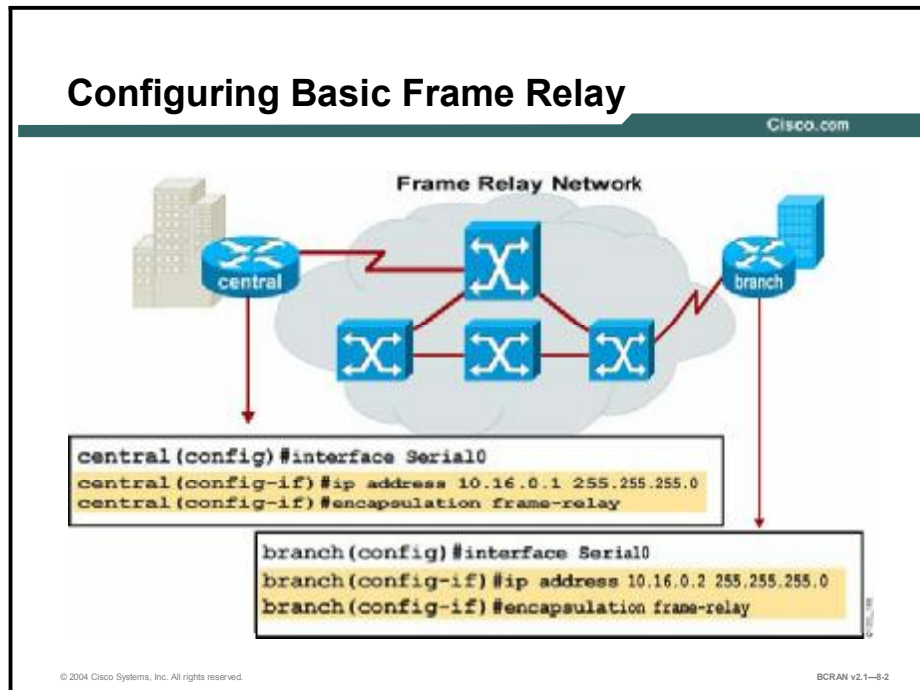
Outline

This lesson includes these topics:

- Overview
- Configuration of Basic Frame Relay
- Dynamic Address Mapping
- Configuration of Static Address Mapping
- Different DLCIs at the Remote Routers
- Hub-and-Spoke Topology
- Spoke Router
- Summary
- Quiz

Configuration of Basic Frame Relay

This topic describes the steps and commands that are required to configure a basic Frame Relay connection.



There are five steps required to configure a basic Frame Relay connection:

- Step 1** Select the interface and enter interface configuration mode.
- Step 2** Configure a network-layer address, for example, an IP address.
- Step 3** Select the encapsulation type used to encapsulate data traffic end-to-end using the following command:

```
encapsulation frame-relay [cisco | ietf]
```

The default argument is **cisco**. It is the recommended setting if connecting to another Cisco router. Select **ietf** if connecting to a router from another vendor.

- Step 4** If using Cisco IOS Software Release 11.1 or earlier, specify the LMI type used by the Frame Relay switch using this command:

```
frame-relay lmi-type {ansi | cisco | q933a}
```

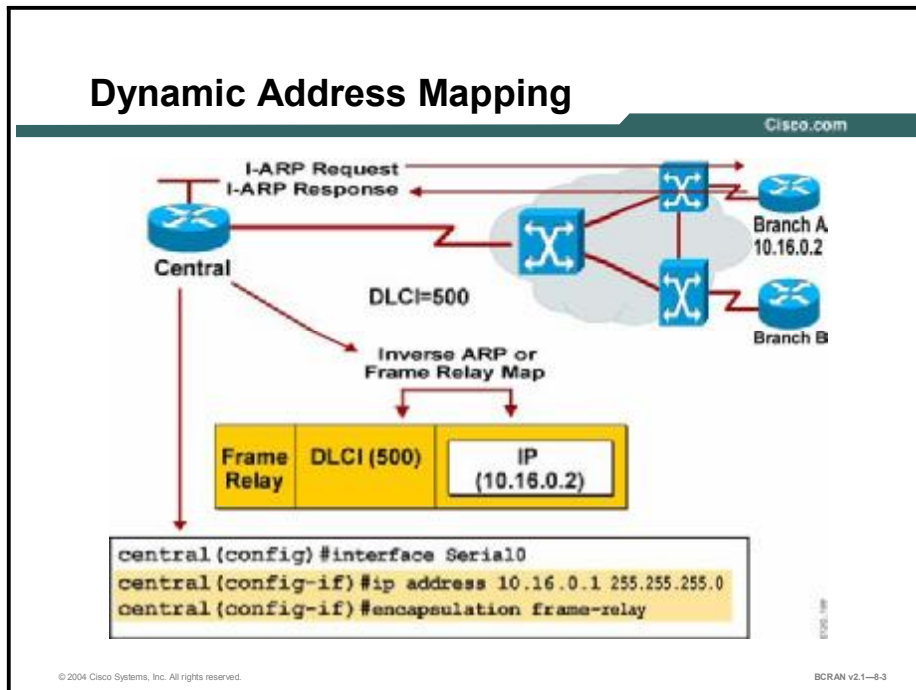
With Cisco IOS Software Release 11.2 or later, the LMI type is autosensed and manual configuration is required. Otherwise, the customer can obtain the LMI type from their Frame Relay service provider and manually configure it. The default LMI type is **cisco**.

- Step 5** Configure address mapping.

On Cisco routers, the address mapping of a local DLCI to a remote IP address can be configured manually with static address mapping, or with dynamic address mapping. In the above example, the address mapping is dynamic.

Dynamic Address Mapping

This topic describes how DLCI numbers are dynamically mapped to IP addresses. The DLCI to IP address mapping can be done dynamically or statically.



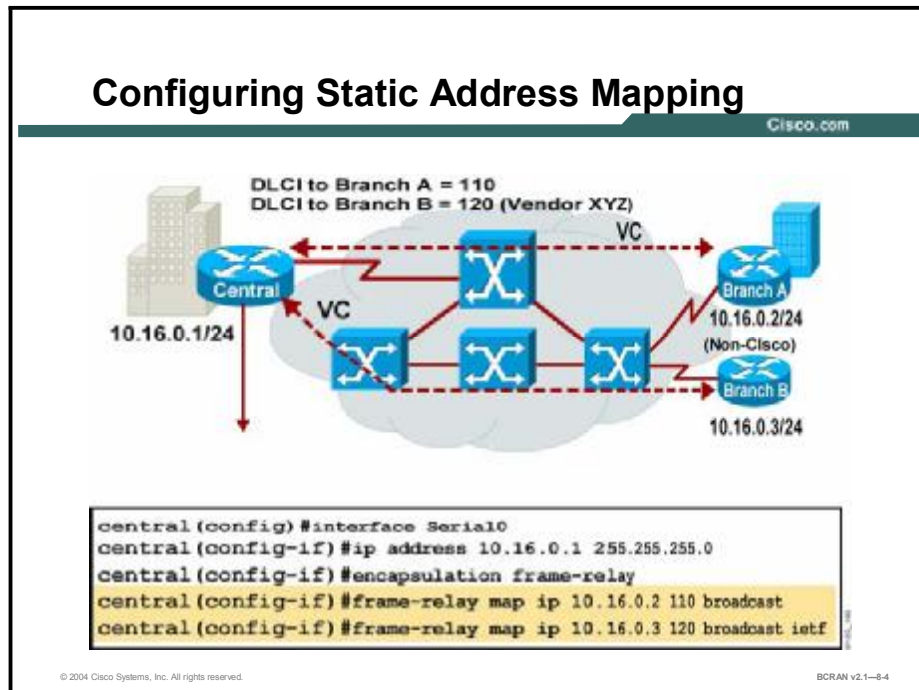
If you use dynamic address mapping, Frame Relay Inverse ARP dynamically associates a given DLCI with the next-hop protocol addresses for that connection. The router then updates its mapping table and uses the information in the table to route outgoing traffic to the appropriate PVC. Frame Relay Inverse ARP, and therefore dynamic addressing, is enabled by default for all protocols that are enabled on a physical interface. No additional commands are necessary.

If Inverse ARP has been previously disabled on a Frame Relay interface, it can be reenabled using the **frame-relay inverse-arp** command in interface configuration mode.

Note LMI must be functioning on an interface to use Frame Relay Inverse ARP because LMI is used to determine the PVCs to map.

Configuration of Static Address Mapping

This topic describes how DLCI numbers are statically mapped to IP addresses. The DLCI to IP address mapping can be done dynamically or statically.



Whether the mapping of a DLCI to a remote IP address happens dynamically or statically, the DLCI that is used does not have to be the same number at both ends of the PVC.

If you use static address mapping, you must use the **frame-relay map** command to statistically map destination network protocol addresses to a designated DLCI. In this figure, the central site router is configured with static maps to both branch routers, Branch A and Branch B.

The static address mapping command syntax is as follows:

```
frame-relay map protocol protocol-address dcli [broadcast]
[ietf | cisco]
```

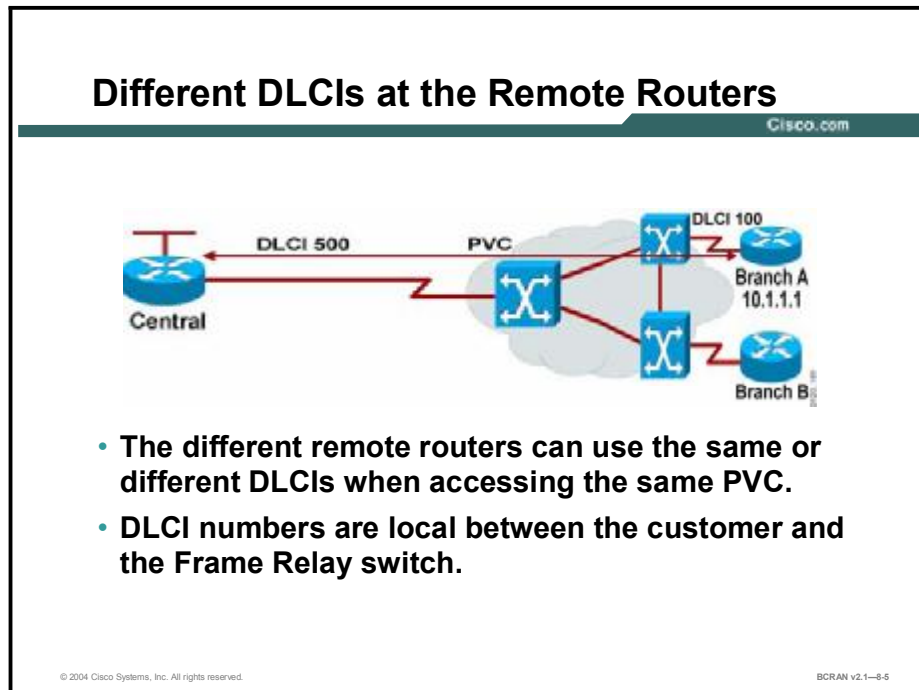
The following table describes the **frame-relay map** command syntax.

frame-relay map Command

Command	Description
<i>protocol</i>	Selects the protocol type. Commonly used protocols are dls , ip , and ipx .
<i>protocol-address</i>	Specifies the destination protocol address.
<i>dci</i>	Specifies the DLCI number used to connect to the specified protocol address on the interface.
broadcast	(Optional) Specifies that broadcasts should be forwarded when multicast is not enabled.
ietf	(Optional) Enables the Internet Engineering Task Force (IETF) encapsulation.
cisco	(Optional) Enables the Cisco encapsulation.

Different DLCIs at the Remote Routers

This topic describes the significance of DLCI numbers. DLCI numbers are locally significant only and do not have to be the same at each end of the PVC.



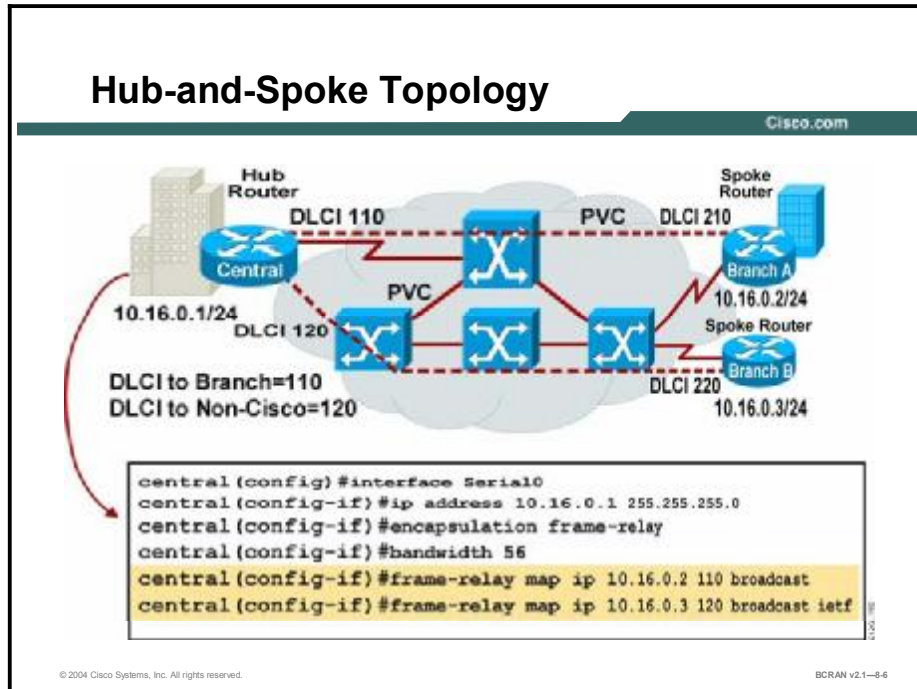
Whether the mapping of a DLCI to a remote IP address happens dynamically or statically, the DLCI that is used does not have to be the same number at both ends of the PVC. In this example, the central router is using DLCI 500 and the Branch A router is using DLCI 100. Each router is communicating with the other router using a different DLCI over the same PVC.

Locally significant DLCIs mean that the DLCI number has meaning between the individual customer and the Frame Relay switch only. Different customers may use the same DLCI number to communicate with different switches within the same Frame Relay network.

Although not a requirement, Frame Relay providers usually assign the same DLCI number to VCs that connect to a common site. For example, all remote sites that have a Frame Relay connection to the headquarters site may be assigned DLCI 100 for this hub connection. Network topology diagrams often display this common DLCI assignment at the hub location. This DLCI assignment represents the DLCI that remote devices use to connect to that site, even though the DLCI value is actually assigned to each of the remote locations and not to the hub.

Hub-and-Spoke Topology

This topic describes the function of a hub-and-spoke topology and the commands that are required to configure it. Frame Relay is most commonly configured in a hub-and-spoke topology.



The topology shown is known as a Frame Relay hub-and-spoke topology. The central site is acting as the hub and the Branch A and Branch B routers are acting as the spokes. Each of the spoke routers is connected only to the hub. When two spoke routers need to communicate with each other, the traffic is sent via the hub router. The advantage to this type of topology is that there does not have to be a full mesh of PVCs between all routers. This will provide a cost savings on the number of PVCs needed.

The configurations for the hub-and-spoke routers in the example would be as follows:

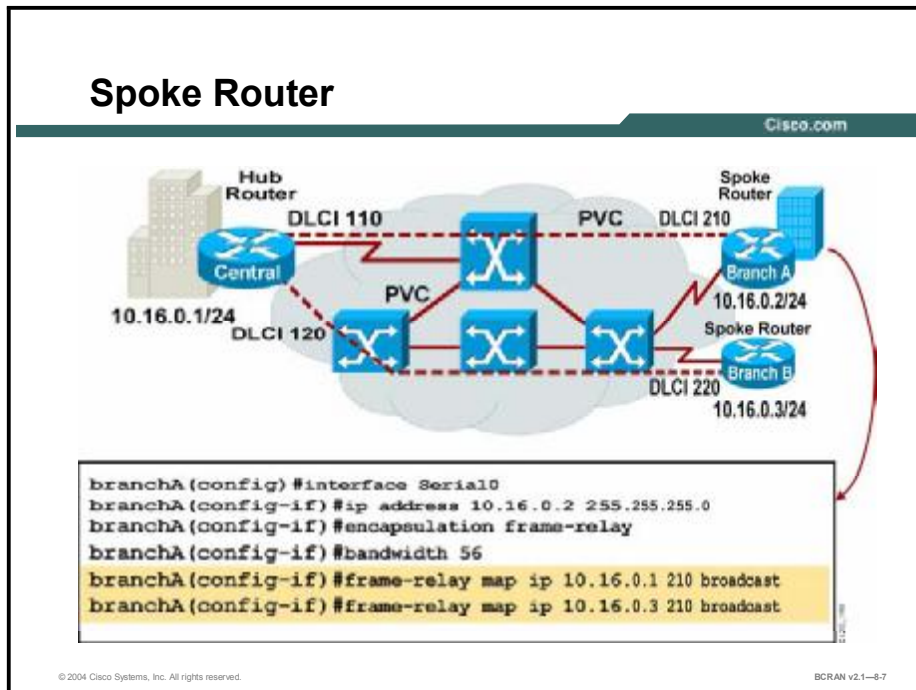
```
central (config)#interface serial1
central (config-if)#ip address 10.16.0.1 255.255.255.0
central (config-if)#encapsulation frame-relay
centralA (config-if)#frame-relay map ip 10.16.0.2 110 broadcast
centralA (config-if)#frame-relay map ip 10.16.0.3 120 broadcast ietf
```

```
branchA (config)#interface serial0
branchA (config-if)#ip address 10.16.0.2 255.255.255.0
branchA (config-if)#encapsulation frame-relay
branchA (config-if)#frame-relay map ip 10.16.0.1 210 broadcast
branchA (config-if)#frame-relay map ip 10.16.0.3 210 broadcast
```

```
branchB(config)#interface serial0
branchB(config-if)#ip address 10.16.0.3 255.255.255.0
branchB(config-if)#encapsulation frame-relay
branchB(config-if)#frame-relay map ip 10.16.0.1 220 broadcast ietf
branchB(config-if)#frame-relay map ip 10.16.0.2 220 broadcast ietf
```


Spoke Router

This topic describes how static DLCI maps should be configured to reach the hub site and the other spoke sites. Static DLCI maps are configured with the **frame-relay map** command.



In this example, both branch routers are using static mapping to communicate with the central office (CO) router and the other branch office router. Notice that the branch routers use the same DLCI to communicate with both the CO and the other branch office router. The only difference is the remote IP address.

The branch routers can be configured using Inverse ARP to the central site and a static map to the other branch office, both using the same DLCI. This arrangement works until the branch office router is rebooted. After the router reboots, the static map disables Inverse ARP for that DLCI. This situation means that the branch router will not be able to reach either the central site or the other branch office. Because there is no dynamic mapping to the central site, there is no way to reach the other branch office via the hub router, even though a static map is configured. When configuring the branch office routers, static map addresses should be used to reach both the central site and the other branch router, as shown in the example.

Note None of these example configurations take into account the routing updates and split-horizon issues with distance-vector routing protocols. This will be discussed further along in this module.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **There are five steps required to configure a basic Frame Relay connection.**
- **The DLCI to IP Address mapping can be done dynamically or statically.**
- **Locally significant DLCIs have meaning between the customer and the Frame Relay switch only.**
- **Frame Relay is commonly configured in a hub-and-spoke topology.**
- **Static DLCI maps are configured with the frame-relay map command.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8.8

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which Frame Relay LMI type is the default on Cisco routers?
- A) ANSI
 - B) IETF
 - C) Cisco
 - D) Q.933I
- Q2) Which function does Inverse ARP perform?
- A) multicast support
 - B) periodic keepalive transmission
 - C) static mappings of DLCIs to local Layer 3 addresses
 - D) dynamic mappings of DLCIs to remote Layer 3 addresses
- Q3) The **frame-relay map** command is used to create a static map between an IP address and a DLCI.
- A) true
 - B) false
- Q4) Locally significant DLCIs mean that the DLCI number has meaning between the individual customer and the Frame Relay switch only.
- A) true
 - B) false
- Q5) What is an advantage of designing a hub-and-spoke Frame Relay network?
- A) full redundancy
 - B) requires subinterfaces
 - C) cost effective
 - D) partial redundancy
- Q6) Which type of encapsulation should be used when connecting equipment from another vendor to a Cisco Frame Relay network?
- A) Cisco
 - B) IETF
 - C) ANSI
 - D) Q.933A

Quiz Answer Key

- Q1) C
Relates to: Configuration of Basic Frame Relay
- Q2) D
Relates to: Dynamic Address Mapping
- Q3) A
Relates to: Configuration of Static Address Mapping
- Q4) A
Relates to: Different DLCIs at the Remote Routers
- Q5) C
Relates to: Hub-and-Spoke Topology
- Q6) B
Relates to: Spoke Router

Verifying Frame Relay Configuration

Overview

This lesson highlights Cisco IOS commands that help verify proper Frame Relay configuration.

Relevance

Implementing and troubleshooting Frame Relay is a necessary skill for network engineers. This lesson provides an overview of various commands to verify Frame Relay connectivity.

Objectives

Upon completing this lesson, you will be able to:

- List commands that are useful when implementing and troubleshooting a Frame Relay connection
- Identify key fields for each command

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Verification of Frame Relay Operation
- Summary
- Quiz

Verification of Frame Relay Operation

This topic describes the Frame Relay monitoring commands and highlights key fields for each command. Various commands are required to monitor and troubleshoot a Frame Relay connection.

Verifying Frame Relay Operation

Cisco.com

```
central@>show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.16.0.1/24
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent 96, LMI stat recvd 90, LMI upd recvd 0, DLE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 20/0, interface broadcasts 0
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  <Output Omitted>
```

- Displays line, protocol, DLCI, and LMI information

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-8.2

After you configure Frame Relay, you can verify that the connections are active using the available **show** commands. The **show interface** command displays information regarding the encapsulation and Layer 1 and Layer 2 status. It also displays Frame Relay LMI information for the interface, including the number of LMI messages exchanged, LMI type, and the DLCI that is used by LMI.

Verifying Frame Relay Operation (Cont.)

Cisco.com

```
central#show frame-relay pvc 110
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 37          output pkts 25          in bytes 8337
  out bytes 5048         dropped pkts 0          in FECN pkts 0
  in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
  in DE pkts 0          out DE pkts 0          out DE pkts 0
  out hcart pkts 14     out hcart bytes 3948
  pvc create time 00:16:33, last time pvc status changed 00:12:51
central#
```

- Displays PVC traffic statistics

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8.3

The **show frame-relay pvc** command displays the status of each configured connection as well as traffic statistics. This command is also useful for viewing the number of backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) packets received by the router. The PVC STATUS can be active, inactive, or deleted.

If you enter the **show frame-relay pvc** command without any additional arguments, you will see the status of all the PVCs configured on the router. If you specify the PVC, you will see the status for that PVC only. In the figure, the **show frame-relay pvc 110** command displays the status of PVC 110 only.

Verifying Frame Relay Operation (Cont.)

Cisco.com

```
central#show frame-relay map
Serial0 (up): ip 10.16.0.2 dlci 110(0x6E,0x18E0), static,
              broadcast,
              CISCO, status defined, active
Serial0 (up): ip 10.16.0.3 dlci 120(0x78,0x1C80), dynamic,
              broadcast,, status defined, active
central#
```

- Displays the route maps, either statistic or dynamic.
- In this example DLCI 110 was configured statistically while DLCI 120 was learned dynamically.

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8.4

Use the **show frame-relay map** command to display the current DLCI protocol address map entries and information about the connections.

The **show frame-relay map** command will display various information including the remote protocol address, the DLCI number, dynamic or static address mapping, and the state of the PVC.

In the example, DLCI 120 on interface Serial0 maps to remote IP address 10.16.0.3; the mapping was dynamically discovered using Inverse ARP.

Verifying Frame Relay Operation (Cont.)

Cisco.com

```
central#show frame-relay lmi
LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = ANSI
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 113100 Num Status msgs Rcvd 113100
Num Update Status Rcvd 0 Num Status Timeouts 0
central#
```

- Displays LMI information

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8.5

The **show frame-relay lmi** command displays LMI traffic statistics. For example, the command shows the number of status messages exchanged between the local router and the Frame Relay switch, including the number of invalid LMI packets by type.

Verifying Frame Relay Operation (Cont.)

Cisco.com

```
central#debug frame-relay lmi
Serial3/1(in): Status, myseq 214
RT IE 1, length 1, type 0
KA IE 3, length 2, yourseq 214, myseq 214
FVC IE 0x7, length 0x6, dlci 130, status 0x2, bw 0
Serial3/1(out): StEnq, myseq 215, yourseen 214, DTE up
datagramstart = 0x1959DF4, datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 01 03 02 D7 D6

Serial3/1(in): Status, myseq 215
RT IE 1, length 1, type 1
KA IE 3, length 2, yourseq 215, myseq 215
Serial3/1(out): StEnq, myseq 216, yourseen 215, DTE up
datagramstart = 0x1959DF4, datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 01 03 02 D8 D7
```

- Displays LMI debug information

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8-6

The **debug frame-relay lmi** command allows you to verify and troubleshoot the Frame Relay connection.

The “(out)” status field is an LMI status inquiry sent by the router. The “(in)” status is a reply by the Frame Relay switch.

The “type 1” field is a keepalive message sent by the router to the Frame Relay switch approximately every 10 seconds. The purpose of the keepalive message is to verify that the Frame Relay switch is still active.

The “type 0” field represents a full LMI status message sent every 60 seconds. The “dlci 130, status 0x2” field indicates that the status of DLCI 130 is active. The most common values of the status field are as follows:

- **0x0:** Added/inactive. The switch has this DLCI programmed but for some reason (such as the other end of this PVC is down) it is not usable.
- **0x2:** Added/active. The Frame Relay switch has the DLCI and everything is operational. You can start sending traffic with this DLCI in the header.
- **0x4:** Deleted. The Frame Relay switch does not have this DLCI programmed for the router. However, it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the telco in the Frame Relay cloud.

Verifying Frame Relay Operation (Cont.)

Cisco.com

```
central#show frame map
Serial0 (up): ip 10.16.0.2 dlci 110(0x6E,0x18E0), dynamic,
              broadcast,, status defined, active
Serial0 (up): ip 10.16.0.3 dlci 120(0x78,0x1C80), dynamic,
              broadcast,, status defined, active
central#
central#clear frame-relay-inarp
central#show frame-relay map
central#
```

- Clears dynamically created Frame Relay maps
- Disables Inverse ARP

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8.7

To clear dynamically created Frame Relay maps, which are created by the use of Inverse ARP, use the **clear frame-relay-inarp** privileged EXEC command. This command disables Inverse ARP for the router.

Note Do not use this command in a production network. Doing so will cause user traffic to be stopped because of the lack of a Layer 2 DLCI mapped to a Layer 3 protocol address. To re-enable Inverse ARP, use the interface command **frame-relay inverse-arp**.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The show frame-relay pvc command displays the status of each configured connection, as well as traffic statistics.**
- **The show frame-relay map command displays the DLCI-protocol address map entries, as well as information about the connection.**
- **The show frame-relay lmi command displays LMI traffic statistics.**
- **The debug frame-relay lmi command allows you to verify and troubleshoot the Frame Relay connection.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—8-8

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which information from a **show interfaces** display indicates that your Frame Relay connection is operating correctly?
- A) Bandwidth is 128 kbps.
 - B) Hardware is in sync mode.
 - C) MTU size is 1500 bytes or more.
 - D) LMI enq sent and stat recvd are non-zero.

Quiz Answer Key

Q1) D

Relates to: Verification of Frame Relay Operation

Configuring Frame Relay Subinterfaces

Overview

This lesson provides a review of Frame Relay subinterfaces, and explains why and when you would use subinterfaces.

Relevance

A Frame Relay network can be connected in a star, full-mesh, or partial-mesh topology. Depending on the topology configured, there may be some reachability issues with routing updates because of the split horizon rule. Subinterfaces can be configured to resolve this issue.

Objectives

Upon completing this lesson, you will be able to:

- Explain the issues that can occur with routing protocols in a multipoint Frame Relay configuration
- Explain the issues that can occur with distance-vector routing protocols and the split horizon rule in a multipoint Frame Relay configuration
- Explain why it is not recommended to disable split horizon in a multipoint Frame Relay configuration
- Identify the reasons why subinterfaces can be used to help solve issues with distance-vector routing protocols and the split horizon rule in a multipoint Frame Relay configuration
- Describe how point-to-point subinterfaces can solve reachability issues
- Explain how multipoint subinterfaces can solve reachability issues
- List the steps and commands required to configure a subinterface on a basic Frame Relay connection

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

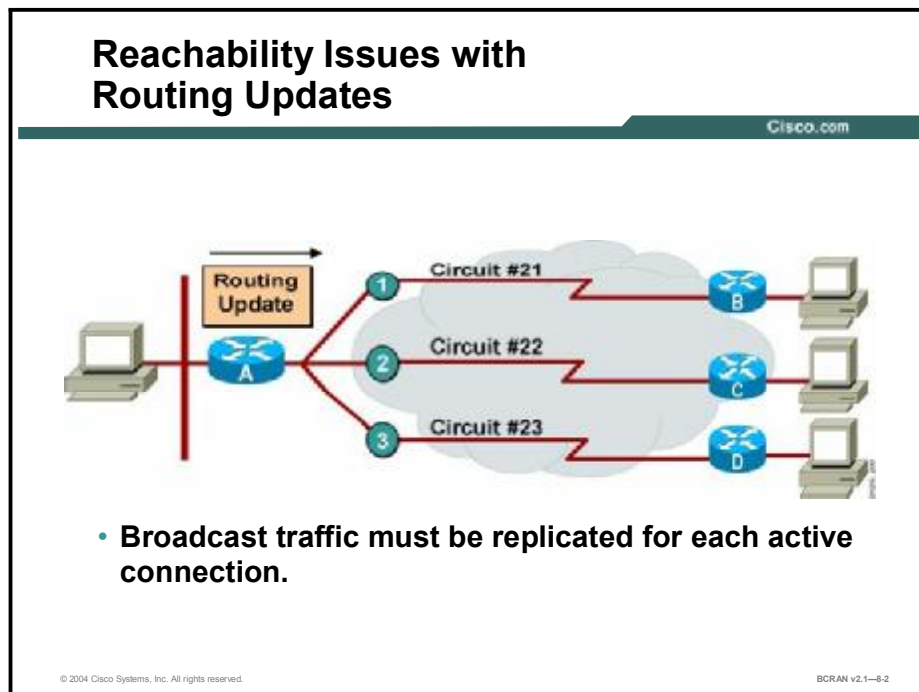
Outline

This lesson includes these topics:

- Overview
- Reachability Issues with Routing Updates
- Resolution of Reachability Issues
- Subinterface Usages
- Point-to-Point Subinterfaces
- Multipoint Subinterfaces
- Configuration of Subinterfaces
- Subinterface Configuration Example
- Summary
- Quiz

Reachability Issues with Routing Updates

This topic describes reachability issues with routing updates in a multipoint Frame Relay configuration. Multipoint Frame Relay connections are prone to reachability issues.



There is a major issue with a router that supports multipoint connections over a single interface. Because many DLCIs terminate in a single router, that router must replicate routing updates and service advertising updates on each DLCI to the remote routers. The updates can consume access-link bandwidth and cause significant latency variations in user traffic. The updates can also consume interface buffers and lead to higher packet-rate loss for both the user data and routing updates.

The amount of broadcast traffic and the number of VCs terminating at each router should be evaluated during the design phase of a Frame Relay network. Overhead traffic, such as routing updates, can impact the delivery of critical user data, especially when the delivery path contains low-bandwidth (56 kbps) links.

Resolution of Reachability Issues

This topic describes the problems that are associated with disabling split horizon in a multipoint Frame Relay configuration. Disabling split horizon could be used to resolve distance-vector protocols and split horizon rule reachability issues.

Resolving Reachability Issues

Cisco.com

The diagram shows a 'Logical Interface' box on the left containing three subinterfaces: S0.1, S0.2, and S0.3. These are connected to a 'Physical Interface' labeled 'S0'. From the physical interface, three lines branch out to three separate routers, each representing a 'Subnet' (Subnet A, Subnet B, and Subnet C). The routers are depicted as blue icons with a white 'X' on top.

- **Split horizon can cause problems in NBMA environments.**
- **A single physical interface simulates multiple logical interfaces.**
- **Subinterfaces can resolve split horizon issues.**

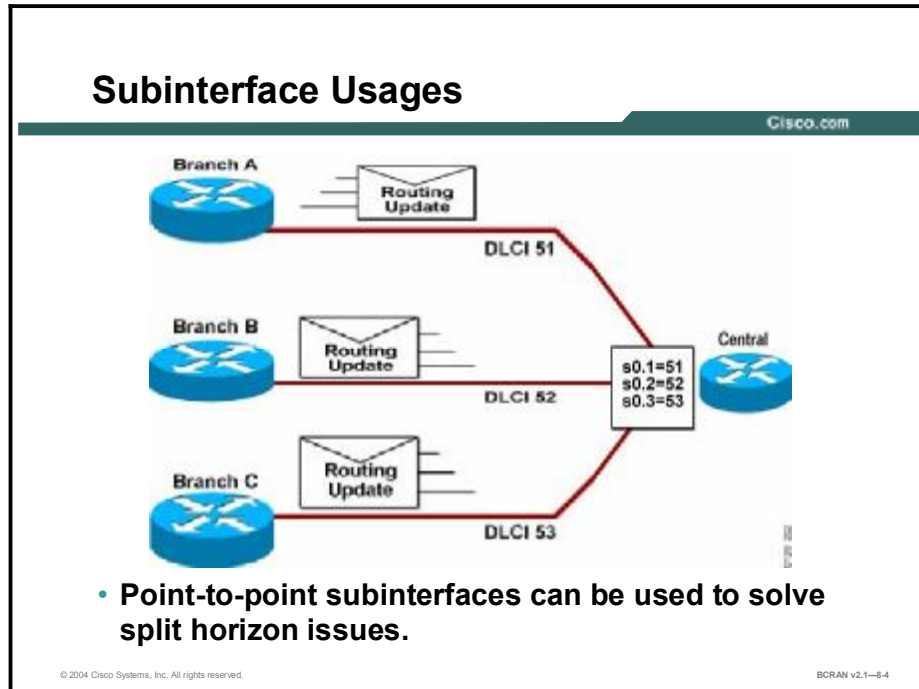
© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-3

The simplest answer to resolving the reachability issues brought on by split horizon may seem to be to turn off split horizon. Two problems exist with this solution. First, only IP allows you to disable split horizon. Second, disabling split horizon increases the chances of routing loops in your network.

Note Split horizon is disabled by default for the IP protocol on Frame Relay interfaces. Enhanced Interior Gateway Routing Protocol (EIGRP) is an exception. EIGRP requires IP split horizon to be manually disabled.

Subinterface Usages

This topic describes subinterfaces to help solve issues with distance-vector routing protocols and the split horizon rule in a multipoint Frame Relay configuration. Subinterfaces are logical subdivisions of a physical interface.



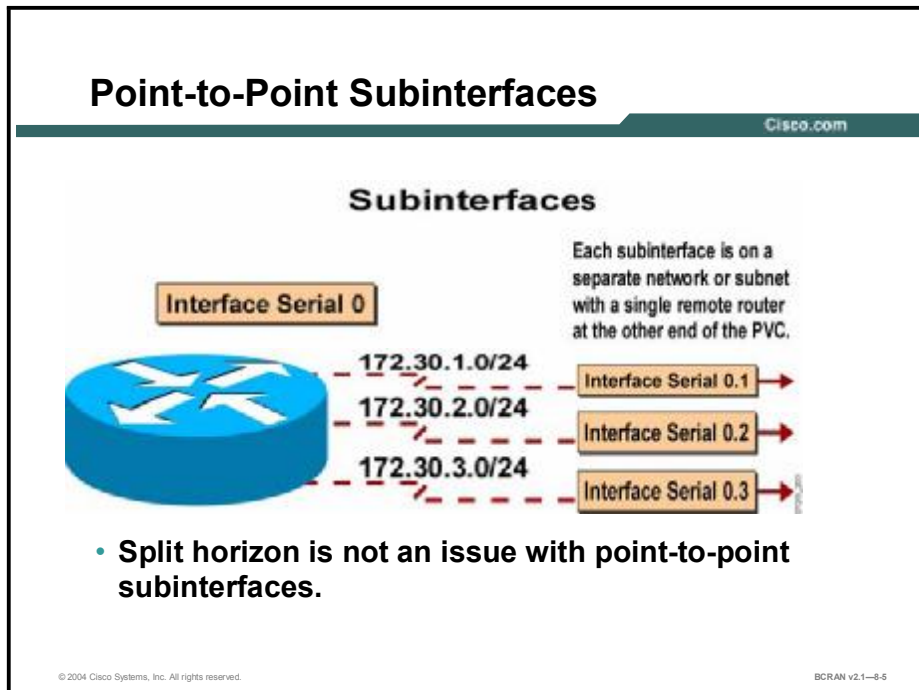
To enable the forwarding of broadcast routing updates in a Frame Relay network, you can configure the router with logically assigned interfaces called subinterfaces. Subinterfaces are logical subdivisions of a physical interface.

You can configure subinterfaces to support these connection types:

- Point-to-point
- Multipoint

Point-to-Point Subinterfaces

This topic describes how point-to-point subinterfaces can solve reachability issues in a Frame Relay configuration. Subinterfaces can be configured either as point-to-point or multipoint.

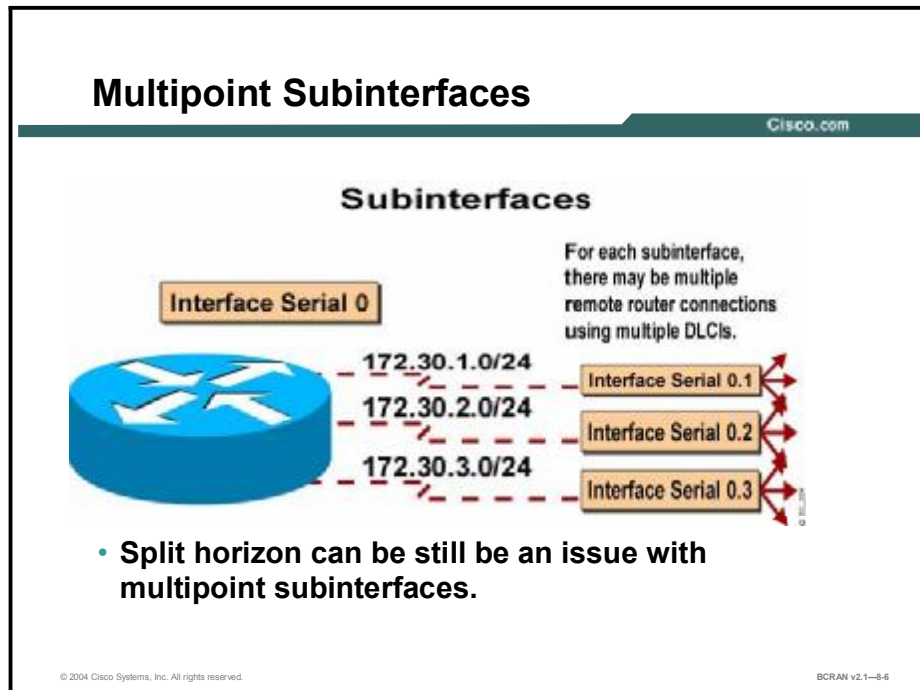


In point-to-point subinterface configurations, a single subinterface is used to establish one PVC connection to another physical or subinterface on a remote router. In this case, the subinterfaces would be in the same subnet and each subinterface would have a single DLCI. Each point-to-point connection is its own subnet.

In split horizon routing environments, routing updates received on one point-to-point subinterface can be sent out another point-to-point subinterface. Each VC can be configured as a point-to-point connection, which allows the subinterface to act like a leased line. This is because each point-to-point subinterface is treated as a separate physical interface.

Multipoint Subinterfaces

This topic describes how multipoint subinterfaces can solve reachability issues in a Frame Relay configuration.



In multipoint subinterface configurations, a single subinterface is used to establish multiple PVC connections to multiple physical or subinterfaces on remote routers. In this case, all the participating interfaces would be in the same subnet and each interface would have its own local DLCI. In this environment, because the subinterface is acting like a regular NBMA Frame Relay network, broadcast traffic is subject to the split horizon rule.

Cisco routers can be configured to simultaneously support both point-to-point and multipoint subinterfaces. Each subinterface is configured as one or the other, not both. This permits a company to configure individual Frame Relay connections as needed, and to provide a more flexible transition from one configuration to another.

Configuration of Subinterfaces

There are a total of six steps that are required to configure a subinterface on a basic Frame Relay connection. This topic describes the first four steps.

Configuration of Subinterfaces

Cisco.com

- **Point-to-point**
 - Subinterfaces act as leased line
 - Each point-to-point connection requires its own subnet
 - Good for star or partial-mesh topologies
- **Multipoint**
 - Subinterfaces act as default NBMA network
 - Can save subnets because uses single subnet
 - Good for full-mesh topology

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-8-7

To configure subinterfaces on a physical interface, perform these steps:

- Step 1** Select the interface upon which you want to create subinterfaces, and enter the interface configuration mode.
- Step 2** Remove any network-layer address assigned to the physical interface. If the physical interface has an address, frames will not be received by the local subinterfaces.
- Step 3** Configure Frame Relay encapsulation, as discussed in the Configuring Frame Relay lesson in this module.
- Step 4** Select the subinterface you want to configure, as follows:

```
interface serial number.subinterface-number {multipoint |  
point-to-point}
```

The following table lists the command and parameters to use when setting up a subinterface on a serial link.

interface serial Command Parameters

Command	Description
<i>subinterface-number</i>	Subinterface number. The interface number that precedes the period (.) must match the interface number to which this subinterface belongs. The number of subinterfaces possible on one interface is interface description block (IDB)-dependent. The IDB is a set of data structures that provide hardware and software views of network interfaces.
multipoint	Select if you want the router to forward the broadcasts and routing updates that it receives. Select this option if you are routing IP and you want all routers in the same subnet.
point-to-point	Select if you do not want the router to forward broadcasts or routing updates and if you want each pair of point-to-point routers to have its own subnet.

Subinterface Configuration Example

This topic describes the last two steps and commands that are required to configure a subinterface on a basic Frame Relay connection.

Subinterface Configuration Example

Cisco.com

```
central (config) #<Output Omitted>
central (config-if) #interface Serial0
central (config-if) #no ip address
central (config-if) #encapsulation frame-relay
?
central (config) #interface Serial0.110 point-to-point
central (config-subif) #description PVC to BranchX
central (config-subif) #ip address 10.17.0.1 255.255.255.0
central (config-subif) #frame-relay interface-dlci 110
?
central (config) #interface Serial0.120 point-to-point
central (config-subif) #description PVC to BranchY
central (config-subif) #ip address 10.18.0.1 255.255.255.0
central (config-subif) #frame-relay interface-dlci 120
?
<Output Omitted>
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8.8

- Step 5** Configure a network-layer address on the subinterface. If the subinterface is point-to-point and you are using IP, you can configure an unnumbered subinterface as follows:

ip unnumbered interface

The *interface* parameter specifies a router interface with an IP address assigned. The subinterface associates itself with this interface for address purposes. If you use this command, it is recommended that the interface be a loopback interface because the Frame Relay link will not work if this command is pointing to an interface that is not fully operational. The loopback interface is a stable interface that is accessible from all other interfaces.

- Step 6** If you configured the subinterface as point-to-point, you must configure the local DLCI for the subinterface to distinguish it from the physical interface as follows:

frame-relay interface-dlci dlci-number

The *dlci-number* parameter defines the local DLCI number being linked to the subinterface. This is the only way to link an LMI-derived PVC to a subinterface, because LMI does not know about subinterfaces.

This command is required for all point-to-point subinterfaces. It is also required for multipoint subinterfaces for which dynamic addressing is enabled through the use of Inverse ARP. It is not required for multipoint subinterfaces configured with static address mappings (those using the **frame-relay map** command).

Remember, within the Frame Relay network, the service provider handles the actual mapping of the DLCIs between the routers.

Note If you defined a subinterface for point-to-point communication, you cannot reassign the same subinterface number to be used for multipoint communication without first rebooting the router. Instead, you can avoid using that subinterface number and use a different subinterface number.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Disabling split horizon should not be used to resolve distance-vector protocols and split horizon rule reachability issues.**
- **In point-to-point subinterface configurations, a single subinterface is used to establish one PVC connection to another physical connection or subinterface on a remote router.**
- **In multipoint subinterface configurations, a single subinterface is used to establish multiple PVC connections to multiple physical connection or subinterfaces on remote routers.**
- **There are six steps required to configure a subinterface on a basic Frame Relay connection.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—8-9

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Turning off split horizon on an NBMA environment increases the chance of creating routing loops.
- A) true
 - B) false
- Q2) What is the recommended solution to avoid split horizon issues?
- A) Do not use a distance-vector protocol over Frame Relay.
 - B) Enable broadcast on the serial interface.
 - C) Configure subinterfaces.
 - D) Turn off split horizon.
- Q3) Which type of Frame Relay connection will eliminate broadcast and split horizon issues?
- A) multipoint subinterface
 - B) point-to-point subinterface
 - C) multipoint
 - D) point-to-point
- Q4) What must be configured on the hub router to allow one subnet to be used for all router interfaces participating in the Frame Relay circuit?
- A) multipoint subinterfaces
 - B) point-to-point subinterfaces
 - C) IP unnumbered with multipoint subinterfaces
- Q5) To configure Frame Relay subinterfaces, you must specify which parameter?
- A) ARP
 - B) traffic rate
 - C) map class
 - D) traffic shaping
 - E) multipoint or point-to-point
- Q6) The command **frame-relay interface-dlci** should be used only on subinterfaces.
- A) true
 - B) false

Quiz Answer Key

- Q1) A
Relates to: Reachability Issues with Routing Updates
- Q2) C
Relates to: Resolution of Reachability Issues
- Q3) B
Relates to: Point-to-Point Subinterfaces
- Q4) A
Relates to: Multipoint Subinterfaces
- Q5) E
Relates to: Configuration of Subinterfaces
- Q6) A
Relates to: Subinterface Configuration Example

Identifying Frame Relay Traffic Shaping Features

Overview

This lesson describes the Frame Relay traffic shaping (FRTS) features that are available in Cisco IOS software and explains why you use FRTS.

Relevance

A Frame Relay switch cannot determine which packets take precedence, and therefore which packets should be dropped when congestion occurs. Traffic shaping is also critical for real-time traffic such as Voice over Frame Relay (VoFR). Failure to do so can result in bottlenecks and packet loss. Traffic shaping controls the traffic going out an interface so that it can match its flow to the speed of the remote target interface, ensuring that the traffic conforms to policies for which it was contracted.

Objectives

Upon completing this lesson, you will be able to:

- List the strategies for implementing FRTS
- Define the terminology associated with FRTS
- Identify the purpose of FRTS

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

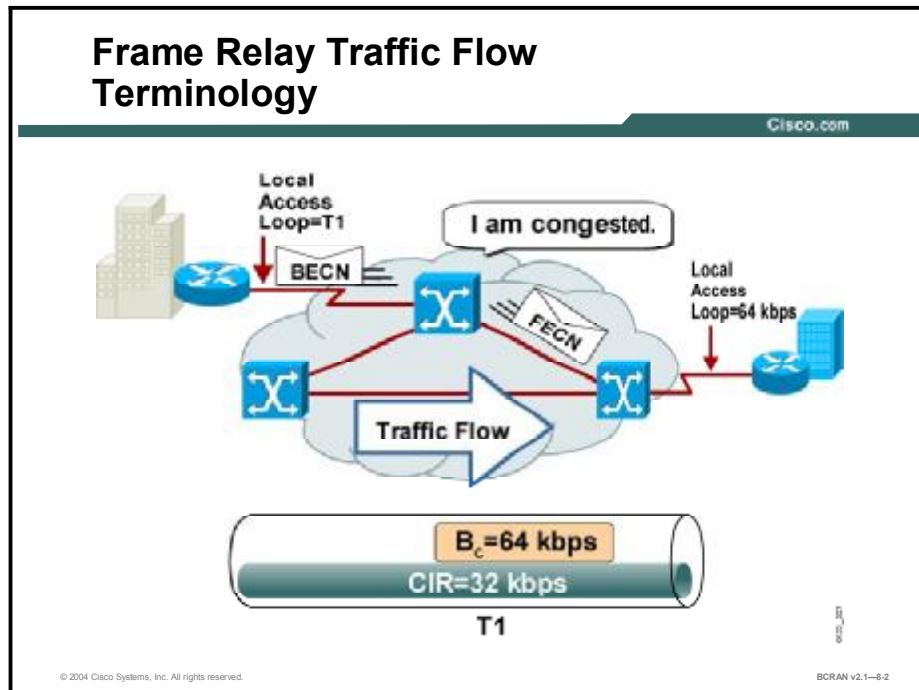
Outline

This lesson includes these topics:

- Overview
- Frame Relay Traffic Flow Terminology
- Traffic Shaping Over Frame Relay
- Summary
- Quiz

Frame Relay Traffic Flow Terminology

This topic describes the terminology that is associated with FRTS. Traffic shaping can address bottlenecks and packet loss from mismatched data rates between source and destination.

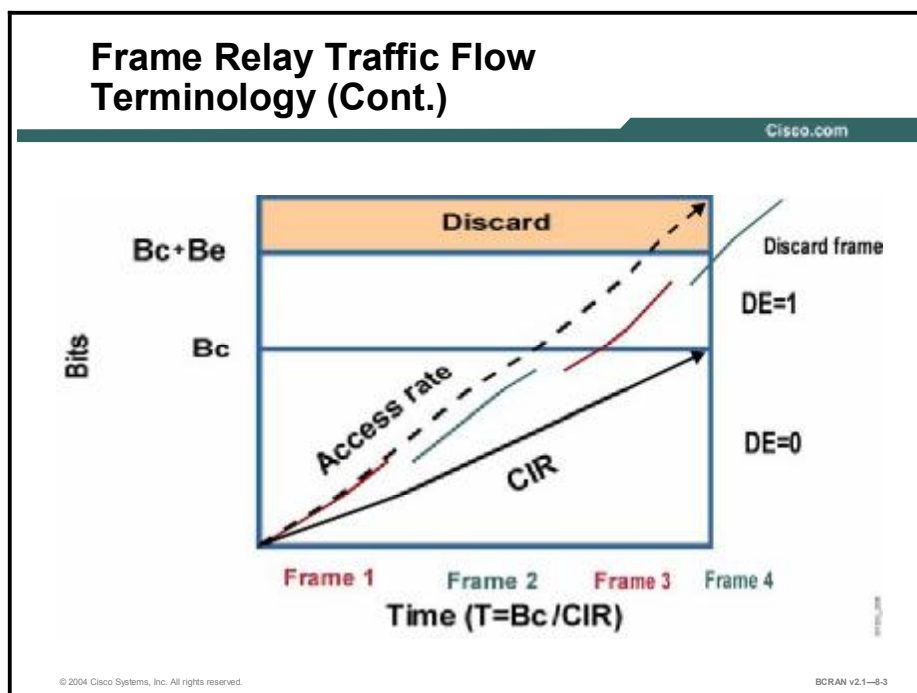


You should be familiar with some of the terminology that is related to Frame Relay traffic flow, as listed here:

- **Local access rate:** The clock speed (port speed) of the connection (local loop, access line, or access circuit) to the Frame Relay cloud. This is the rate at which data travels into or out of the network, regardless of other settings.
- **Committed information rate (CIR):** The rate, in bits per second, at which the Frame Relay switch agrees to transfer data. The rate is usually averaged over a period of time, referred to as the committed time window (T_c).
- **Oversubscribe, oversubscription:** Oversubscription occurs when the sum of the CIRs on all the VCs coming into a device exceeds the access line speed. Oversubscription also occurs when the access line supports the sum of the CIRs purchased, but not the sum of the CIRs plus the bursting capacities of the VCs. Oversubscription results in frames being dropped if the access line rate is exceeded.
- **Committed burst (B_c):** The maximum number of data (in bits) that the switch agrees to transfer during any T_c . For example, if the T_c is 125 milliseconds and the CIR is 32 kbps, the B_c is 64 kbps. ($CIR = B_c / T_c$)
- **Excess burst (B_e):** The maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR for the first time interval only. B_e is dependent on the service offerings available by your vendor, but is typically limited to the port speed of the local access line.

- **FECN:** When a Frame Relay switch is in congestion locally, it marks the FECN bit in the frame header, indicating that congestion has been encountered. Other switches in the path forward the frame, never resetting the FECN or BECN flag.
- **BECN:** When a Frame Relay switch is in congestion locally, it marks the BECN bit in the frame header, indicating that congestion has been encountered. With Cisco IOS Software Release 11.2 or later, Cisco routers can respond to BECN notifications. This topic is discussed in this lesson.
- **Discard eligible (DE) indicator:** The DE bit is set on the oversubscribed traffic, that is, the traffic that was received after the CIR was met. Until the release of Cisco IOS Software Release 12.2(6), Cisco routers were not able to set the DE bit.

Note These are generic Frame Relay terms. They may be the same or slightly different than the terms your Frame Relay service provider uses.



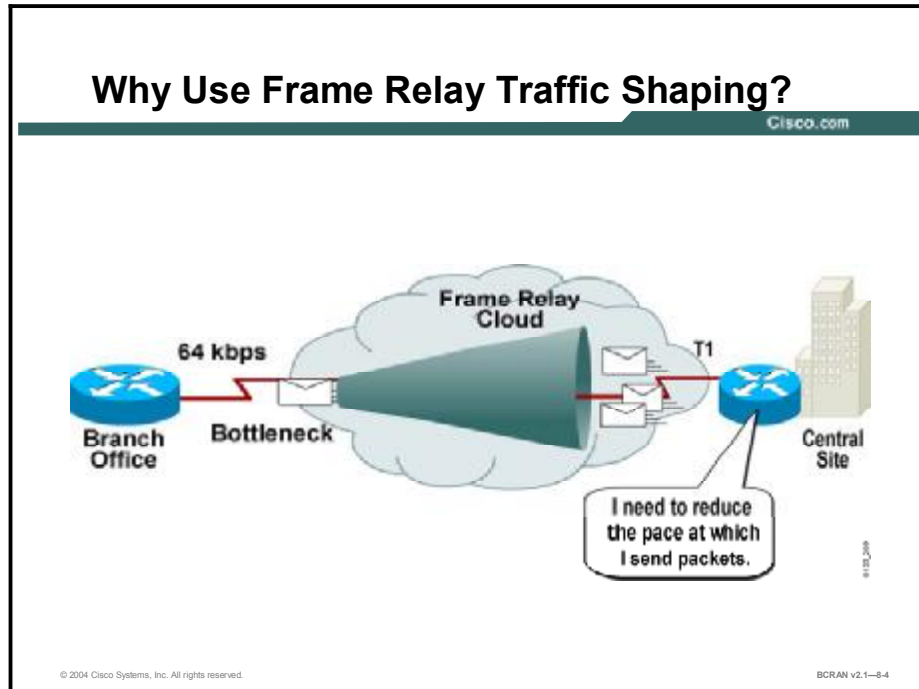
The CIR, by itself, does not provide much flexibility when dealing with varying traffic rates. In practice, the Frame Relay switch measures traffic over a time interval specific to each logical connection.

The B_c and B_e are amounts of data that a Frame Relay network agrees to transfer over a time interval, T_c . B_e is the maximum amount in excess of the B_c that the network attempts to transfer under normal conditions. The traffic that is beyond the B_c is marked with the DE bit set.

Notice that the actual frame transfer rate parallels the access rate. When a frame is being transmitted on a channel, that channel is dedicated to that transmission.

Traffic Shaping Over Frame Relay

This topic describes why FRTS is used. Traffic shaping is used to control access to available bandwidth and to regulate the flow of traffic to avoid congestion that can occur when the transmitted traffic exceeds the access speed of its remote target interface.

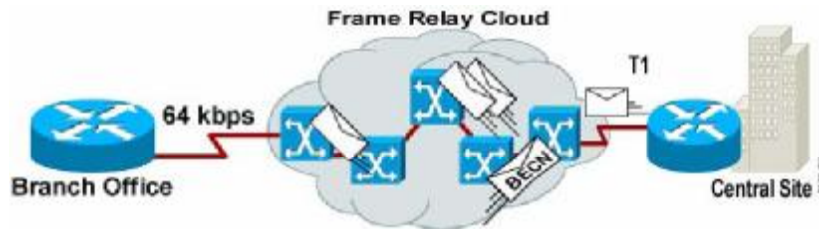


FRTS is used in these typical situations:

- When you have a Frame Relay network topology that consists of a high-speed (T1 line speed) connection at the central site and low-speed (64-kbps) connections at the branch sites. Because of the speed mismatch, a bottleneck often exists for traffic on a VC when the central site tries to communicate with the branch site. This bottleneck results in poor response times for traffic such as Systems Network Architecture (SNA) or interactive Telnet when it is stuck behind a large FTP packet on the low-speed line. Packets get dropped or delayed at the bottleneck, resulting in lost SNA sessions and possibly causing the central site to retransmit unacknowledged packets, making the congestion problem worse. The rate enforcement capability in FRTS can be used to limit the rate at which data is sent on the VC at the central site. Rate enforcement can also be used in conjunction with the existing DLCI prioritization feature to further improve performance in this situation.
- The VCs send traffic as fast as the physical line speed allows. This occurs when you have a Frame Relay network that is constructed with many VCs to different locations on a single physical line into the network. The rate enforcement capability of FRTS enables you to control the transmission speed used by the router by other criteria, such as the CIR or excess information rate (EIR). The rate enforcement feature preallocates the bandwidth that each VC receives on the physical line into the network, effectively creating a virtual statistical time-division multiplexing (TDM) network.

Why Use Frame Relay Traffic Shaping? (Cont.)

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-8-6

- If you have noticed that your Frame Relay connections occasionally get congested, you may want the router to throttle traffic instead of sending it into the network. Throttling the traffic may help prevent packet loss in the network. The BECN-based throttling capability provided with FRTS allows you to have the router dynamically throttle traffic based on receiving BECN-tagged packets from the network. This throttling holds packets in the buffers of the router to reduce the data flow from the router into the Frame Relay network. The throttling is done on a per-VC basis, and the rate is dynamically increased as fewer BECNs are received.
- Quite often you may have several different types of traffic to transmit on the same Frame Relay VC, such as IP, SNA, or Internetwork Packet Exchange (IPX). You may want to ensure that each different traffic type receives a certain amount of bandwidth. Using custom queuing with the per-VC queuing and rate enforcement capabilities enables you to configure VCs to perform this task. Prior to Cisco IOS Software Release 11.2, custom queuing was defined at the interface level only. Today, custom queuing can be defined at the VC level.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Local access rate is the clock speed of the connection to the Frame Relay cloud.**
- **Committed information rate is the rate in which the Frame Relay switch agrees to transfer data.**
- **Oversubscription occurs when the sum of the CIRs on all the virtual circuits coming into a device exceeds the access line speed.**
- **Committed burst is the maximum number of bits that the switch agrees to transfer during any committed rate measurement interval.**
- **Excess burst is the maximum number of uncommitted bits that the Frame Relay switch will attempt to transfer beyond the CIR for the first time interval only.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-6

Summary (Cont.)

Cisco.com

- **When a Frame Relay switch is in congestion locally, it marks the FECN bit in the frame header towards the destination device indicating that congestion has been encountered.**
- **When a Frame Relay switch is in congestion locally, it marks the BECN bit in the frame header indicating that congestion has been encountered.**
- **The DE bit is set on the oversubscribed traffic.**
- **Traffic shaping is used to control access to available bandwidth and to regulate the flow of traffic in order to avoid congestion that can occur when the transmitted traffic exceeds the access speed of its remote target interface.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-6-7

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) When a Frame Relay switch recognizes congestion in the network, which bit field will the switch use to notify the destination that congestion was experienced in the network?
- A) DE
 - B) FECN
 - C) BECN
 - D) CIR
- Q2) Traffic shaping is primarily used to _____.
- A) direct traffic flow to particular networks
 - B) break up data into smaller segments
 - C) control traffic transmission speeds
 - D) encapsulate data on Frame Relay connections

Quiz Answer Key

Q1) B

Relates to: Frame Relay Traffic Flow Terminology

Q2) C

Relates to: Traffic Shaping Over Frame Relay

Configuring Frame Relay Traffic Shaping

Overview

This lesson discusses Frame Relay traffic shaping (FRTS) configuration tasks.

Relevance

Traffic shaping controls the traffic leaving an interface to match its flow to the speed of the remote target interface. Traffic shaping also ensures that the traffic conforms to the policies for which it was contracted. For this reason, it is important to know how to configure FRTS. This lesson covers the concepts and commands for configuring FRTS.

Objectives

Upon completing this lesson, you will be able to:

- List the steps and commands that are required when configuring FRTS
- Manually configure FRTS
- Describe Frame Relay rate enforcement with BECN support
- Configure Frame Relay rate enforcement with BECN support

Learner Skills and Knowledge

To fully benefit from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Step 1: Configuration of FRTS
- Step 2: Configuration of FRTS
- Steps 3-5: Configuration of FRTS
- Traffic-Shaping Rate Enforcement
- Traffic-Shaping Rate Enforcement Configuration Example
- Traffic-Shaping BECN Support Example
- Traffic-Shaping BECN Support Configuration Example
- Traffic-Shaping Example
- Verification of FRTS
- **show traffic-shape** Command
- **show traffic-shape statistics** Command
- Summary
- Quiz

Step 1: Configuration of FRTS

There are five steps that are required to configure FRTS. This topic describes the commands that are required in the first step.

Step 1: Configuration of FRTS

Cisco.com

```
Router(config)#map-class frame-relay map-class-name
```

- Enters map class configuration mode so you can define a map class

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-8-2

To enable FRTS, perform these steps:

- Step 1** Specify a map class name to be defined with the **map-class frame-relay *map-class-name*** command.

Step 2: Configuration of FRTS

This topic describes the second step to configure FRTS, the specification of traffic-shaping bit rates (versus multiple commands to set individual rate parameters).

Step 2: Configuration of FRTS

Cisco.com

`Router(config-map-class)#frame-relay traffic-rate average [peak]`

- Defines the average and peak rates

or

`Router(config-map-class)#frame-relay adaptive-shaping becn`

- Specifies that the router fluctuates the sending rate based on the BECNs received

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-8.3

- Step 2** Define the map class. When you define a map class for Frame Relay, you can use these options for traffic shaping:
- Define the average and peak rates (in bits per second) allowed on virtual circuits associated with the map class.
 - Specify that the router dynamically changes the rate at which it sends packets, depending on the BECNs that it receives.
 - Specify either a custom queue list or a priority queue group to use on virtual circuits associated with the map class.

Regarding the first option, define the average and peak rates if the data is being sent faster than the speed at which the destination is receiving. If you define the average and peak rates (in bits per second) allowed on VCs that are associated with the map class, use the **frame-relay traffic-rate average [peak]** command.

The command syntax is described in the following table:

frame-relay traffic-rate Command Parameters

Command	Description
<i>average</i>	Average rate in bits per second; equivalent to specifying the contracted CIR.
<i>peak</i>	(Optional) Peak rate, in bits per second; equivalent to $CIR + Be/Tc = CIR + EIR$.

Specify that the sending router adjust its transmission rate based on the BECNs received. To select BECN as the mechanism to which traffic shaping will adapt, use the **frame-relay adaptive-shaping becn** command.

Note The **frame-relay adaptive-shaping** command replaces the **frame-relay becn-response-enable** command.

Step 2: Configuration of FRTS (Cont.)

Cisco.com

or

```
Router (config-map-class)#frame-relay custom-queue-list number
```

- Specifies a custom queue list

or

```
Router (config-map-class)#frame-relay priority-group number
```

- Specifies a priority group

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—8-4

- (Optional) If you want to distinguish and control traffic flow, you must specify a queuing mechanism such as a custom queue list or a priority group. To specify a custom queue list, use the **frame-relay custom-queue-list** *number* command. To specify a priority queue list, use the **frame-relay priority-group** *number* command. The *number* is a required number assigned to the custom or priority queue list. The command syntax is described in the following table.

frame-relay custom-queue-list and frame-relay priority-group Commands

Command	Description
frame-relay custom-queue-list <i>number</i>	Assigns a custom queue to VCs associated with the map class. Use this command when you want to guarantee a particular protocol or service. Use this command after you have defined a custom queue using the queue-list command.
frame-relay priority-group <i>number</i>	Assigns a priority queue to VCs that are associated with the map class. Use this command when you want to guarantee an absolute priority for a protocol or service. Use this command after defining the priority queue using priority-list command.

Only one queuing mechanism may be associated with a map class. To change the queuing mechanism from a type other than the default (FIFO), the previous queuing mechanism must first be disabled using the **no** form of the command.

Note Custom and priority queuing are not recommended methods of queuing. Low latency queuing (LLQ) and class-based weighted fair queuing (CBWFQ) have replaced them.

Steps 3-5: Configuration of FRTS

This topic describes last three steps to configure FRTS.

Steps 3-5: Configuration of FRTS

Cisco.com

Step 3

```
Router(config-if)#encapsulation frame-relay
```

- Enables Frame Relay on an interface

Step 4

```
Router(config-if)#frame-relay class map-class-name
```

- Maps the map class to virtual circuits on the interface

Step 5

```
Router(config-if)#frame-relay traffic-shaping
```

- Enables Frame Relay traffic shaping on an interface

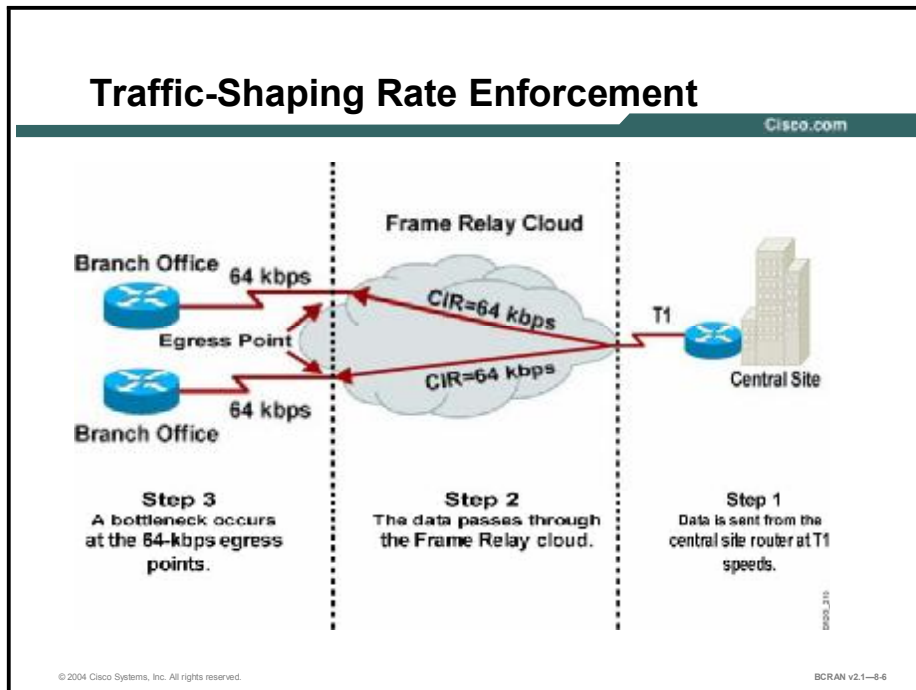
© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-8.5

- Step 3** After you have defined a map class with queuing and traffic-shaping parameters, enter interface configuration mode and enable Frame Relay encapsulation on an interface with the **encapsulation frame-relay** command.
- Step 4** Map a map class to all VCs on the interface with the **frame-relay class map class-name** command. The *map class-name* argument must match the *map class-name* of the map class that you configured.
- Step 5** Enable FRTS shaping on an interface with the **frame-relay traffic-shaping** command. Enabling FRTS on an interface enables both traffic shaping and per-VC queuing on all the PVCs and SVCs on the interface. Traffic shaping enables the router to control the output rate of the circuit and react to congestion notification information, if that is also configured.

Note You can map the map class to the interface or a specific subinterface on the interface. Subinterfaces inherit the class parameters mapped to the main interface, unless a specific class is applied to the subinterface.

Traffic-Shaping Rate Enforcement

Traffic shaping is used to implement rate enforcement. This topic describes a typical scenario where Frame Relay rate enforcement should be configured.



The figure illustrates a typical Frame Relay environment. The central site has a T1-speed local loop connection, and the branch offices have slower local loop connections, in this case 64 kbps. In addition, the CIR for each PVC going from the central site to each branch office is 64 kbps. In this environment, the following process occurs:

1. The central site may send data across the T1-speed line. Even though the CIR is 64 kbps, the router continues to send the data based on the T1 rate.
2. The data goes through the cloud.
3. When the data reaches the local loop that is connected to the branch office, a bottleneck occurs because the data is being sent faster than the speed of the branch office local loop. At this point packets are buffered at the egress point of the network, which increases line response time and can cause problems, particularly for latency-sensitive protocols such as SNA.

The solution to this bottleneck is to slow the speed at which the central site router is sending data. With FRTS, you can define and enforce a rate on the VC at which the router will send data. The pace you set can be the CIR, EIR, or some other value.

Traffic-Shaping Rate Enforcement Configuration Example

This topic describes how to manually configure Frame Relay rate enforcement.

Configuring Traffic-Shaping Rate Enforcement Example

Cisco.com

```
central (config)#interface Serial2
central (config-if)#no ip address
central (config-if)#encapsulation frame-relay
central (config-if)#frame-relay traffic-shaping
central (config-if)#frame-relay class branch
!
!
!
central (config)#map-class frame-relay branch
central (config-map-class)#frame-relay traffic-rate 32000 64000
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-7

Perform these steps to configure FRTS rate enforcement:

Step 1 Define a map class and enter map class configuration mode, as follows:

```
map-class frame-relay map-class-name
```

Step 2 Define the rate enforcement parameters to use, as follows:

```
[no] frame-relay traffic-rate average [peak]
```

- *average* is the “average rate” (equivalent to setting CIR).
- *peak* is the “peak rate” (equivalent to $CIR + Be/Tc = CIR(1 + Be/Bc) = CIR + EIR$).

If the peak value is not configured, the peak rate will default to the *average* value configured.

For SVCs, the configured peak and average rates are converted to the equivalent CIR, Be, and Bc values for use by SVC signaling.

- The **frame-relay traffic-rate** command configures all of the traffic-shaping characteristics of a VC (CIR, Bc, Be) in a single command. It is much simpler than setting each parameter individually in the map class, but it does not provide the additional granularity. Only one command format—either traffic rate or setting individual values for CIR, Be, or Bc—will be accepted in one map class. The user is warned when entering a second command type that the previous traffic rate is being overwritten.

Step 3 Enable both traffic shaping and per-VC queuing for all VCs (PVCs and SVCs) on a Frame Relay interface, as follows:

frame-relay traffic-shaping

For VCs where no specific traffic-shaping or queuing parameters are specified, the values are inherited from the parent interface; otherwise, a default set of values is used.

Step 4 Associate a map class with an interface or subinterface, as follows:

frame-relay class name

Each VC created on the interface or subinterface inherits all of the relevant parameters defined in the Frame Relay class name. For each VC, the precedence rules are as follows:

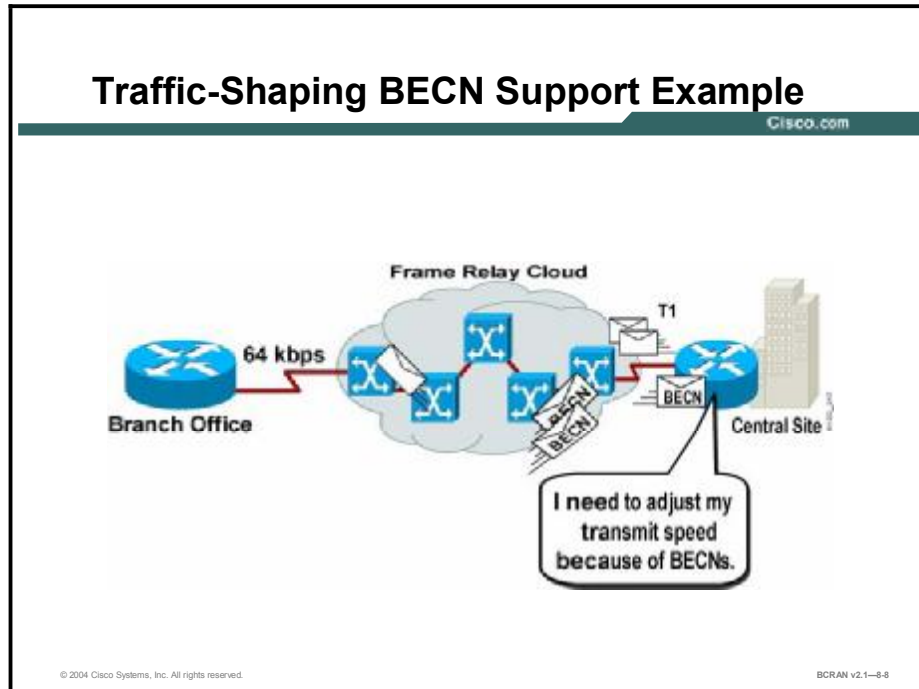
- Use a map class associated with the VC, if it exists.
- If not, use a map class associated with the subinterface, if it exists.
- If not, use a map class associated with the interface, if it exists.
- If not, use the default parameters.

Step 5 (Optional) Apply a map class to a specific DLCI for which a Frame Relay map statement exists, as follows:

```
frame-relay interface-dlci dlci [ietf | cisco]  
class name
```

Traffic-Shaping BECN Support Example

This topic describes Frame Relay rate enforcement with BECN support.



The figure illustrates a Frame Relay environment where a site has a different speed on its local loop connections to the Frame Relay cloud.

In this environment, without FRTS, the following process can occur:

1. The central site router sends data to the branch office router.
2. One of the switches within the cloud determines that it is getting congested with traffic. In this case, the congested switch sets the BECN bit in reply packets from the branch office router to the central site router.
3. The central site router notes that the BECN is received but does not slow its transmission rate.
4. At this point, packets from the central site router begin dropping within the switch that is encountering the congestion. This condition results in retransmissions, further congesting the link.

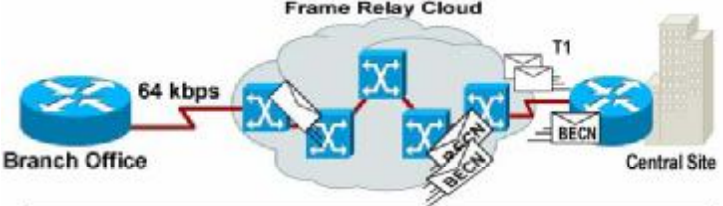
The solution for this problem is to enable the router to dynamically fluctuate the rate at which it sends packets, depending on the BECNs that it receives. For example, if the router begins receiving many BECNs, it reduces the packet transmit rate. As the BECNs become intermittent, the router increases the packet transmit rate. The goal is to send the optimal amount of traffic without incurring drops, thus maximizing throughput.

Traffic-Shaping BECN Support Configuration Example

This topic describes how to configure Frame Relay rate enforcement with BECN support.

Configuring Traffic-Shaping BECN Support Example

Cisco.com



```
central(config)#interface serial 0
central(config-if)#no ip address
central(config-if)#encapsulation frame-relay
central(config-if)#frame-relay traffic-shaping
central(config-if)#frame-relay class becnnotify
!
!
!
central(config)#map-class frame-relay becnnotify
central(config-map-class)#frame-relay adaptive-shaping becn
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-0

Perform these steps to configure traffic shaping with Frame Relay BECN support:

Step 1 Define a map class and enter map class configuration mode, as previously discussed.

Step 2 Make sure that BECN support is enabled, as follows:

frame-relay adaptive-shaping becn

- BECN support is disabled by default.
- When enabled, BECNs received from the network on this VC are used to further regulate the output rate on the VC. As the frequency of BECNs increases, the output rate is steadily reduced from *peak* to *average* (equivalent of CIR). As congestion eases in the network and the frequency of BECNs decreases, the output rate is allowed to increase gradually to its configured *peak*.

Step 3 Enable both traffic shaping and per-VC queuing for all VCs (PVCs and SVCs) on a Frame Relay interface, as follows:

frame-relay traffic-shaping

For VCs where no specific traffic-shaping or queuing parameters are specified, a set of default values are used.

Step 4 Associate a map class with an interface or subinterface, as follows:

frame-relay class name

Step 5 (Optional) Apply the map class to a specific DLCI for which a Frame Relay map statement exists, as follows:

```
frame-relay interface-dlci dlci [broadcast] [ietf | cisco]  
class name
```

Traffic-Shaping Example

This topic describes an example of Frame Relay rate enforcement with BECN support configuration.

Traffic-Shaping Example

Cisco.com

```
interface Serial0
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay traffic-shaping
frame-relay class slow_vcs
!
interface Serial0.1 point-to-point
ip address 10.128.30.1 255.255.255.248
ip ospf cost 200
bandwidth 10
frame-relay interface-dlci 101
!
interface Serial0.2 point-to-point
ip address 10.128.30.9 255.255.255.248
ip ospf cost 400
bandwidth 10
frame-relay interface-dlci 102
frame-relay class fast_vcs
!
interface Serial0.3 point-to-point
ip address 10.128.30.17 255.255.255.248
ip ospf cost 200
bandwidth 10
frame-relay interface-dlci 103
```

```
!
map-class frame-relay slow_vcs
frame-relay traffic-rate 9600 4800
frame-relay custom-queue-list 1
!
map-class frame-relay fast_vcs
frame-relay traffic-rate 64000 16000
frame-relay priority-group 2
!
access-list 100 permit tcp any any eq 255
access-list 115 permit tcp any any eq 256
!
priority-list 3 protocol decnet high
priority-list 2 protocol ip normal
priority-list 2 default medium
!
queue-list 1 protocol ip 1 list 100
queue-list 1 protocol ip 2 list 115
queue-list 1 default 3
queue-list 1 queue 1 byte-count 1400 limit 300
queue-list 1 queue 2 byte-count 600 limit 200
queue-list 1 queue 3 byte-count 500 limit 200
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-10

In this example, the VC on subinterfaces Serial0.1 and Serial0.3 inherit class parameters from the main interface, namely those defined in *slow_vcs*. However, the virtual circuit defined on subinterface Serial0.2 (DLCI 102) is specifically configured to use map class *fast_vcs*.

Map class *slow_vcs* uses a peak rate of 9600 bps and an average rate of 4800 bps. If BECN adaptive shaping is configured for this map class, the output rate will be cut back to as low as 4800 bps in response to received BECNs. This map class is configured to use custom queuing using queue-list 1. In this example, queue-list 1 has three queues, with the first two queues being defined by access lists 100 and 115.

Map class *fast_vcs* uses a peak rate of 64,000 bps and an average rate of 16,000 bps. If BECN adaptive shaping was configured for this map class, the output rate would be cut back to as low as 4800 bps in response to received BECNs. This map class is configured to use priority queuing using priority-group 2.

Verification of FRTS

Various commands are required to monitor and troubleshoot FRTS. This topic describes the **show frame-relay pvc** command, which is useful for displaying the parameters that are used in traffic shaping and the queuing algorithm that is in use for all interfaces.

Verification of FRTS

Cisco.com

```
central#show frame-relay pvc 110
PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

  input pkts 2713          output pkts 1181          in bytes 1738767
  out bytes 119488        dropped pkts 0            in pkts dropped 0
  out pkts dropped 0      out bytes dropped 0
  in FECN pkts 0         in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0        in DE pkts 0             out DE pkts 0
  out hoast pkts 1       out hoast bytes 34

  Shaping adapts to BECN
  pvc create time 00:16:09, last time pvc status changed 00:16:09
  cir 9600    bc 9600    bo 0    byte limit 150    interval 125
  mincir 4800  byte increment 150    Adaptive Shaping BULKY
  pkts 1182    bytes 120092    pkts delayed 27    bytes delayed 3660
  shaping active
  traffic shaping drops 0
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN V2.1-8-11

In addition to Frame Relay PVC status, traffic, and DLCI information, the **show frame-relay pvc [interface interface] [dlci]** command includes the parameters that are used in traffic shaping, if enabled, and the queuing algorithm that is in use for all interfaces. The specific details displayed for traffic shaping and queuing depend on the specific Cisco IOS software release.

show traffic-shape Command

This topic describes another command that is used to monitor and troubleshoot FRTS. The **show traffic-shape** command is used to display the current traffic-shaping configuration.

show traffic-shape Command

Cisco.com

$MAX = Bc + Be$
 Be
 $Bc = Tc + CIR$

```

Router#show traffic-shape
Interface  Se0/0
  Access Target  Byte  Sustain  Excess  Interval  Increment Adapt
 VC   List   Rate  Limit  bits/int bits/int  (ms)    (bytes)  Active
 110  9600  150   5600    0       125      150     BECN
    
```

CIR

Bc

$Tc = Bc / CIR$

Do we listen to
FECN / BECN?

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1--8-12

Use the **show traffic-shape** command to display the current traffic-shaping configuration. The command output contains these fields:

show traffic-shape Command Fields

Field	Description
Target Rate	Rate that traffic is shaped to, in bps.
Byte Limit	Maximum number of bytes transmitted per internal interval.
Sustain bits/int	Configured sustained bits per interval.
Excess bits/int	Configured excess bits per interval.
Interval (ms)	Interval being used internally. This interval may be smaller than the Bc divided by the CIR if the router determines that traffic flow will be more stable with a smaller configured interval.
Increment (bytes)	Number of bytes that are sustained per internal interval.
Adapt Active	Contains BECN if Frame Relay has BECN adaptation configured.

show traffic-shape statistics Command

This topic describes the **show traffic statistics** command, which is used to display the current traffic-shaping statistics.

show traffic-shape statistics Command

Cisco.com

Number of packets or bytes sent on the interface

```

Router# show traffic-shape statistics
      Access Queue  Packets  Bytes  Packets  Bytes  Shaping
      List   Depth                Delayed Delayed  Active
-----
Se0/0         2      2595    317116    119    58921    yes
    
```

Current depth of the associated
queue for delayed packets

Actual number of packets or bytes
subject to delay due to traffic shaping

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-13

Use the **show traffic-shape statistics** command to display the current traffic-shaping statistics. The command output contains the fields in the following table.

show traffic-shape statistics Command Fields

Field	Description
Queue Depth	Number of messages in the queue
Packets	Number of packets sent through the interface
Bytes	Number of bytes sent through the interface
Packets Delayed	Number of packets sent through the interface that were delayed in the traffic-shaping queue
Bytes Delayed	Number of bytes sent through the interface that were delayed in the traffic-shaping queue
Shaping Active	Contains "yes" when timers indicate that traffic shaping is occurring and "no" if traffic shaping is not occurring

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Traffic shaping can be used to address bottlenecks and packet loss due to mismatched data rates between source and destination.**
- **Traffic shaping controls the traffic going out an interface in order to match its flow to the speed of the remote, target interface, and to ensure that the traffic conforms to policies contracted for it.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-8-14

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 8-1: Establishing a Dedicated Frame Relay Connection and Controlling Traffic Flow

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) In the command **frame-relay adaptive-shaping becn**, what does **becn** indicate?
- A) the mechanism that traffic shaping will use
 - B) the name to represent this process
 - C) how packets will be prioritized
- Q2) How many queuing mechanism(s) may be associated with a map class?
- A) one
 - B) two
 - C) three
 - D) four
- Q3) The **encapsulation frame-relay** command enables Frame Relay on an interface.
- A) true
 - B) false
- Q4) Your central site has a T1 connection and the branch offices have 56-kbps connections. You should apply traffic shaping at the _____ to limit _____ traffic.
- A) central site; outgoing
 - B) central site; incoming
 - C) branch offices; outgoing
 - D) branch offices; incoming
- Q5) Traffic-shaping rate enforcement will optimize asynchronous Frame Relay connections.
- A) true
 - B) false
- Q6) The command **frame-relay class *name*** may be used on physical interfaces only.
- A) true
 - B) false
- Q7) Which command is used to configure traffic-shaping BECN support?
- A) **frame-relay class becn**
 - B) **frame-relay adaptive-shaping becn**
 - C) no configuration necessary, enabled by default

- Q8) What does 1200 refer to in the command **frame-relay traffic-rate 1200 4800**?
- A) committed information rate
 - B) average rate
 - C) peak rate
 - D) normal rate
- Q9) Both the **show queuing** and **show interfaces** commands display queuing information about interfaces.
- A) true
 - B) false
- Q10) The **show traffic-shape** command output contains the following fields except:
- A) target rate
 - B) byte limit
 - C) interval (sec)
 - D) increment (bytes)
- Q11) The **show traffic-shape statistics** command contains the following fields except:
- A) packets
 - B) bytes
 - C) packets delayed
 - D) packets rejected

Quiz Answer Key

- Q1) A
Relates to: Step 1: Configuration of FRTS
- Q2) A
Relates to: Step 2: Configuration of FRTS
- Q3) A
Relates to: Steps 3-5: Configuration of FRTS
- Q4) A
Relates to: Traffic-Shaping Rate Enforcement
- Q5) A
Relates to: Traffic-Shaping Rate Enforcement Configuration Example
- Q6) B
Relates to: Traffic-Shaping BECN Support Example
- Q7) B
Relates to: Traffic-Shaping BECN Support Configuration Example
- Q8) B
Relates to: Traffic-Shaping Example
- Q9) A
Relates to: Verification of FRTS
- Q10) C
Relates to: **show traffic-shape** Command
- Q11) D
Relates to: **show traffic-shape statistics** Command

Implementing DDR Backup

Overview

This module describes how to configure a backup connection for a primary connection, such as a Frame Relay serial connection, in the event that the link goes down or is overused.

Objectives

Upon completing this module, you will be able to:

- Configure a backup connection that activates upon primary line failure
- Configure a backup connection to engage when the primary line reaches a specified threshold
- Configure a dialer interface and a specific physical interface to function as backup to the primary interface

Outline

The module contains these lessons:

- Configuring Dial Backup
- Routing with the Load Backup Feature

Configuring Dial Backup

Overview

This lesson describes how to configure a backup connection for a primary connection, such as a Frame Relay serial connection, in the event that the link goes down or is overused.

Relevance

Dial backup provides protection against WAN downtime by allowing the network administrator to configure a backup serial line through a circuit-switched connection.

Objectives

Upon completing this lesson, you will be able to:

- Configure a backup connection that activates upon primary line failures
- Configure a backup connection to engage when the primary line reaches a specified load threshold
- Identify the steps that are needed to correctly configure a backup connection to engage when the primary line fails
- Configure a backup connection to correctly identify when the primary line fails and to delay engaging when the primary line fails
- Configure a backup connection to delay engaging when the primary line fails and delay the shutdown of the backup interface after the primary interface is re-enabled
- Show an example of a configuration of a backup connection that will engage when the primary line reaches a specified load threshold of 60 percent
- Identify the limitations of using a physical interface as a backup interface
- Identify scalability measures for backup interfaces by using dialer profiles

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

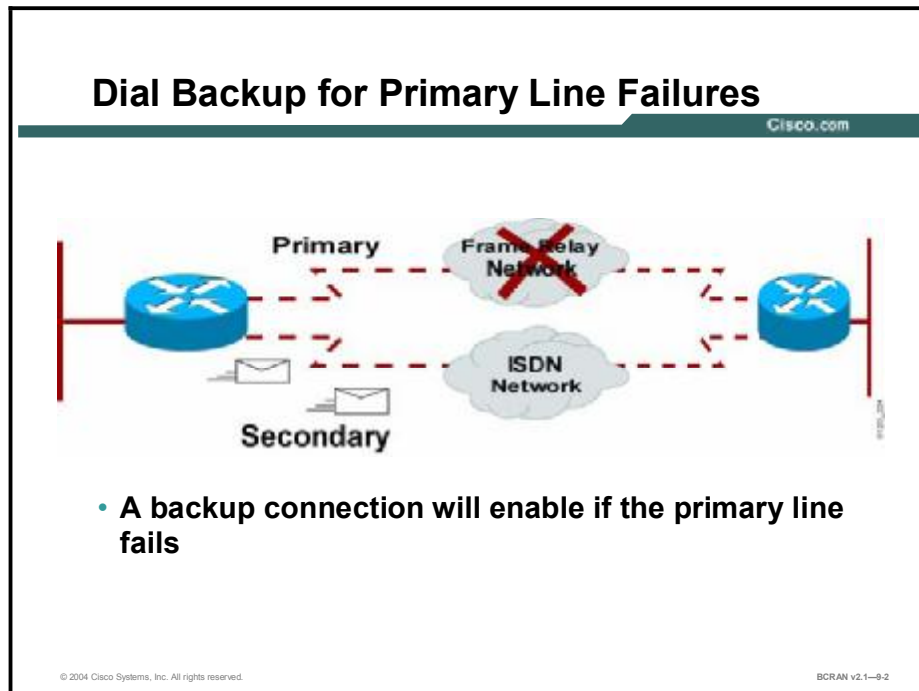
Outline

This lesson includes these topics:

- Overview
- Dial Backup Overview
- Dial Backup for High Primary Line Usage
- Activation of Backup Interfaces for Primary Line Failures
- Activation of Dial Backup
- Dial Backup Activation Example
- Configuration of Dial Backup for Excessive Traffic Load
- Configuration Example of Dial Backup for Excessive Traffic Load
- Backup Limitations with Physical Interfaces
- Dial Backup with Dialer Profile
- Configuration of a Backup Dialer Profile
- Dialer Profile Backup Example
- Summary
- Quiz

Dial Backup Overview

This topic describes configuring a backup connection that activates upon primary line failures.



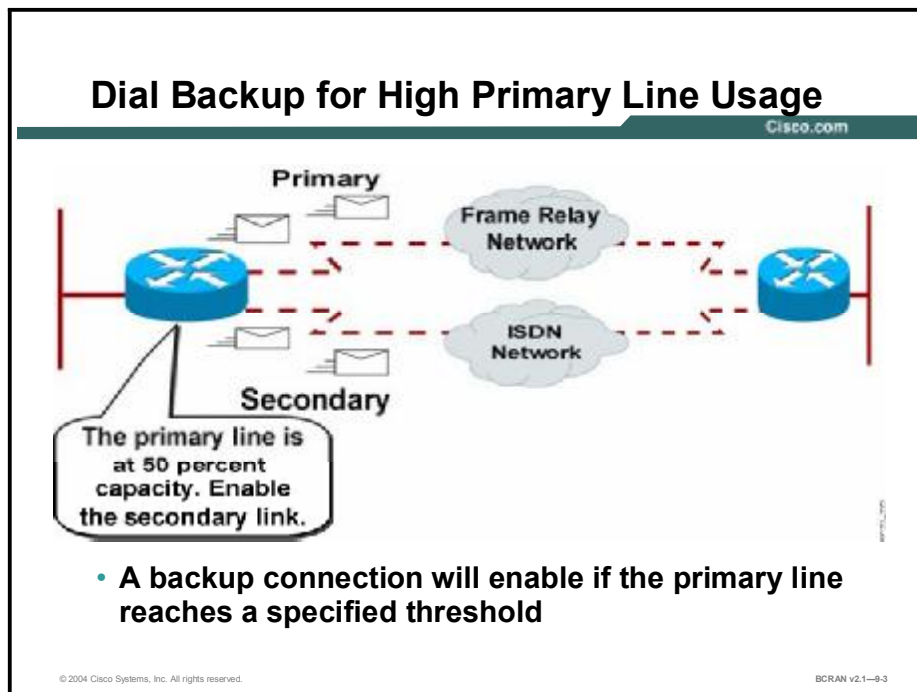
Dial-on-demand routing (DDR) backup is a method of bringing up an alternate dialup link if the primary WAN link fails. When the router configured for DDR backup recognizes that the primary connection to the remote site has been lost, it initiates a DDR connection to the remote site using an alternative dialup connection. In some cases, when a single permanent virtual connection (PVC) or data-link connection identifier (DLCI) fails on a Frame Relay multipoint interface, the PVC failure will not initiate a dial backup connection. The router will initiate a DDR backup connection only if it detects that the primary interface has failed.

The backup interface can be a physical interface or an assigned backup interface to be used in a dialer pool. Backup interfaces for a primary line can be an ISDN BRI interface, an asynchronous interface, dialer interface, or another serial interface.

Backup interfaces are beneficial for redundancy in case primary lines fail. The example in the figure illustrates an ISDN backup for a Frame Relay network.

Dial Backup for High Primary Line Usage

This topic describes configuring a backup connection to engage when the primary line reaches a specified threshold.



In addition to backing up a primary line in case of failure, a secondary backup interface can be configured to activate when one of the following circumstances occurs:

- The load on the primary line reaches a specified threshold
- The load on the primary line exceeds a specified threshold

Activation of Backup Interfaces for Primary Line Failures

This topic describes the steps needed to correctly configure a backup connection to engage when the primary line fails.

Activating Dial Backup for Line Failures

Cisco.com

```
Router(config-if)#backup interface interface-type number
```

- Specifies the backup interface

```
Router(config-if)#backup delay {enable-delay | never}  
{disable-delay | never}
```

- Designates when to activate the backup line if a primary line fails

© 2004 Cisco Systems, Inc. All rights reserved.BICRAN v2.1-9.4

Perform these steps to configure backup if a primary line goes down:

- Step 1** Select the primary interface and configure it as needed (for DDR, Frame Relay interfaces and subinterfaces, ATM, and so on).
- Step 2** On the primary interface, use the **backup interface *interface-type number*** command to specify the backup to be used if a dial backup is needed. The command syntax is shown in the table.

backup interface *interface-type number* Command

Command	Description
<i>interface-type number</i>	Specifies the interface or dialer interface to use for backup. Interface number specifications vary from router to router. For example, some routers require you to just specify the port number, while others require you to specify the slot and port.

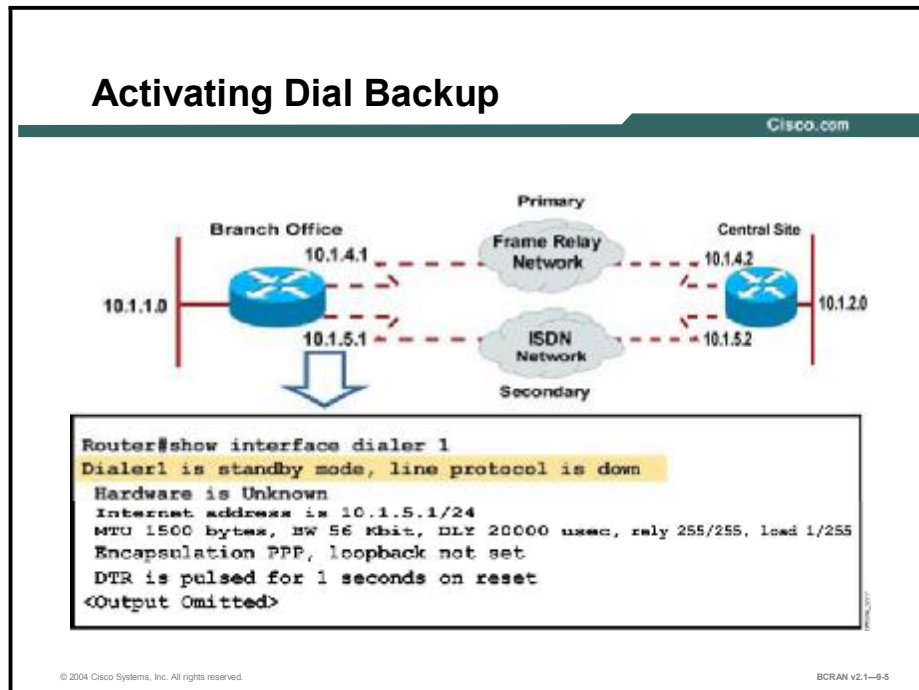
Step 3 Define the period of time to wait before enabling the backup link when the primary link goes down with the **backup delay** *{enable-delay | never} {disable-delay | never}* command. The command syntax is shown in the table.

backup delay *{enable-delay | never} {disable-delay | never}* Command

Command	Description
<i>enable-delay</i>	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line
<i>disable-delay</i>	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line
<i>never</i>	Prevents the secondary line from being activated or deactivated

Activation of Dial Backup

This topic describes configuring a backup connection to correctly identify when the primary line fails, and configuring a backup connection to delay engaging when the primary line fails.



When a backup interface is specified on a primary line, the backup interface is placed in standby mode, as illustrated in the figure. Once in standby mode, the backup interface is effectively shut down until enabled. The backup route between the two company sites is not resolvable and does not appear in the routing table.

The primary link is the only route that appears in the routing table. The branch office router continues to monitor the line protocol of the primary interface or subinterface.

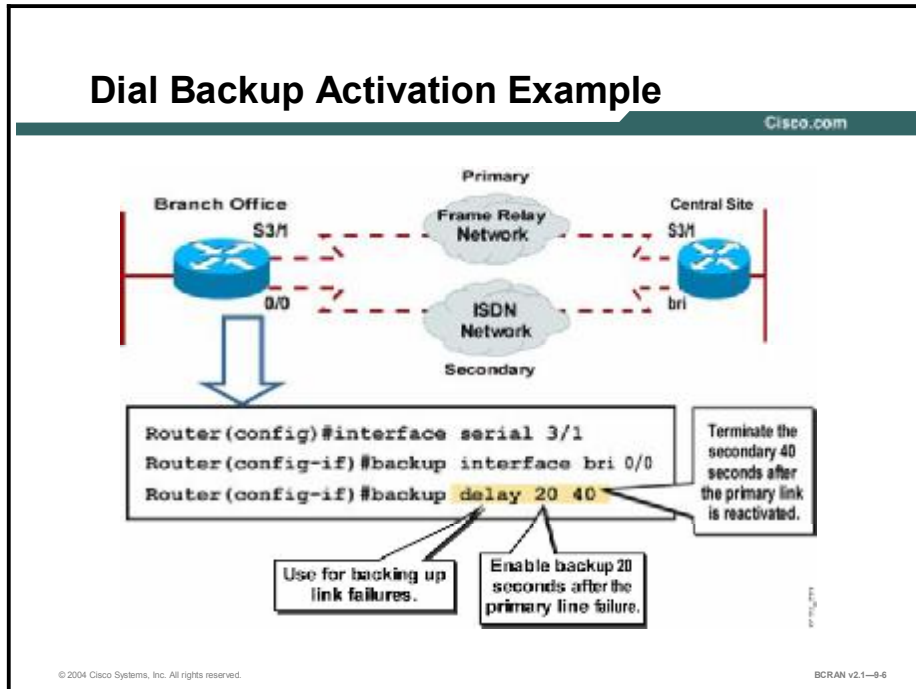
When the branch office router receives an indication that the primary interface is down, the backup interface is brought up. The amount of time that the device waits to bring up the backup interface is adjustable using the **backup delay** command. You can also configure the backup interface to go down (after a specified time) when the primary connection is restored.

The **backup interface** command is dependent on the router identifying that an interface is physically down. Because of this, the **backup interface** command is commonly used to back up ISDN BRI connections, asynchronous lines, and leased lines. This is because the interfaces to such connections go down when the link fails; therefore, the backup interface can quickly identify such failures. The backup interface approach may also be used for point-to-point Frame Relay subinterfaces. However, with Frame Relay, the main or multipoint interfaces can remain in an up/up state even if the PVC goes down. This could cause the router to fail to detect a down primary Frame Relay connection, and thereby fail to bring up the backup link.

A new development for end-to-end PVC management is a Cisco proprietary feature known as Frame Relay end-to-end keepalive. In Frame Relay end-to-end keepalive, keepalive packets are encapsulated in Frame Relay. This feature provides a status to verify that end-to-end communications are working and that traffic is getting through. This feature also allows a Cisco device to quickly detect that a link is down and enable the backup link.

Dial Backup Activation Example

This topic describes configuring a backup connection to delay engaging when the primary line fails, and delaying the shutdown of the backup interface after the primary interface is re-enabled.



In the figure, interface serial 3/1 is the primary interface. If the primary interface is down for 20 seconds, the backup interface, bri 0/0, is activated. The secondary line deactivates 40 seconds after the primary line is re-enabled.

Note The example in the figure illustrates only the commands to enable a backup. The interface must also be configured as needed (for DDR, Frame Relay, ATM, and so on).

Configuration of Dial Backup for Excessive Traffic Load

This topic describes configuring a backup connection to engage when the primary line reaches a specified load threshold. Also discussed are the steps that are needed to engage a backup interface when the primary line reaches a specified load threshold.

Configuring Dial Backup for Excessive Traffic Load

Cisco.com

```
Router(config-if)#backup interface interface-type number
```

- Specifies the backup interface

```
Router(config-if)#backup load {enable-threshold | never}  
{disable-load | never}
```

- Specifies when the backup interface should enable or disable

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-9-7

You can configure a backup to activate the secondary line based on the traffic load on the primary line. The software monitors the traffic load and computes a 5-minute moving average. The 5-minute moving average can be modified to provide a more responsive load backup with the **load-interval** command. If this average exceeds the value you set for the line, the secondary line is activated. In addition, depending on how the line is configured, some or all of the traffic flows onto the secondary dialup line.

Perform these steps to configure backup if a primary line reaches or exceeds a certain threshold:

- Step 1** Select the primary interface and configure it as needed (for DDR, Frame Relay interfaces and subinterfaces, ATM, and so on).
- Step 2** On the primary interface, use the **backup interface** *interface-type number* command to specify the backup to be used if a dial backup is needed. The command syntax is shown in the table.

backup interface *interface-type number* Command

Command	Description
<i>interface-type number</i>	Specifies the interface or dialer interface to use for backup. Interface number specifications vary from router to router. For example, some routers require you to just specify the port number, while others require you to specify the slot and port.

- Step 3** To set the traffic load threshold for dial backup service, use the **backup load** *{enable-threshold | never} {disable-load | never}* command. The command syntax is shown in the table.

backup load *{enable-threshold | never}{disable-load | never}* Command

Command	Description
<i>enable-threshold</i>	Percentage of the available bandwidth of the primary line that the traffic load must exceed to enable dial backup
<i>disable-load</i>	Percentage of the available bandwidth of the primary line that the traffic load must be less than to disable dial backup
<i>never</i>	Prevents the secondary line from being activated or deactivated

Note Because the backup load is determined on an interface, the backup load feature cannot be configured on a subinterface.

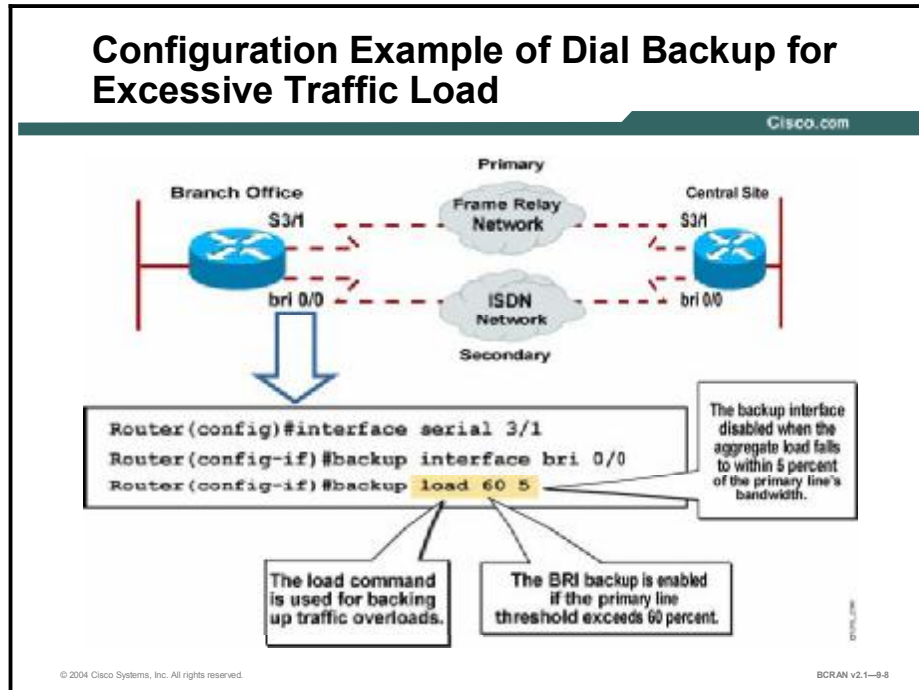
- Step 4** (Optional) To change the length of time for which data is used to compute load statistics, use the **load-interval** *seconds* interface configuration command. The command syntax is shown in the table.

load-interval *seconds* Command

Command	Description
<i>seconds</i>	Length of time for which data is used to compute load statistics; a value between 30 and 600 that is a multiple of 30. Used to increase the accuracy of the interface load. Warning: This command will increase the load on the CPU because of more frequent calculations.

Configuration Example of Dial Backup for Excessive Traffic Load

This topic describes the configuration of a backup connection to engage when the primary line reaches a specified load threshold of 60 percent.

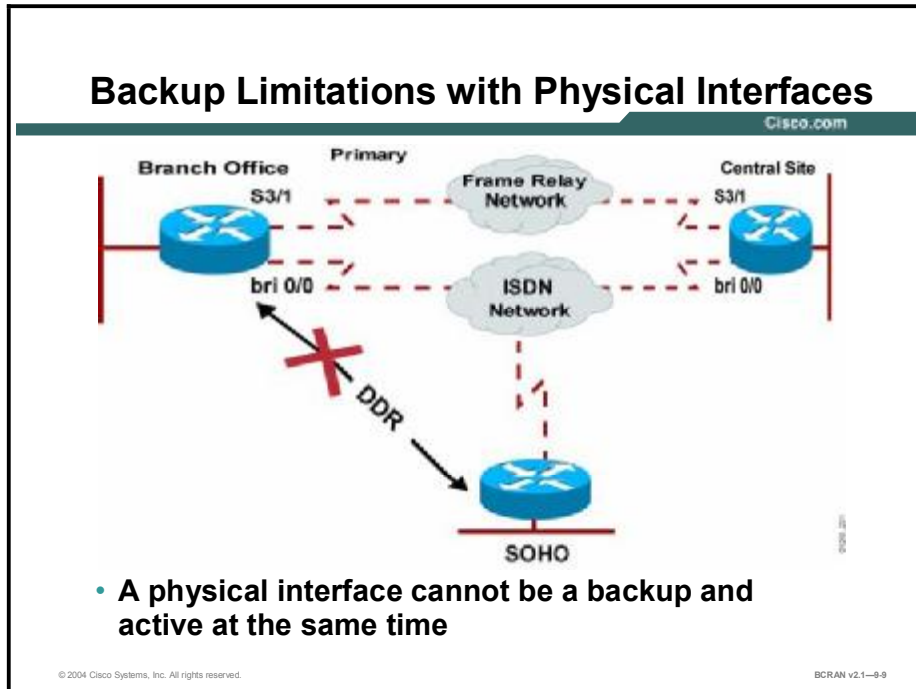


The example in the figure sets the traffic threshold to 60 percent of the primary line serial 3/1. When the load is exceeded, the secondary line, BRI 0/0, is activated, and is not deactivated until the load is less than 5 percent of the primary bandwidth.

Note The example in the figure illustrates only the commands to enable a backup. The interface must also be configured as needed (for DDR, Frame Relay, ATM, and so on).

Backup Limitations with Physical Interfaces

This topic describes the limitations of using a physical interface as a backup interface.

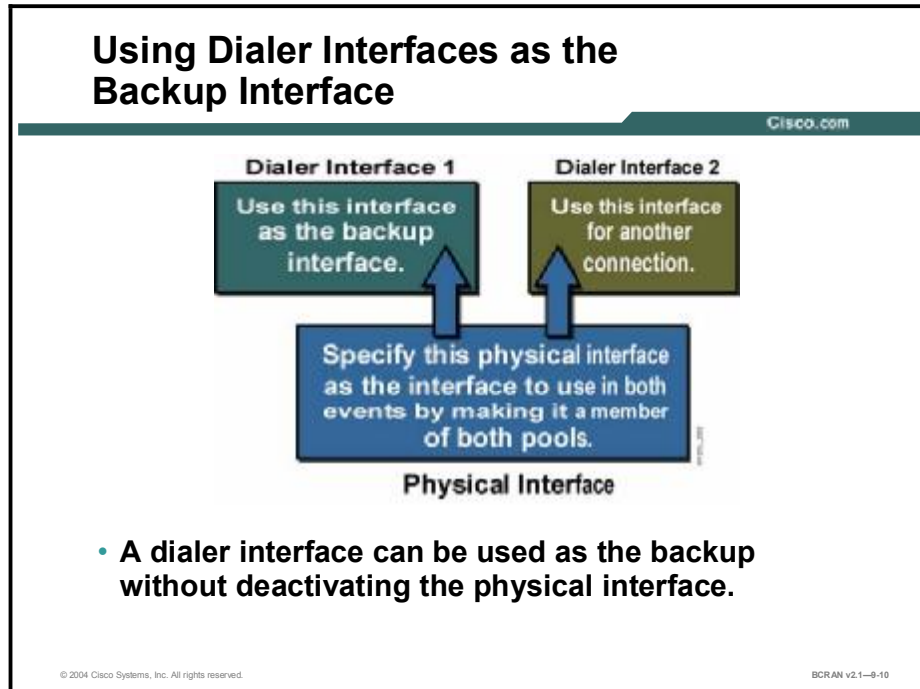


If a physical ISDN BRI interface is used as a backup to a primary connection, it will be placed in standby mode and cannot be used as a link to another site. This method illustrates an inefficient use of router resources, because the physical BRI interface can be used to send traffic across the WAN.

In the figure shown, the branch office wants to back up its Frame Relay connection with ISDN BRI. However, the branch office also wants to use the same BRI interface as a DDR link to a small office, home office (SOHO). If the branch office places the physical BRI link in standby mode, it is deactivated and will not activate until the primary line fails or reaches a specified threshold. Thus, the BRI link cannot be used to connect to the SOHO.

Dial Backup with Dialer Profile

This topic describes the scalability measures for backup interfaces by using dialer profiles.



With dialer profiles, the BRI connection in the preceding figure can be used to back up the primary Frame Relay link between the central site and branch office. At the same time, a BRI connection can be configured for DDR between the branch office and SOHO. By configuring one dialer profile to act as the backup line, this profile will be in standby mode until engaged. Configuring another dialer profile allows for communication between the branch office and SOHO sites. Thus, configuring the physical BRI interface to be a member of both dialer pools enables the physical BRI interface for backup and remote connectivity.

Note When you use a BRI for a dial backup, neither of the bearer (B) channels can be used while the interface is in standby mode. In addition, when a BRI is used as a backup interface and the BRI is configured for legacy DDR, only one B channel is usable. After the backup is initiated over one B channel, the second B channel is unavailable. If the backup interface is configured for dialer profiles, both B channels can be used.

Configuration of a Backup Dialer Profile

This topic describes configuring a backup connection to engage when the primary line fails, using dialer profiles. Also described is configuring a backup connection to engage when the primary line reaches a specified load threshold, using dialer profiles.

Configuring a Backup Dialer Profile

Cisco.com

Step 1

Dialer
Pool

```
interface dialer number
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name name
 dialer string string
 dialer pool number
 dialer-group number
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-9-11

A dialer interface can be configured as the logical intermediary between one or more physical interfaces. Another physical interface that is configured to belong to a dialer pool can also be used as the backup interface.

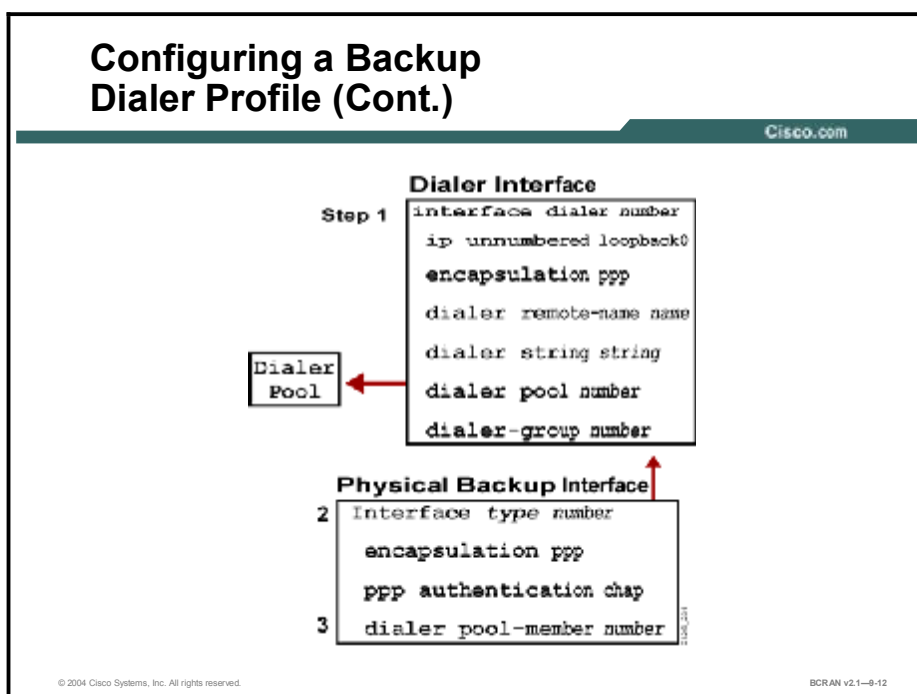
Perform these steps to configure a dialer interface and a specific physical interface to function as a backup to other physical interfaces:

- Step 1** Create and configure a dialer interface as described in Module 7, “Using DDR Enhancements.”

This table reviews how to configure a dialer interface.

Review of Commands for Configuring a Dialer Interface

Command	Description
interface dialer number	Creates a dialer interface
ip unnumbered loopback0	Specifies an IP address for your dialer interface
encapsulation ppp	Specifies PPP encapsulation
dialer remote-name name	Specifies the CHAP authentication name of the remote router
dialer string string	Specifies the remote destination to call
dialer pool number	Specifies the dialer pool to use for calls to this destination
dialer-group number	Assigns the dialer interface to a dialer group



Step 2 Configure the physical BRI interface for ISDN using PPP encapsulation.

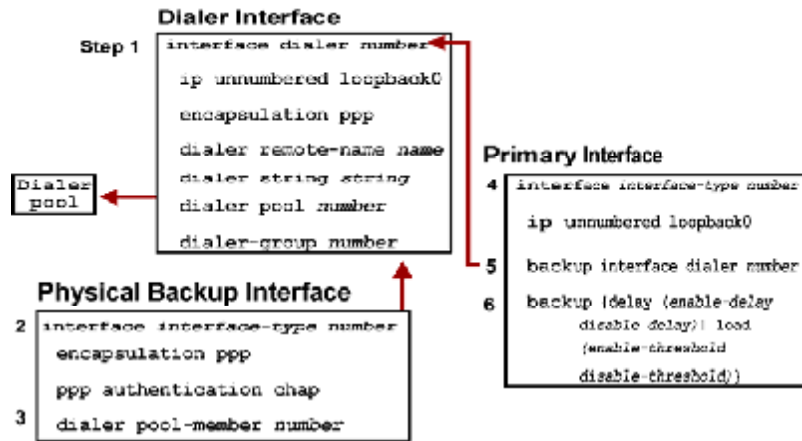
Step 3 Use the **dialer pool-member** *number* command to place the physical BRI interface into the same dialer pool as the backup dialer interface.

dialer pool-member *number* Command

Command	Description
<i>number</i>	Makes the interface a member of the dialer pool. This value must match the appropriate dialer pool number.

Configuring a Backup Dialer Profile (Cont.)

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1--9-13

Now configure the primary interface to use the dialer interface as backup.

- Step 4** Enter interface configuration mode for the primary interface.
- Step 5** Specify the backup interface dialer to be used with the **backup interface dialer number** command.

backup interface dialer *number* Command

Command	Description
<i>number</i>	Specifies the interface or dialer interface to use for backup. Interface number specifications vary from router to router. For example, some routers require you to only specify the port number, while others require you to specify the slot and port.

- Step 6** Specify the delay or the load percent after which the backup engages with the **backup {delay enable-delay disable delay | load enable-threshold disable-threshold}** command.

Dialer Profile Backup Example

This topic describes a backup connection that engages when the primary line fails. This is done using dialer profiles and configuring a backup connection.

Dialer Profile Backup Example

Cisco.com

```
interface dialer 0
ip unnumbered loopback0
encapsulation ppp
dialer remote-name Remote0
dialer pool 1
dialer string 5551212
dialer-group 1

interface bri 0/0
encapsulation ppp
dialer pool-member 1
ppp authentication chap

interface serial 3/1
ip unnumbered loopback0
backup interface dialer 0
backup delay 5 10
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-9-14

The figure shows the configuration of a site that backs up a leased line using a BRI interface. One dialer interface, dialer 0, is defined. The leased line, serial 3/1, is configured to use the dialer interface, dialer 0, as a backup. The dialer interface uses dialer pool 1, which has physical interface bri 0/0 as a member. Thus, physical interface bri 0/0 can back up the serial interface.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Dial backup provides protection against WAN downtime.**
- **DDR backup is a method of bringing up an alternate dialup link should the primary WAN link fail.**
- **When a backup interface is specified on a primary line, the backup interface is placed in standby mode.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-9-15

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Backup interfaces for a primary line can be any of the following, except ____.
- A) an ISDN interface
 - B) an asynchronous interface
 - C) an Ethernet interface
 - D) a dialer pool
- Q2) A secondary backup interface can be configured to activate when any of the following circumstances occur, except when ____.
- A) the primary line load exceeds a specified threshold
 - B) the primary line fails
 - C) the primary line load reaches a specified threshold
 - D) the router hardware fails
- Q3) Which command specifies the interface or dialer interface to use for backup?
- A) **interface number**
 - B) **interface-type number**
 - C) **interface-type**
 - D) **enable-delay**
- Q4) Which command is used to adjust the amount of time that the device waits to bring up the backup interface?
- A) **interface backup**
 - B) **backup interface**
 - C) **delay backup**
 - D) **backup delay**
- Q5) In the command **backup delay 25 40**, how long will it take the backup line to activate if the primary goes down?
- A) 25 seconds
 - B) 40 seconds
 - C) between 25 to 40 seconds
 - D) greater than 40 seconds

- Q6) The software monitors the traffic load and computes a moving average for what period of time?
- A) 200 seconds
 - B) 250 seconds
 - C) 300 seconds
 - D) 350 seconds
- Q7) In the command **backup load 60 5**, when the load is exceeded the secondary line is activated and will not be deactivated until the combined load is _____.
- A) equal to 5 percent of the primary bandwidth
 - B) less than 5 percent of the primary bandwidth
 - C) greater than 60 percent of the primary bandwidth
 - D) equal to 60 percent of the primary bandwidth
- Q8) If a physical link is used as a backup to a primary connection, what mode is it in?
- A) standby mode, and can be used as a link to another site
 - B) active mode, and cannot be used as a link to another site
 - C) active mode, and can be used as a link to another site
 - D) standby mode, and cannot be used as a link to another site
- Q9) Using dialer profiles, a BRI connection can be used for both a backup for a Frame Relay connection and DDR between the branch office and SOHO, provided _____.
- A) the physical BRI interface is a member of both dialer pools and the profile is in active mode
 - B) the physical BRI interface is a member of both dialer pools and the profile is in standby mode
 - C) the physical BRI interface is a member of one of the pools and the profile is in standby mode
- Q10) Which of the following commands is required to set up a dialer profile?
- A) **dialer rotary-group 1**
 - B) **dialer map ip 131.108.2.5 name cisco 5552121**
 - C) **dialer string 5551234**
 - D) **PPP multilink**

- Q11) In which situation would it be advantageous to use dialer profiles over legacy DDR configurations?
- A) One physical interface needs to call multiple sites with the same communication parameters.
 - B) All asynchronous interfaces need to share the same configuration parameters.
 - C) All of the asynchronous interfaces are members of the same hunt group.
 - D) Physical interfaces need to have different characteristics based on incoming or outgoing calls.

Quiz Answer Key

- Q1) C
Relates to: Dial Backup Overview
- Q2) D
Relates to: Dial Backup for High Primary Line Usage
- Q3) B
Relates to: Activation of Backup Interfaces for Primary Line Failures
- Q4) D
Relates to: Activation of Dial Backup
- Q5) A
Relates to: Dial Backup Activation Example
- Q6) C
Relates to: Configuration of Dial Backup for Excessive Traffic Load
- Q7) B
Relates to: Configuration Example of Dial Backup for Excessive Traffic Load
- Q8) D
Relates to: Backup Limitations with Physical Interfaces
- Q9) B
Relates to: Dial Backup with Dialer Profile
- Q10) C
Relates to: Configuration of a Backup Dialer Profile
- Q11) D
Relates to: Dialer Profile Backup Example

Routing with the Load Backup Feature

Overview

This lesson discusses how load sharing and load balancing work with different routing protocols when the load backup feature is enabled.

Relevance

To effectively manage an enterprise network, you must understand how to maintain communication in the event of a primary line failure or add additional bandwidth during times of primary line congestion.

Objectives

Upon completing this lesson, you will be able to:

- Identify bandwidth utilization issues affecting OSPF routing during load sharing when the primary line reaches a specified load threshold
- Identify bandwidth utilization issues affecting EIGRP and static routing during load sharing when the primary line reaches a specified load threshold
- Identify the commands to verify dial backup configuration
- Configure a floating static route as a backup connection that activates upon primary line failures
- Describe how to use dialer watch as a backup connection that activates upon primary line failures
- Configure dialer watch as a backup connection that activates upon primary line failures

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies (CCNAB)* course
- All knowledge presented in the *Interconnecting Cisco Network Devices (ICND)* course

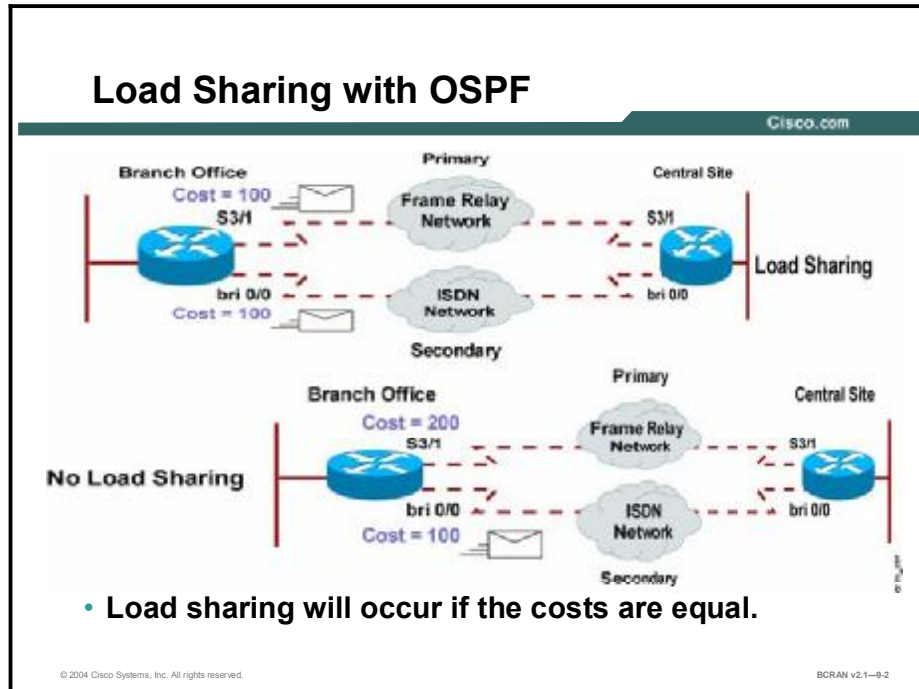
Outline

This lesson includes these topics:

- Overview
- Load Sharing with OSPF and EIGRP
- Verification of Dial Backup Configuration
- Configuration of Floating Static Routes as Backup
- Dialer Watch as Backup
- Configuration of Dialer Watch
- Summary
- Quiz

Load Sharing with OSPF and EIGRP

This topic describes the bandwidth utilization issues affecting Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) routing during load sharing when the primary line reaches a specified load threshold.

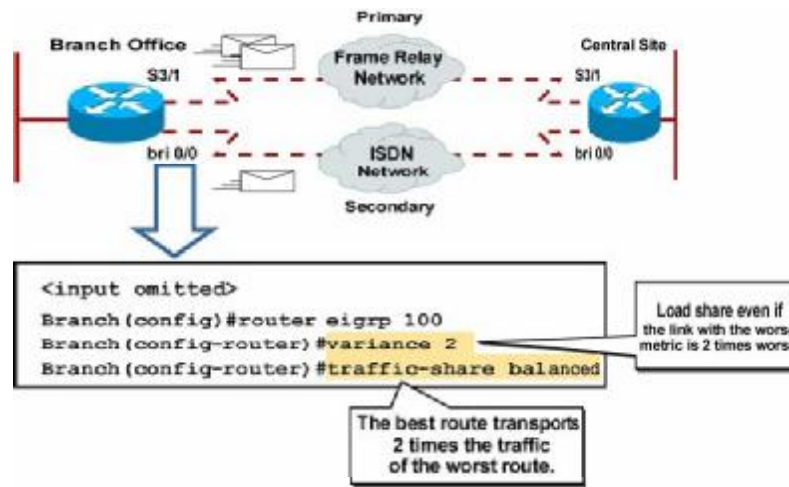


If the OSPF routing protocol is used, the load backup feature load-shares between the primary and backup links after the backup link is activated. However, the cost assigned to the primary link and the backup link must be equal if both links are used. If one link has a lower cost than the other, all routing will occur over the link with the lower cost, even though both lines are up.

OSPF does not support load balancing between the primary link and the backup connection if the links are not equal. If load balancing is to occur in this environment, the backup connection must be able to support comparable bandwidth environments. (For example, a 64-kbps ISDN connection backs up a 64-kbps serial connection.)

Load Sharing with EIGRP

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-9-3

If EIGRP is used, the load backup feature will load-share between the primary and backup links after the backup link is activated. However, the metric assigned to the primary link and the backup link must be equal if both links are to be used. If one link has a lower metric than the other, all routing will occur over the link with the lower metric even though both lines are up. If load balancing is to occur in this environment, each connection must be able to support comparable bandwidth environments. (For example, a 64-kbps ISDN link backs up a 64-kbps serial connection.)

Instead of relying on equal metrics to load-share and load-balance, the **variance** configuration command can also be used to control load balancing in an EIGRP environment. Use the **variance multiplier** command to configure unequal-cost load balancing by defining the difference between the best metric and the worst acceptable metric. An oversimplified explanation is that a router can use paths with worse routing metrics up to a value less than the current best route metric times the variance.

variance multiplier Command

Command	Description
<i>multiplier</i>	The range of metric values that will be accepted for load balancing. Acceptable values are nonzero, positive integers. The default value is 1, which means equal-cost load balancing. In the example, the multiplier is set to 2.

Setting this value lets the router determine the feasibility of a potential route.

If the following two conditions are met, the route is deemed feasible and can be added to the routing table for load sharing:

- Local best metric (current FD) > best metric (AD) learned from the next router. This condition exists if the next router in the path is closer to the destination than the current router. This approach prevents routing loops.
- The variance number multiplied by the local best metric (current FD) > metric (FD) through the next router. This condition is true if the metric of the alternate path is within the variance.

In the figure, the **variance 2** command specifies to use both paths even if the metric of the backup path is two times worse than the primary path.

You can use the **traffic-share {balanced | min}** command to control how traffic is distributed among EIGRP load-sharing routes. The default is four routes and the maximum is six routes.

The **traffic-share balanced** command distributes traffic proportionally to the ratios of the metrics. As a result of the **variance 2** command, the best route will transport two times the traffic of the worst route. The **traffic-share min** command specifies to use routes with the least cost.

Note Advertisable distance (AD) is the metric that a neighbor uses to reach a given destination network. The AD is advertised as part of the EIGRP update for a given network. A router receiving the update adds its cost to reach that neighbor to the AD. The sum of these values provides the feasible distance (FD) to reach that destination network through that neighbor router.

Verification of Dial Backup Configuration

This topic describes the commands that are used to verify dial backup configuration.

Verifying the Dial Backup Configuration

Cisco.com

Primary Interface

```
Router#show interface s 3/1.1
Serial3/1.1 is up, line protocol is up
Hardware is CD2430 in sync mode
Internet address is 10.1.4.1/24
Backup interface Dialer1, failure delay 20 sec, restore delay 40 sec
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY
<Output Omitted>
```


Backup Interface

```
Router#show interface dialer 1
Dialer1 is standby mode, line protocol is down
Hardware is Unknown
Internet address is 10.1.5.1/24
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
<Output Omitted>
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-94

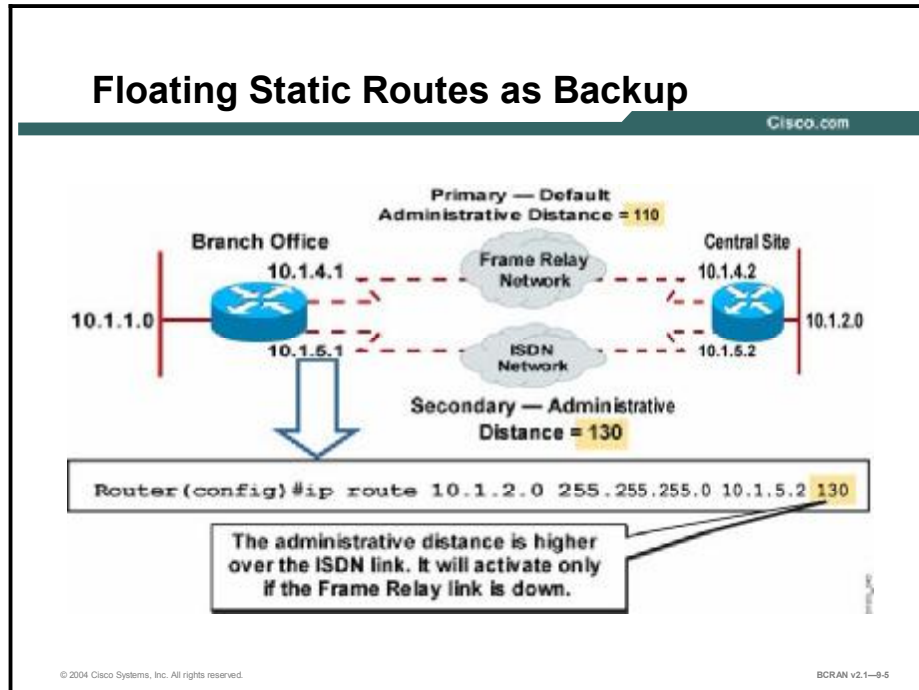
To verify a backup line link for a primary line connection, enter the **show interface *type number*** command.

The primary interface output in the figure illustrates that dialer 1 is specified as a backup if the serial subinterface 3/1.1 fails. If the line protocol on the subinterface goes down because of the Local Management Interface (LMI) state changing from ACTIVE to INACTIVE or DELETED, the backup will be enabled 20 seconds later. The backup will deactivate 40 seconds after the serial subinterface reactivates.

The backup interface output shows the backup link in standby mode until the primary line subinterface line protocol goes down.

Configuration of Floating Static Routes as Backup

This topic describes configuring a floating static route as a backup connection that activates upon primary line failures.



Floating static routes are static routes that have an administrative distance greater than the administrative distance of dynamic routes. The administrative distance can be configured on a static route so that the static route is less desirable than a dynamic route, and the static route is not used when the dynamic route is available. However, if the dynamic route is lost, the static route can take over and traffic can be sent through this alternate route. If the alternate route is provided by a DDR interface, the DDR can then be used as a backup mechanism.

Note The administrative distance values of some common Interior Gateway Routing Protocols (IGRPs) are: EIGRP: 90, IGRP: 100, OSPF: 110, Routing Information Protocol (RIP): 120, and External EIGRP: 170.

In the previous example, the dynamic primary route to the central site Ethernet network, 10.1.2.0, is over the Frame Relay network, 10.1.4.0. A floating static route over the ISDN network, 10.1.5.0, is configured with the administrative distance of 130. However, the route over the ISDN network will only be used to get to network 10.1.2.0 if the Frame Relay network is down because the administrative distance is set higher on the ISDN connection.

Floating static routes are independent of line protocol status. The line protocol of a Frame Relay multipoint interface may not go down if the PVC becomes inactive. This situation defeats the purpose of configuring backup interfaces. A failed PVC may not bring down a line protocol status; thus, dynamic routes will not be flushed from the routing table. The floating static route with a higher administrative distance will not be installed in the routing table of that router.

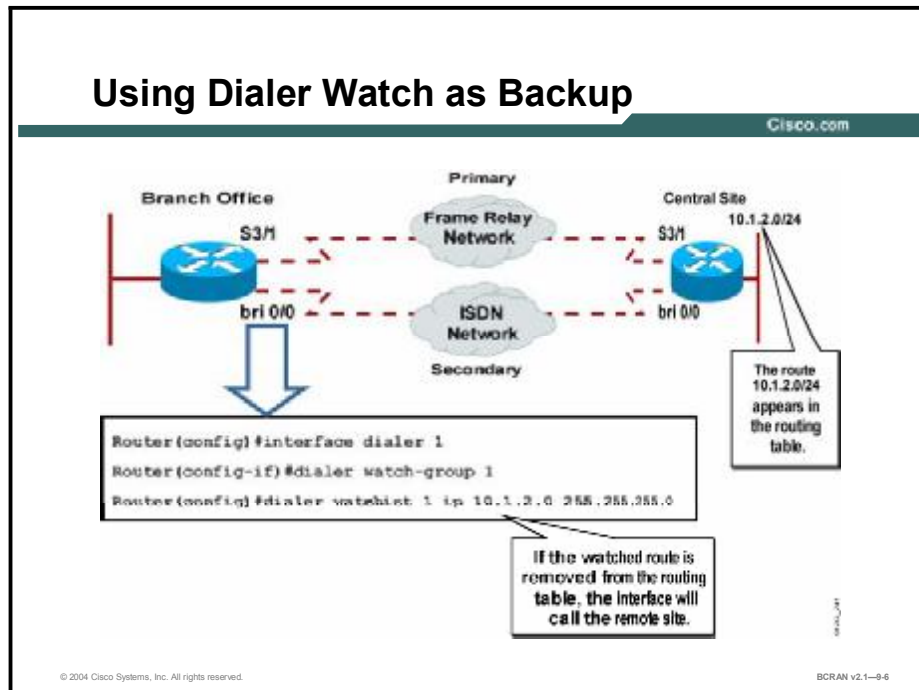
To configure a floating static route, establish a static route for a designated network by specifying a higher administrative distance than that of the dynamic routing protocol. Use the **ip route** command to configure a floating static route. The **ip route** command arguments are listed in the table.

ip route Command Arguments

Command	Description
<i>Network-number</i>	IP address of the target network or subnet
<i>Network-mask</i>	Network mask that lets you mask network and subnetwork bits
<i>IP address</i>	IP address of the next hop that can be used to reach that network in standard IP address notation. Example 1.1.1.1
<i>Interface</i>	Network interface to use
<i>Distance</i>	(Optional) An administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers

Dialer Watch as Backup

This topic describes how to use dialer watch as a backup connection that activates upon primary line failures.



As an alternative to floating static routes, you can use the **dialer watch** commands. Dialer watch is a backup feature that integrates dial backup with routing capabilities. Dialer watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls to the central site router. Hence, dialer watch can also be considered regular DDR with no requirement for interesting traffic, just lost routes. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted.

The figure shows the configuration of the branch site using dialer watch to monitor the network 10.1.2.0/24 coming from the central site. This network and mask must be an exact match or dialer watch will fail.

With dialer watch, the router monitors the existence of a specified route and if that route is not present, it initiates dialing of the backup link. Unlike the other backup methods (such as backup interface or floating static routes) dialer watch *does not* require interesting traffic to trigger the dial. Instead it triggers a dial backup call when a watched route is deleted from the routing table.

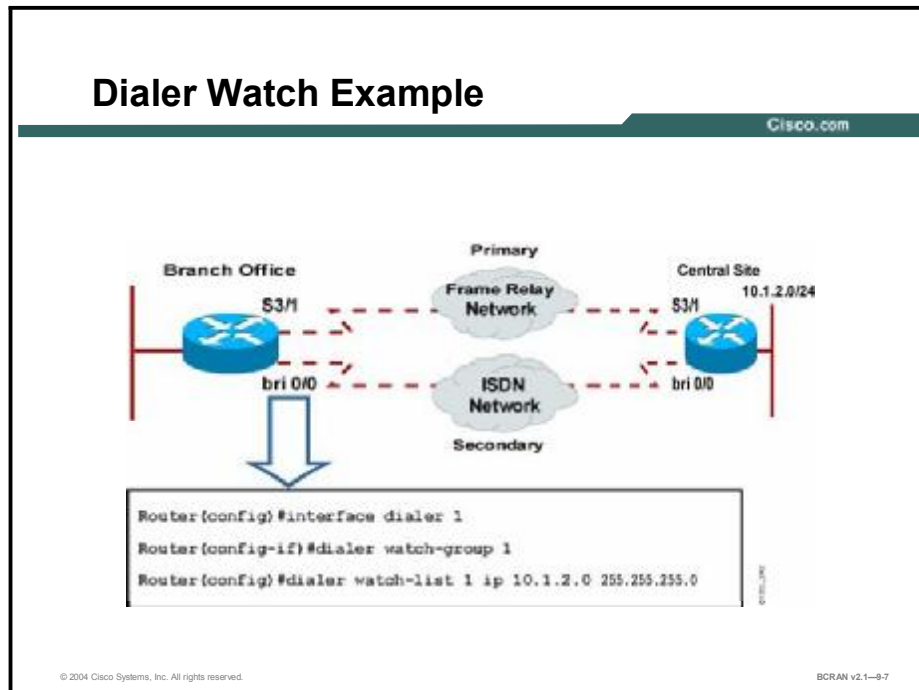
When a monitored network is deleted from the routing table of a dialer watch router, the router checks for another valid route for the lost network. If an alternate valid route using a nonbackup interface exists for a deleted watched network, the primary link is considered active and the backup link is not initiated. However, if there is no valid route, the primary line is considered down and unusable, and the router then initiates a dial backup call. Upon activation of the secondary link, the router forwards all traffic destined for the remote network over the backup link.

After the dial backup link is initialized, the router checks to see if the primary link has been re-established after each idle timeout period. If the router finds that the primary link remains down, the idle timer resets and the backup link remains active. As soon as the primary link is re-established, the router updates its routing table and routes traffic over the primary link. Because traffic is no longer routed over the dialup connection, the backup link deactivates as the idle timeout expires.

Note Dialer watch is supported with IGRP, EIGRP, and OSPF routing protocols only.

Configuration of Dialer Watch

This topic describes how to configure dialer watch as a backup connection that activates upon primary line failures.



Use the three steps below to configure a dialer watch function. The command parameters are described respectively in the tables below.

Step 1 Define the IP addresses or networks to be watched using the **dialer watch-list** *group-number ip ip-address address-mask* command in global configuration mode.

dialer watch-list *group-number ip ip-address address-mask* Command

Command	Description
<i>group-number</i>	Dialer list number
<i>ip-address address-mask</i>	The IP address of the network being watched

Step 2 Enable dialer watch on the backup interface. Use the **dialer watch-group** command in interface configuration mode.

dialer watch-group *group-number* Command

Command	Description
<i>group-number</i>	Dialer watch group number references the dialer list number

Step 3 To set a delay timer on the backup interface to ensure stability for flapping interfaces, use the optional **dialer watch-disable** *seconds* command.

dialer watch-disable *seconds* Command

Command	Description
<i>seconds</i>	Number of seconds to set for the delay timer

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **To effectively manage an enterprise network, you must use the load backup feature to maintain communication in the event of a primary line failure, or add additional bandwidth during times of primary line congestion.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-9-8

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 9-1: Enabling a Backup to a Primary Connection

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) How many links will OSPF load-balance across if the costs are different?
- A) 0
 - B) 1
 - C) 2
 - D) 3
- Q2) Under what conditions will unequal-cost load balancing occur?
- A) The metric assigned to the primary link must be greater than the backup link.
 - B) The metric assigned to the primary link and the backup link must be equal if both links are to be used.
 - C) The metric assigned to the primary link must be less than the backup link.
 - D) There can be no metric assigned to the backup link.
- Q3) What command must be entered to verify a backup line link for a primary line connection?
- A) **show running-config**
 - B) **show version**
 - C) **show startup-config**
 - D) **show interface**
- Q4) Under what conditions is the static route NOT used when the dynamic route is available?
- A) when the static route has an administrative distance greater than the administrative distance of dynamic routes
 - B) when the static route has an administrative distance less than the administrative distance of dynamic routes
 - C) when the static route has an administrative distance equal to the administrative distance of dynamic routes
 - D) when the static route is administratively enabled
- Q5) With **dialer watch**, what causes the router to initiate dialing of the backup link?
- A) The monitored route is not present.
 - B) The monitored route is in active state.
 - C) The monitored route has a higher variance.
 - D) There cannot be a mask on the network address.

- Q6) What is the function of the **dialer watch-list** command?
- A) verifies IP addresses
 - B) defines the networks to be watched
 - C) sets up a list of dialer strings
 - D) all of the above

Quiz Answer Key

- Q1) A
Relates to: Load Sharing with OSPF and EIGRP
- Q2) B
Relates to: Load Sharing with OSPF and EIGRP
- Q3) D
Relates to: Verification of Dial Backup Configuration
- Q4) A
Relates to: Configuration of Floating Static Routes as Backup
- Q5) A
Relates to: Dialer Watch as Backup
- Q6) B
Relates to: Configuration of Dialer Watch

Using QoS in Wide-Area Networks

Overview

This module explains why you may need to implement queuing technologies on your WAN connection. It also describes how to implement the queuing technologies available with Cisco IOS software so you can prioritize traffic over your WAN connection. This module also explains how you can use compression to optimize WAN utilization.

Objectives

Upon completing this module, you will be able to:

- Discuss QoS categories of service models
- Discuss the queuing options available using Cisco IOS software
- Describe where weighted fair queuing can be used and what problems it will solve
- Use Cisco IOS commands to configure weighted fair queuing
- Describe where class-based weighted fair queuing can be used and what problems it can solve
- Use Cisco IOS commands to configure class-based weighted fair queuing
- Describe where low latency queuing can be used and what problems it can solve
- Use Cisco IOS commands to configure low latency queuing
- Use **show** commands to identify queuing anomalies in an operational router
- Verify proper queuing configuration
- Implement compression in the network to optimize throughput

Outline

The module contains these lessons:

- Identifying Quality of Service Models and Tools
- Configuring Congestion Management
- Verifying Congestion Management
- Implementing Link Efficiency

Identifying Quality of Service Models and Tools

Overview

The connection between your network and the service provider network is commonly made with a serial point-to-point connection. This lesson describes the features and components of queuing to assist with traffic management during times of congestion.

Relevance

Before you configure queuing, it is helpful to know the general principles in the context of a WAN.

Objectives

Upon completing this lesson, you will be able to:

- Define and describe the considerations for quality of service
- Discuss QoS service models and mechanisms
- Identify situations where traffic prioritization would be beneficial
- Determine which queuing method best suits a situation
- Specify the queuing options available using Cisco IOS software

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

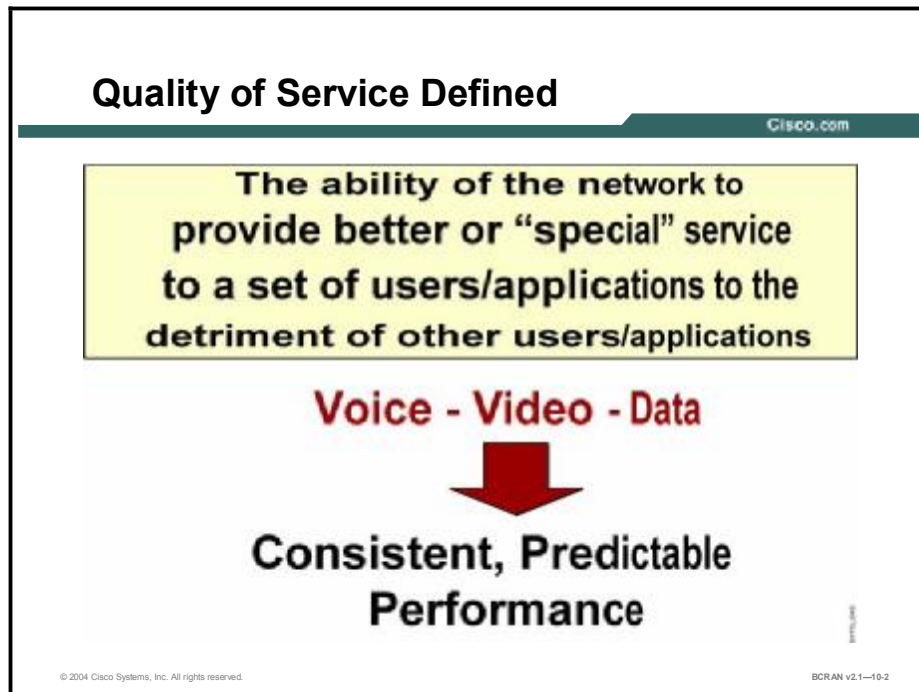
Outline

This lesson includes these topics:

- Overview
- Quality of Service Defined
- Converged Networks: Quality Issues
- QoS Considerations
- QoS Application Requirements
- QoS Models
- QoS Mechanisms
- QoS Mechanisms and Remote Access
- Congestion Avoidance: Random Early Detection
- Congestion Avoidance: Weighted Random Early Detection
- Effective Use of Traffic Prioritization
- Queuing Overview
- Establishing a Queuing Policy
- Cisco IOS Queuing Options
- Link Efficiency Usage
- Summary
- Quiz

Quality of Service Defined

This topic describes the features of quality of service (QoS).



QoS is “the ability of the network to provide better or “special” service to selected users and/or applications to the detriment of other users and/or applications.”

Cisco IOS QoS features enable network administrators to control and predictably service a variety of networked applications and traffic types, thus allowing network managers to take advantage of a new generation of media-rich and mission-critical applications.

The goal of QoS is to provide better and more predictable network service by doing the following:

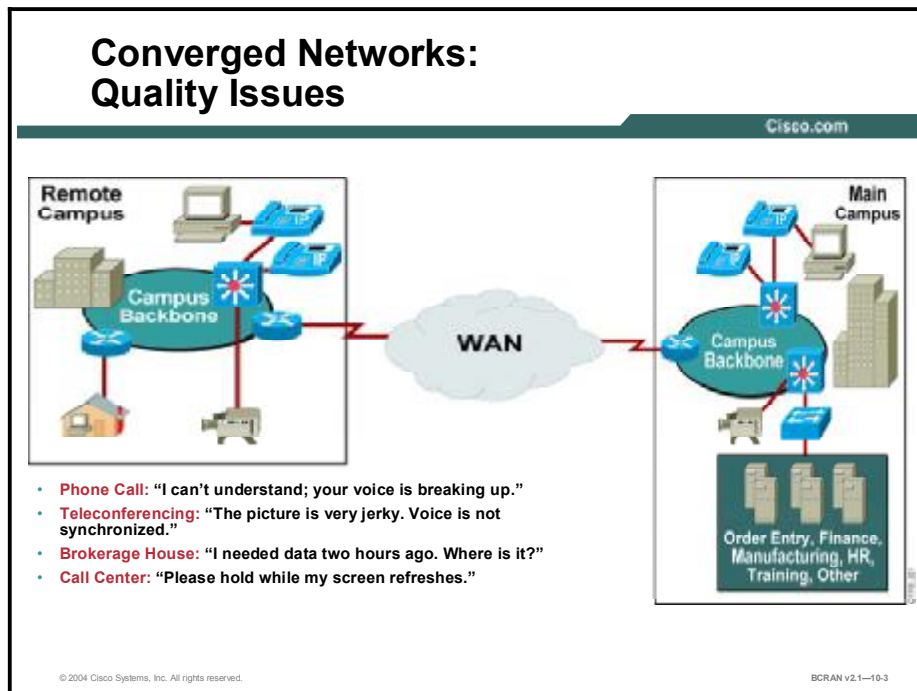
- Providing dedicated bandwidth
- Controlling jitter and latency
- Optimize loss characteristics

QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network.

QoS offers intelligent network services that, when correctly applied, help to provide consistent, predictable performance.

Converged Networks: Quality Issues

This topic describes the types of problems that can occur when you are merging different traffic streams.



A converged network is one in which voice, video, and data traffic use the same network facilities. Merging different traffic streams with dramatically differing requirements can lead to a number of problems.

While packets carrying voice traffic are typically very small, they cannot tolerate delay and delay variation as they traverse the network or voice quality will suffer. Voices will break up and words will become incomprehensible.

On the other hand, packets carrying file transfer data are typically large and can survive delays and drops. It is possible to retransmit part of a dropped file, but it is not feasible to retransmit a part of a conversation.

The constant, but small packet voice flow competes with bursty data flows. Unless some mechanism mediates the overall flow, voice quality will severely degrade at times of network congestion. The critical voice traffic must get priority.

Voice and video traffic are very time-sensitive. They cannot be delayed and they cannot be dropped or the resulting quality of voice and video will suffer.

Finally, a converged network cannot fail. While a file transfer or email packets can wait until the network recovers, voice and video packets cannot. Even a brief network outage on a converged network can seriously disrupt business operations.

Converged Networks: Quality Issues (Cont.)

Cisco.com

- **Packet loss:** Some packets may have to be dropped when a link is congested
- **Delay:**
 - **End-to-end:** Overall delay as packets traverse several devices and links
 - **Jitter:** Adjusting to variable delays from other traffic; causes additional delay
- **Lack of bandwidth:** Multiple flows compete for limited bandwidth

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-4

The three big problems facing converged enterprise networks are packet loss, delays (fixed delay, variable delay, and variation of delay), and lack of sufficient bandwidth capacity.

- **Packet loss:** This usually occurs when a WAN data link is congested. Packet loss can also happen when routers run out of buffer space for a particular interface (output queue) or if the router input queue is full because the main CPU is congested and cannot process packets. Hardware-detected errors in a frame (bad CRC, or runt packet or giant packet) can also cause packet loss.
- **Delay:** This is the time it takes for a packet to reach the receiving endpoint after being transmitted from the sending endpoint-- the "end-to-end delay." It consists of two components: fixed network delay and variable network delay. Jitter is the delta, or difference, in the total end-to-end delay values of two voice packets in the voice flow.

Two types of fixed delay are serialization and propagation delays. Serialization is the process of placing bits on the circuit. The higher the circuit speed, the less time it takes to place the bits on the circuit. Therefore, the higher the speed of the link, the less serialization delay. Propagation delay is the time it takes for frames to transit the physical media.

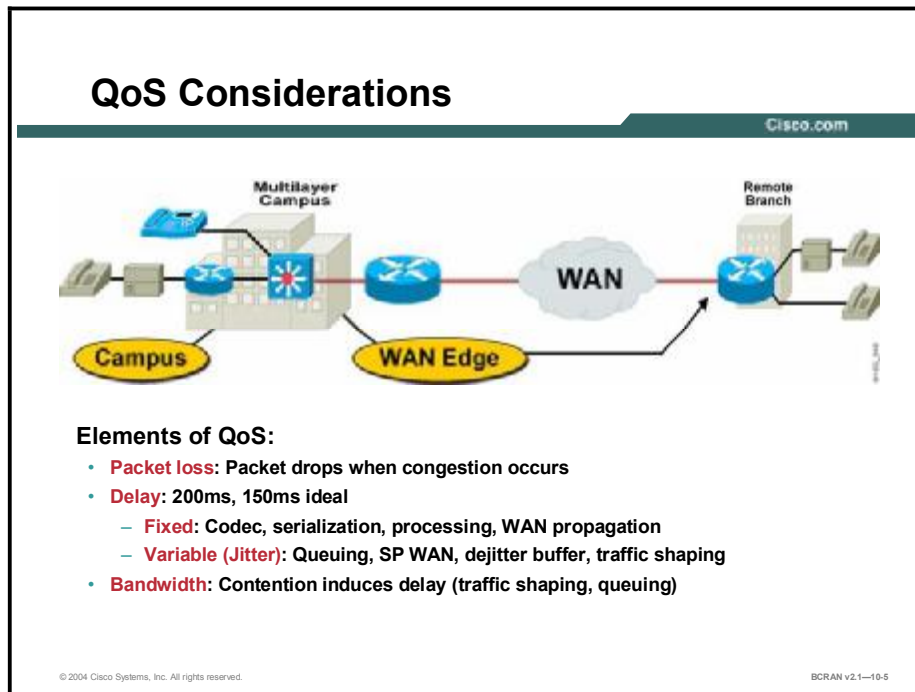
Processing delay is a type of variable delay, and is the time required by a networking device to look up the route, change the header, and complete other switching tasks. In some cases, the packet also must be manipulated. For example, the encapsulation type or the hop count must be changed. Each of these steps can contribute to the processing delay.

- **Lack of bandwidth:** This is insufficient physical capacity of the facility. Until recently, bandwidth was plentiful. But as more applications like IP telephony, videoconferencing, e-learning and mission critical data applications are being implemented lack of bandwidth (among other quality issues) must be addressed. Large graphic files or multimedia with voice and video cause bandwidth capacity problems over data networks.

Calculation of bandwidth is complicated by various multiple flows and the total hops end-to-end. Even with an empty network, the maximum bandwidth available equals the bandwidth of the slowest link.

QoS Considerations

This topic describes the issues that can affect QoS.



There are several areas to be considered when evaluating your QoS.

- **Campus:** On campus there is typically a large bandwidth available, thus minimizing QoS issues on campus.
- **WAN edge:** Often results in slow access links. If less than 2M, QoS techniques are a must to attain acceptable voice quality.
- **WAN considerations:** This area is often forgotten or misunderstood. Speed mismatches; oversubscription; and lack of control over a SP network can have impacts on QoS.

QoS Application Requirements

This topic identifies the varying requirements different applications may have.

Not All Traffic Is Created Equal

Cisco.com

	Voice	Video	Data (Best-Effort)	Mission-Critical Data
Bandwidth	Low to Moderate	Moderate to High	Moderate to High	Low to Moderate
Drop Sensitivity	High	High	High	Moderate to High
Delay Sensitivity	High	High	Low	Moderate to High
Jitter Sensitivity	High	High	Low	Low to Moderate

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-10.6

Each of the various traffic types on modern networks may require a different type of service for the amount of bandwidth required. Different traffic types also vary on how sensitive they are to other transmission quality issues. To be successful, all traffic cannot receive the same service.

Mission-critical data traffic requires different handling than other non-critical data traffic. First come first serve treatment of network traffic may not necessarily handle mission-critical traffic well.

Voice and video traffic are very time-sensitive. This traffic should not be delayed or dropped, or the resulting voice or video fidelity will suffer.

The figure shows how traffic types have the following characteristics:

- Different bandwidth requirements
- Sensitivity to packet drops (and the recovery of any lost packets)
- Sensitivity to end-to-end delay for receiving the packets
- Sensitivity to jitter (variation of that delay)

QoS Models

This topic identifies the three QoS models.

Three Models for Quality of Service

Cisco.com

- **Best Effort (BE):** No QoS is applied to packets
- **Integrated Services (IntServ):** Applications signal that they need QoS to the network
- **Differentiated Services (DiffServ):** The network recognizes classes that require special QoS

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-7

There are three models used to design and implement QoS for a network: Best Effort, Integrated Services, and the Differentiated Services model.

- **Best Effort model:** This model has no applied QoS tools. This model is appropriate if there is enough bandwidth and there is no concern as to when packets arrive or to whom.

This model is easily scalable and requires no special mechanisms. But this model does not allow you to differentiate services, as there are no service guarantees.

- **Integrated Services (IntServ) model:** This model (also known as “Hard QoS”) allows applications to signal the network in advance to request special QoS such as delay or bandwidth. Once the network agrees with the conditions, the traffic cannot be impacted.

Resource Reservation Protocol (RSVP) is commonly used to provide admission control for resources. This protocol includes explicit resource admission control (end to end) per application. This protocol lacks scalability due to the continuous signaling of the stateful architecture and resources used for thousands of per-flow guarantees.

- **Differentiated Services (DiffServ) model:** This model (also known as “Soft QoS”) addresses the limitations of both the Best Effort model and the IntServ model. This model provides a cost effective, “almost guarantee” on a hop-by-hop basis versus end-to-end of IntServ. DiffServ provides QoS by marking packets for special treatment based on groups known as classes. This service is addressed on a hop-by-hop basis versus IntServ’s call admission to guarantee resource end-to-end before packet flows are initiated.

The DiffServ model is highly scalable with many levels of service. But this model also includes complex mechanisms with no absolute service guarantee.

QoS Mechanisms

This topic identifies the mechanisms used to achieve QoS.

An Overview of QoS Mechanisms

Cisco.com

- **Classification:** Each class-oriented QoS mechanism has to support some type of classification
- **Marking:** Used to mark packets based on classification and/or metering
- **Congestion Avoidance:** Used to drop packets early in order to avoid congestion later in the network
- **Congestion Management:** Each interface must have a queuing mechanism to prioritize transmission of packets
- **Policing and Shaping:** Used to enforce a rate limit based on the metering (Example: Frame Relay traffic shaping)
- **Link Efficiency:** Used to improve bandwidth efficiency through compression (or link fragmentation and interleaving)

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10-8

From the moment an IP packet enters the network, it may get the required service needed by the provision of various QoS mechanisms. A packet may be classified and then usually marked with its class identification. From that point on, the packet may be treated by other IP QoS mechanisms, depending on its packet classification. The figure above and the text below outline the main categories of IP QoS mechanisms.

Classification and marking mechanisms identify and split traffic into different classes. Traffic classes get a mark according to the traffic behavior and the intended business policies.

With congestion avoidance various mechanisms discard specific packets based on the markings. These mechanisms attempt to prevent or reduce network congestion.

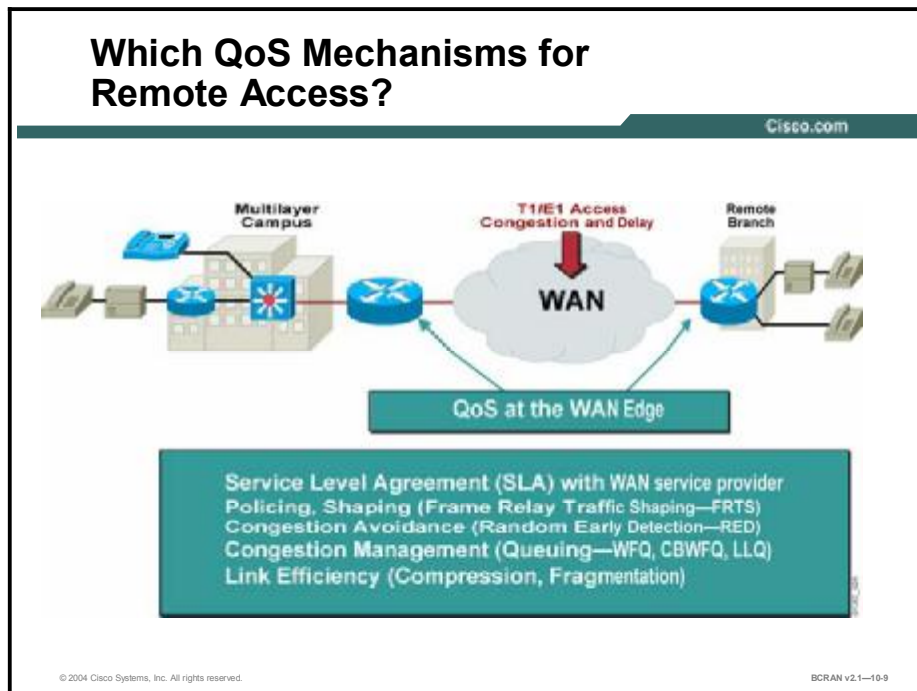
Congestion management mechanisms attempt to prioritize, protect, and isolate traffic based on the markings.

Policing and shaping mechanisms attempt to condition the traffic; policing drops misbehaving traffic to maintain network integrity; shaping controls bursts by queuing network traffic.

Link efficiency mechanisms also provide QoS. One type of link efficiency mechanism is packet header compression to improve the bandwidth efficiency of a link. Another technology is Link Fragmentation and Interleaving (LFI) that can decrease the “jitter” of voice transmission by reducing voice packet delay.

QoS Mechanisms and Remote Access

This topic describes the issues that must be considered when you are applying QoS mechanisms to remote access situations.



To provide end-to-end QoS, both the enterprise and service provider must implement the proper QoS mechanisms to ensure the proper traffic handling across the whole network.

Until recently, IP QoS was not an issue in an enterprise campus network because bandwidth was plentiful. Recent applications such as IP telephony, videoconferencing, e-learning as well as traditional mission-critical data applications have changed the requirement. Now network administrators must address the issues of buffer management and additional bandwidth.

In addition, IP QoS functions such as classification, scheduling, and provisioning are now required within the enterprise to manage bandwidth and buffers to minimize loss, delay, and jitter.

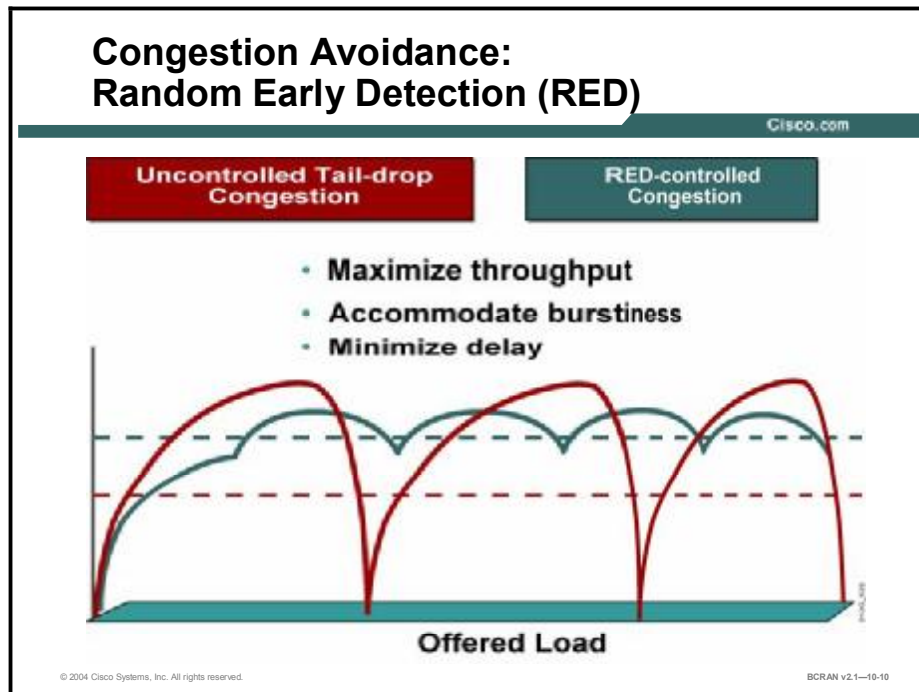
This figure lists some of the requirements within the different building blocks that make up the end-to-end enterprise network.

Most of the more complex QoS configurations of specific interest for remote access occur at the WAN edges. Some QoS tools used specifically at the WAN edge are the following:

- Congestion avoidance using weighted random early detection (WRED)
- Congestion management using queuing
- Link efficiency using compression.

Congestion Avoidance: Random Early Detection

This topic describes the CBWFQ default of using tail drops as a method to avoid congestion.



A router must handle how it queues network traffic to control packet access to the limited network bandwidth. Traffic variations such as packet bursts or flows demanding high bandwidth can cause congestion when packets arrive at an output port faster than they can be transmitted.

The router tries to handle short-term congestion by packet buffering. This absorbs periodic bursts of excessive packets so they can be transmitted later. Although packet buffering has a cost of delay and jitter, packets are not dropped.

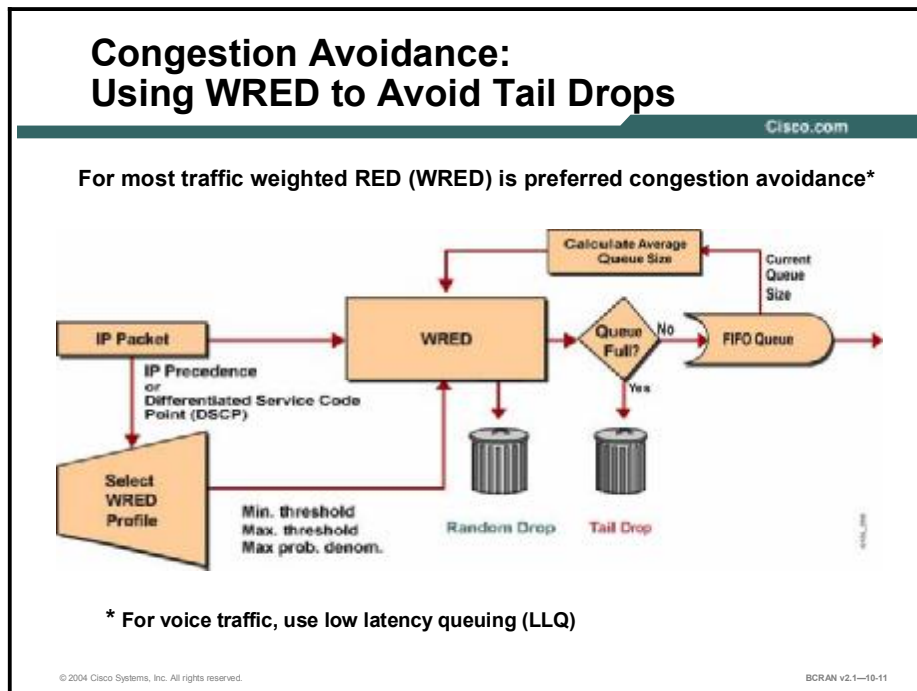
For network traffic causing longer-term congestion, a router using queuing methods faces a need to drop some packets. A traditional strategy is tail drop. With tail drop, a router simply discards a packet when that packet arrives at the tail end of a queue that has completely used up its packet-holding resources. Tail drop is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service (CoS).

Using tail drop, the router drops all traffic that exceeds the queue limit. Many TCP sessions then simultaneously go into slow start (TCP window size reduced). Consequently, traffic temporarily slows down to the extreme. All flows then begin to increase the window size as the congestion is reduced.

This activity creates a condition called global synchronization. Global synchronization occurs when multiple TCP hosts reduce their transmission rates in response to packet dropping, and then increase their transmission rates again when the congestion is reduced. The important point is that the fluctuations of transmission known as global synchronization will result in significant underuse of a link.

Congestion Avoidance: Weighted Random Early Detection

This topic describes WRED as an alternative to tail drops for congestion handling.



The use of tail drops is a passive queue management mechanism. Active queue management mechanisms drop packets before congestion occurs. Larger-scale networks employ algorithms, such as RED, so they can proactively discard packets to prevent (or delay) tail drops.

RED directs one TCP session at a time to slow down, allowing for fuller use of the bandwidth, and it can thereby prevent the traffic crests and troughs from global TCP synchronization.

WRED extends RED functions by permitting more granular RED drop profiles for different types of traffic. WRED combines RED with IP precedence values or with differentiated services code point (DSCP) values. Before tail drops are required, the router can drop packets based on these IP precedence or DSCP markings.

The figure shows how WRED is implemented, and what parameters influence WRED drop decisions. The WRED algorithm is constantly updated with the calculated average queue size, which is based on the recent history of queue sizes.

The configured WRED profiles define the drop thresholds. When a packet arrives at the output queue, the IP precedence or DSCP value is used to select the correct WRED profile for the packet, and the packet is passed to WRED to perform either a drop or enqueue decision.

Based on the profile and the average queue size, WRED calculates the probability for dropping the current packet and either drops it or passes it to the output queue. If the queue is already full, the packet is tail-dropped. Otherwise, it is eventually transmitted out on the interface.

WRED monitors the average queue depth in the router and determines when to begin packet drops based on the queue depth. When the average queue depth crosses the user-specified minimum threshold, WRED begins to drop packets (both TCP and User Data Protocol [UDP]).

If the average queue depth ever crosses the user-specified maximum threshold, then WRED reverts to tail drop, where all incoming packets might be dropped. The idea behind using WRED is to maintain the queue depth at a level somewhere between the minimum and maximum thresholds, and to implement different drop policies for different classes of traffic.

WRED is only useful when the bulk of the traffic is TCP traffic. With TCP, dropped packets indicate congestion, so the packet source reduces its transmission rate. With other protocols, packet sources might not respond or might resend dropped packets at the same rate; therefore dropping packets does not decrease congestion.


WRED can be used wherever there is a potential bottleneck (a congested link) at an access or edge link of the network. It is normally used in the core routers of a network rather than at the edge of the network. Edge routers assign IP precedence to packets as they enter the network. WRED uses these IP precedences to determine how to treat different types of traffic.

Effective Use of Traffic Prioritization

This topic identifies the effective use of traffic prioritization techniques.

Congestion Management: Low-speed Prioritization

Cisco.com



The diagram illustrates a converged network. On the left, three overlapping clouds represent different traffic types: 'File Transfer' (grey), 'Video' (light blue), and 'Voice' (white). These traffic streams enter a blue router labeled 'S0'. A red line representing a WAN link extends from the router to the right, ending at a point labeled 'T1/E1'. The link is shown with a slight zig-zag, indicating a low-speed connection.

- **Prioritization is most effective on bursty WAN links (T1/E1 or below) that experience temporary congestion**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-10-12

The figure shows a converged network in which voice, video, and data file transfers use the same low-speed T1/E1 facilities. Merging these different traffic streams with their respective differing requirements can lead to performance problems. Different types of traffic that share a data path through the network can result in temporary congestion on these data links.

Prioritization may be necessary at the WAN edge congestion points. Prioritization is most effective on WAN links where the combination of bursty traffic and relatively lower data rates can cause temporary congestion. Depending on the average packet size, prioritization is most effective when applied to links at T1/E1 bandwidth speeds or lower.

If there is no congestion on the WAN link, traffic prioritization is not necessary. However, if a WAN link is constantly congested, traffic prioritization may not resolve the problem. Adding bandwidth might be the appropriate solution.

Queuing Overview

This topic describes various queuing options that you can implement.

Congestion Management: Queuing

Cisco.com

- **Prioritizes traffic through router.**
- **Cisco IOS software offers:**
 - **Weighted fair queuing**
 - **Class-based weighted fair queuing**
 - **Low latency queuing**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10-13

A protocol-dependent switching process handles traffic arriving at a router interface. The switching process includes delivery of traffic to an outgoing interface buffer.

FIFO queuing is the classic algorithm for packet transmission. With FIFO, transmission occurs in the same order as messages are received. Until recently, FIFO queuing was the default for all router interfaces. If users require traffic to be ordered differently, they must establish a queuing policy other than FIFO queuing.

In addition to FIFO, Cisco IOS software offers other alternative queuing options:

- **Weighted fair queuing (WFQ):** Prioritizes interactive traffic over file transfers to ensure satisfactory response time for common user applications. WFQ can prioritize traffic based on flows (flow-based WFQ) or user-defined classes (class-based WFQ [CBWFQ]).
- **Class-based weighted fair queuing (CBWFQ) (Cisco IOS Release 12.2)**
- **Low latency queuing (LLQ) (Cisco IOS Release 12.2)**

Establishing a Queuing Policy

This topic describes the considerations for establishing a queuing policy.

Congestion Management: Establishing a Queuing Policy

Cisco.com

The diagram shows a traffic queue on the left with three categories: RTP, SSH, and FTP. These categories are shown entering a blue router. The router's S0 interface is connected to a WAN link labeled 'Bottleneck'.

- **Determines which packets get through first**
- **Helps provide acceptable service levels and control WAN costs**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-10-14

A queuing policy helps network managers meet two challenges: providing an appropriate level of service for all users and controlling expensive WAN costs.

Typically, the corporate goal is to deploy and maintain a single enterprise network that supports a variety of applications, organizations, technologies, and user expectations. Consequently, network managers are concerned with providing all users with an appropriate level of service while continuing to support mission-critical applications and planning for integration of new technologies.

Because the major cost of running a network is also related to WAN circuit charges, network managers balance the capacity and cost of these WAN circuits with an acceptable level of service for their users.

To meet these challenges, queuing allows network managers to prioritize, reserve, and manage network resources, and to ensure the seamless integration and migration of disparate technologies without unnecessary costs.

In the above example, three types of traffic are vying for access to the WAN, because of limited bandwidth. These three types of traffic are as follows:

- **RTP (Real-Time Transport Protocol):** RTP is used to carry multimedia application traffic, including packetized audio and video, over an IP network.
- **SSH (Secure Shell Protocol):** SSH is a secure application used for logging into a remote device, executing commands on a remote device, and moving files from remote device to remote device.
- **FTP:** FTP is a standard protocol in the TCP/IP suite of protocols used to transfer files from one device to another.

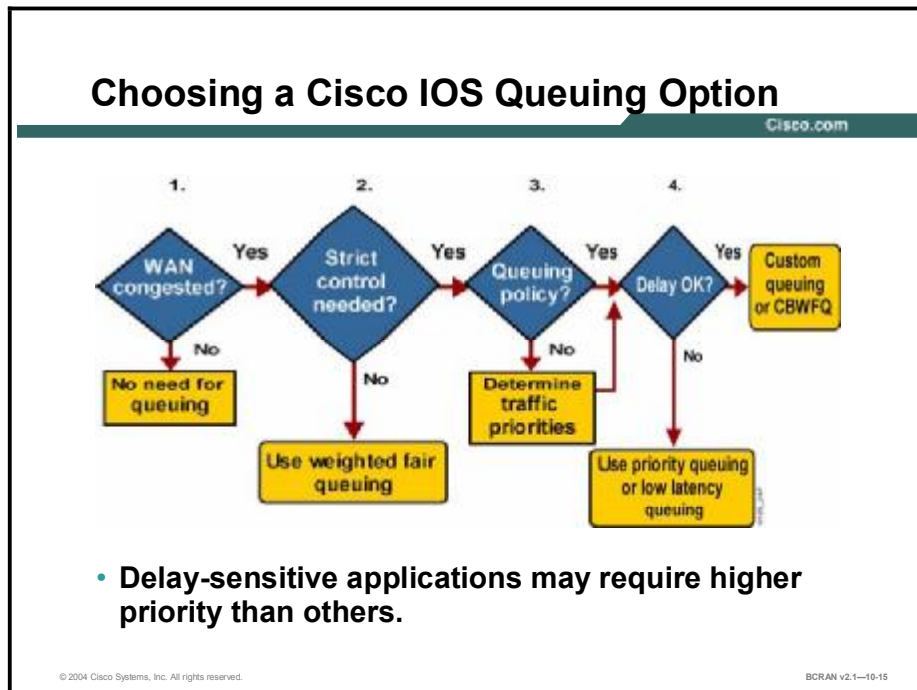
The network administrator needs to determine the priority of each of these traffic types based on the network policy. The administrator then needs to apply the appropriate queuing technique to ensure that each type of traffic is treated according to the policy.

It is likely the administrator prioritizes the RTP traffic first. Due to the delay-sensitive nature of voice and video traffic, the SSH traffic is prioritized second. The FTP traffic is third.

The queuing mechanism used to do this is dependent on the relative importance of each type of traffic, the volume of traffic, and available bandwidth.

Cisco IOS Queuing Options

This topic describes the steps necessary to correctly choose a Cisco IOS queuing option.



Complete these steps when you are choosing a Cisco IOS queuing option:

Step 1 Determine whether the WAN is congested.

If traffic does not back up, there is no need to prioritize it. The traffic is serviced as it arrives. However, if the load exceeds the transmission capacity for periods of time, you may want to prioritize the traffic with one of the Cisco IOS queuing options.

Step 2 Decide whether strict control over traffic prioritization is necessary and whether automatic configuration is acceptable.

Proper queuing configuration is a nontrivial task. The network manager must study the traffic types traversing the interface, determine how to classify them, and decide on their relative priority. The manager must install the filters and test their effect on the traffic. Traffic patterns change over time, so the analysis must be repeated periodically.

Step 3 Establish a queuing policy.

A queuing policy results from the analysis of traffic patterns and the determination of relative traffic priorities discussed in Step 2.

Step 4 Determine whether any of the traffic types identified in your traffic pattern analysis can tolerate a delay. Typically, voice and video have the lowest tolerance for delay.

The table illustrates the typical queuing options a network administrator would choose from when determining how to best implement a queuing policy.

Queuing Options

Queuing Type	Description
FIFO	FIFO queuing is simply sending packets out of an interface in the order in which they arrived.
PQ	Priority queuing (PQ) defines four priorities of traffic—high, normal, medium, and low—on a given interface. As traffic comes into the router, it is assigned to one of the four output queues. Packets on the highest-priority queue are transmitted first; packets on the next highest-priority queue are transmitted second; and so on.
CQ	Custom queuing (CQ) reserves a percentage of bandwidth for specified protocols. Up to 16 output queues can be configured for normal data and an additional queue can be created for system messages such as LAN keepalives. Each queue is serviced sequentially, by transmitting a configurable percentage of traffic and then moving on to the next queue.
WFQ	WFQ provides traffic management that dynamically prioritizes traffic into conversations, or flows, based on Layer 3 or 4 information. It then breaks up a stream of packets within each conversation to ensure that bandwidth is shared equally between individual conversations.
CBWFQ	CBWFQ defines traffic classes, typically using access control lists (ACLs), and then applies parameters, such as bandwidth and queue-limits, to these classes. The bandwidth assigned to a class is used to calculate the "weight" of that class. The weight of each packet that matches the class criteria is also calculated. WFQ is then applied to the classes, which can include several flows, rather than to the flows themselves.
LLQ	LLQ provides strict PQ for CBWFQ, reducing jitter in voice conversations. Strict PQ gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. Low latency queuing is also called PQ/CBWFQ because it is a combination of the two techniques.

Link Efficiency Usage

This topic identifies two link efficiency mechanisms.

Link Efficiency Usage and Tool Categories

Cisco.com

- **Use link efficiency:**
 - For low speed links (768kbps or less)
 - When mixing large data MTU with smaller real time packets
- **Two categories of tools for link efficiency:**
 - Fragmentation/interleaving
 - Compression (Header compression or data compression)

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-16

Link-efficiency mechanisms work best on low speed data links that have large MTU data packets as well as interactive traffic such as Telnet and Voice over IP (VoIP).

Cisco IOS QoS software offers two link efficiency mechanisms that work in conjunction with queuing and traffic shaping to manage existing bandwidth more efficiently and predictably:

- **Link Fragmentation and Interleaving (LFI):** The network fragments data packets and interleaves voice packets to improve the link efficiency.
- **Compressed Real-Time Protocol (CRTP):** The network protocol improves link efficiency as it compresses headers to reduce the overhead of converged traffic.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Quality of Service is “the ability of the network to provide better or ‘special’ service to selected users and/or applications to the detriment of other users and/or applications.”**
- **A converged network is one in which voice, video, and data traffic use the same network facilities.**
- **The three quality of service models are Best Effort, IntServ and DiffServ.**
- **For QoS at the WAN Edge, consider WRED, congestion management and link efficiency mechanisms.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-17

Summary (Cont.)

Cisco.com

- **To provide end-to-end QoS, the enterprise and service providers must implement the proper QoS mechanisms.**
- **Active queuing management mechanisms drop packets before congestion occurs.**
- **First-in-first-out (FIFO) queuing is the classic algorithm for packet transmission.**
- **The queuing options preferred for remote access are WFQ, CBWFQ and LLQ.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-18

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which of the following is true of voice traffic?
- A) can tolerate delays
 - B) is time-sensitive
 - C) can wait until a network recovers
 - D) is typically very large
- Q2) Video has what kind of bandwidth requirement?
- A) average
 - B) moderate to high
 - C) moderate to low
 - D) low
- Q3) Which quality of service model allows applications to signal the network in advance to request special QoS?
- A) Best Effort
 - B) Integrated Services
 - C) Differentiated Services
- Q4) Which QoS mechanism drops packets early in order to prevent congestion later in the network?
- A) classification
 - B) marking
 - C) congestion avoidance
 - D) congestion management
- Q5) What is it called when multiple TCP hosts reduce their transmission rates in response to packet dropping, and then increase their transmission rates again when congestion is reduced?
- A) global synchronization
 - B) global packeting
 - C) packet buffering
 - D) load balancing
- Q6) Prioritization may be necessary in which location?
- A) campus
 - B) end-to-end points
 - C) WAN edge congestion points

- Q7) Which queuing option is NOT an alternative to FIFO queuing on Cisco routers?
- A) weighted fair queuing
 - B) class-based weighted fair queuing
 - C) traffic-rate queuing
 - D) custom queuing
- Q8) Depending on the average packet size, prioritization is most effective when applied to links at _____.
- A) ISDN BRI bandwidth speeds or higher
 - B) T1/E1 bandwidth speeds or lower
 - C) 56 kbps bandwidth speeds or lower
 - D) OC-3 bandwidth speeds or higher
- Q9) Which factors must a network manager consider when establishing a queuing policy?
- A) providing an appropriate level of service for all users
 - B) controlling expensive WAN costs
 - C) A and B
 - D) none of the above
- Q10) Which queuing method would work best on congested WAN links where delay is a concern?
- A) WFQ
 - B) CQ
 - C) LLQ
 - D) CBWFQ

Quiz Answer Key

- Q1) B
Relates to: Converged Networks: Quality Issues
- Q2) B
Relates to: QoS Application Requirements
- Q3) B
Relates to: QoS Models
- Q4) C
Relates to: QoS Mechanisms
- Q5) A
Relates to: Congestion Avoidance: Random Early Detection
- Q6) C
Relates to: Effective Use of Traffic Prioritization
- Q7) C
Relates to: Queuing Overview
- Q8) B
Relates to: Effective Use of Traffic Prioritization
- Q9) C
Relates to: Establishing a Queuing Policy
- Q10) C
Relates to: Cisco IOS Queuing Options

Configuring Congestion Management

Overview

This lesson describes class-based weighted fair queuing (CBWFQ) operation as compared to flow-based weighted fair queuing (WFQ). It also describes the congestion handling technique of tail drops and how these can cause the problem of global synchronization. The lesson finishes with the CBWFQ option of using weighted random early detection (WRED) to actively manage queuing and congestion avoidance.

Relevance

Managing network performance is crucial in the bandwidth-demanding applications of today. CBWFQ is one popular method of managing bandwidth over a WAN. A basic introduction to queuing using techniques that minimize or eliminate tail drops can enable a better understanding of QoS alternatives.

Objectives

Upon completing this lesson, you will be able to:

- Describe a situation where WFQ would be appropriate
- Configure WFQ using Cisco IOS commands
- Describe the operations concept of CBWFQ
- List the benefits of CBWFQ over WFQ
- Describe the configuration that is required to define traffic classes and to specify classification policy
- Configure policies to be applied to packets belonging to one of the classes previously defined through a class map
- Configure CBWFQ with WRED
- Configure a CBWFQ default class
- Configure low latency queuing with the use of the **priority** command for a policy-map class

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

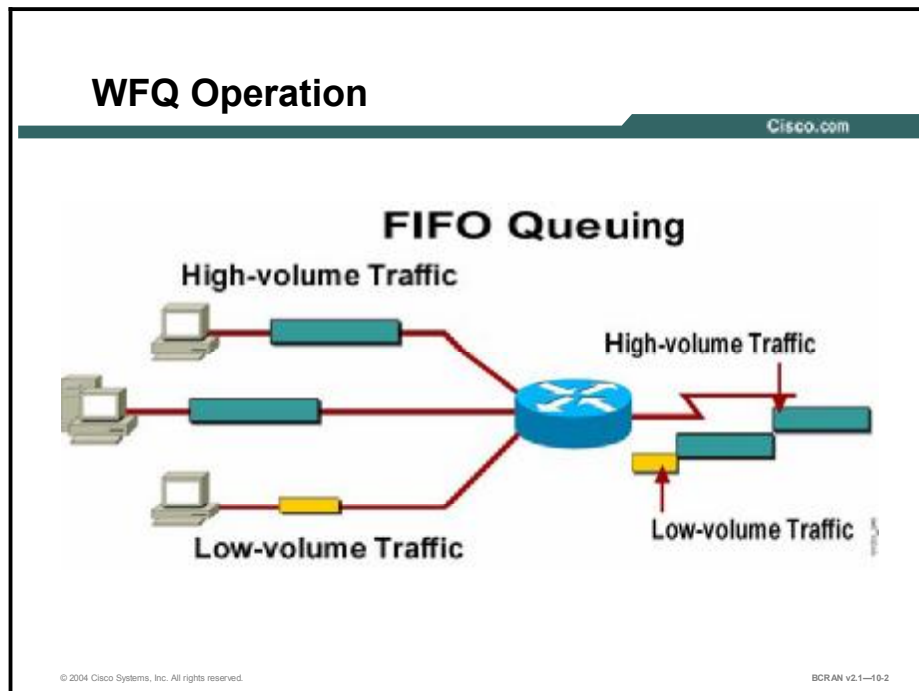
Outline

This lesson includes these topics:

- Overview
- WFQ Operation
- Configuring WFQ
- WFQ Example
- CBWFQ Operation
- CBWFQ vs. Flow-Based WFQ
- Step 1: Configuring CBWFQ
- Step 2a: Configuring CBWFQ with Tail Drop
- Step 2b: Configuring CBWFQ with WRED
- Step 2c: Configuring CBWFQ Default Class (Optional)
- Step 3: Configuring CBWFQ
- CBWFQ Example
- LLQ Operation
- Configuring LLQ
- Summary
- Quiz

WFQ Operation

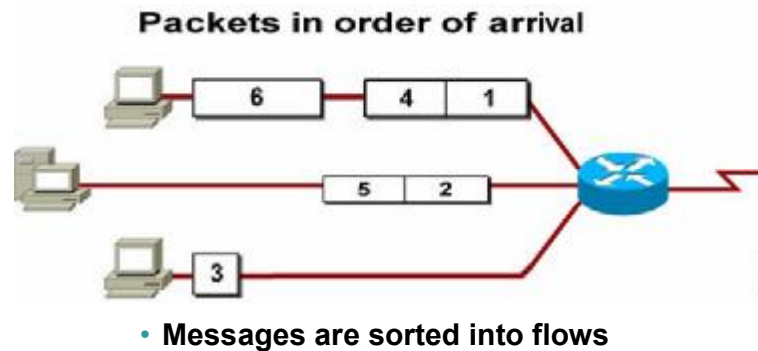
This topic describes an overview of weighted fair queuing (WFQ) and its importance during times of WAN congestion.



When FIFO queuing is in effect, traffic is transmitted in the order received without regard for bandwidth consumption or the associated delays. File transfers and other high-volume network applications often generate a series of packets of associated data known as packet trains. Packet trains are groups of packets that tend to move together through the network. These packet trains can consume all available bandwidth and other traffic flows can back up behind them.

WFQ Operation (Cont.)

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1--10-3

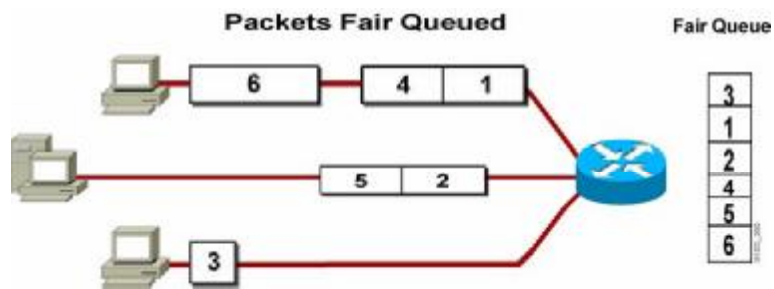
WFQ overcomes an important limitation of FIFO queuing. It is an automated method that provides fair bandwidth allocation to all network traffic. It provides traffic management that dynamically prioritizes traffic into conversations, or flows. WFQ then breaks up a stream of packets within each conversation to ensure that bandwidth is shared fairly between individual conversations. There are four types of WFQ: flow-based, distributed, class-based, and distributed class-based.

WFQ is a flow-based algorithm that moves delay-sensitive traffic to the front of a queue to reduce response time, and shares remaining bandwidth fairly among high-bandwidth flows. By breaking up packet trains, WFQ assures that low-volume traffic is transferred in a timely fashion. WFQ gives low-volume traffic, such as Telnet sessions, priority over high-volume traffic, such as FTP sessions. It gives concurrent file transfers a balanced use of available bandwidth. WFQ automatically adapts to changing network traffic conditions.

WFQ is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps.

WFQ Operation (Cont.)

Cisco.com



- Flows are assigned a channel.
- Sorts the queue by order of the last bit crossing its channel.

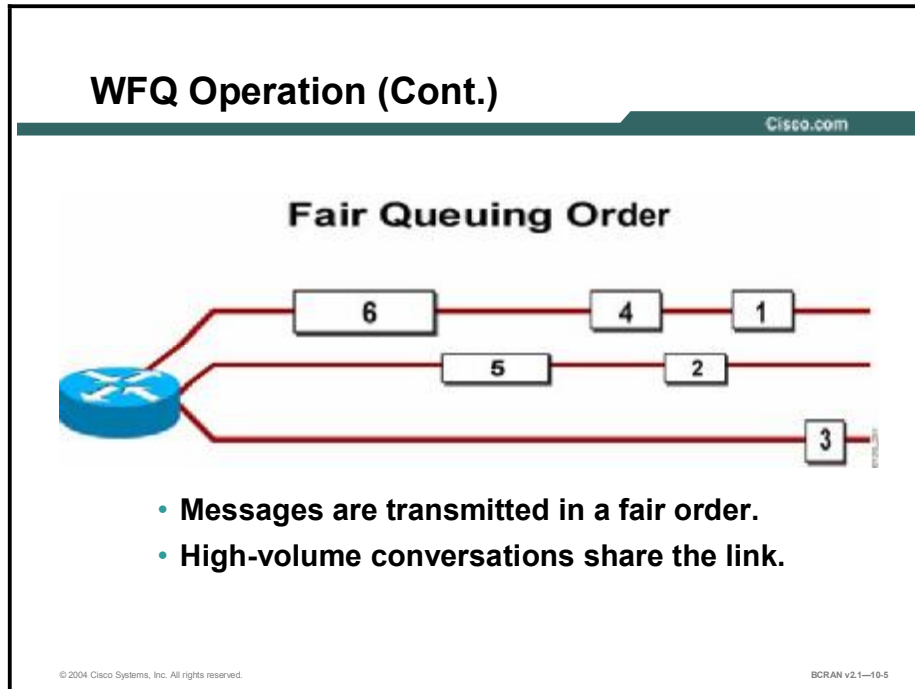
© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-4

The WFQ algorithm arranges traffic into conversations, or flows. The sorting of traffic into flows is based on packet header addressing. Common conversation discriminators are as follows:

- Source or destination network address
- Source or destination MAC address
- Source or destination port or socket numbers
- Frame Relay data-link connection identifier (DLCI) value
- Quality of service (QoS) or type of service (ToS) value

In the figure, the WFQ algorithm has identified three flows.



The flow-based WFQ algorithm places packets of the various conversations in the fair queue before transmission. The order of removal from the fair queue is determined by the virtual delivery time of the last bit of each arriving packet.

WFQ assigns a weight to each flow, which determines the transmit order for queued packets. In this scheme, lower weights are served first. Small, low-volume packets are given priority over large, high-volume conversation packets.

After low-volume conversations have been serviced, high-volume conversations share the remaining link capacity and interleave or alternate transmission timeslots. In this figure, high-volume conversation packets are queued in order of arrival after the low-volume packet.

The queuing algorithm ensures the proper amount of bandwidth for each datagram. With flow-based WFQ, two equal-size file transfers get equal bandwidth, rather than the first file transfer using most of the bandwidth. Although the flow-based WFQ algorithm allocates a separate queue for each conversation, each queue can belong to one of only seven priority classifications, based on the IP precedence.

In the example, packet 3 is queued before packets 1 or 2 because packet 3 is a small packet in a low-volume conversation.

The result of the queuing order and the transmission order is that short messages that do not require much bandwidth are given priority and transmitted on the link first. For example, packet 3 before packets 1 and 2.

Configuring WFQ

This topic describes how to configure WFQ on an interface.

Configuring WFQ

Cisco.com

```
Router(config-if)#fair-queue {congestive-discard-threshold}
```

- Enables WFQ

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-10-6

The **fair-queue** command enables WFQ on an interface.

fair-queue Command

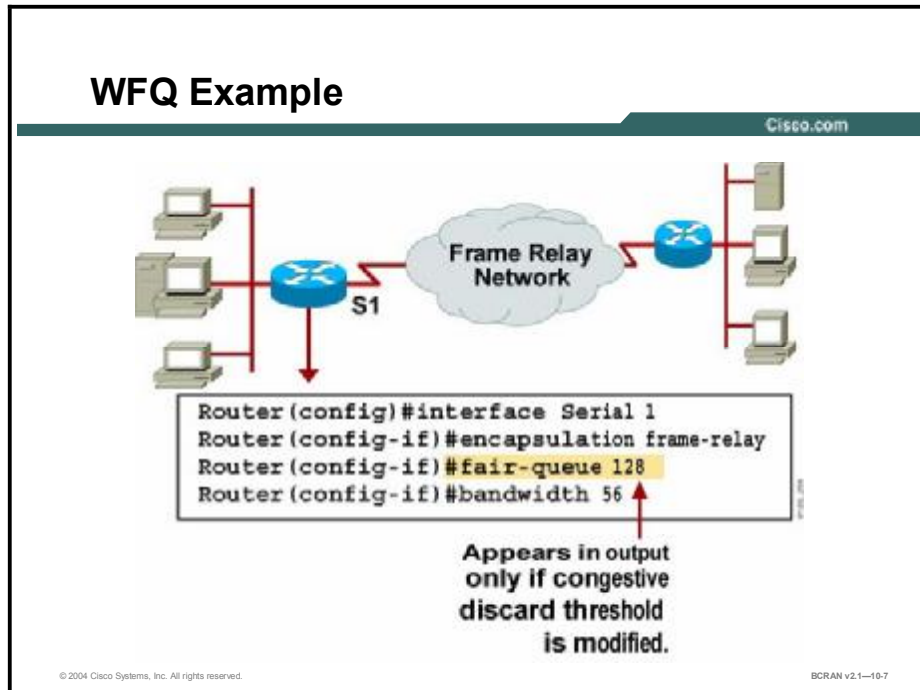
Command	Description
<i>congestive-discard-threshold</i>	The number of messages creating a congestion threshold after which messages for high-volume traffic will no longer be queued. It is the maximum number of packets in a conversation held in a queue before they are discarded. Valid values are 1 to 512, inclusive. The default is 64 messages. The fair-queue 128 command sets the <i>congestive-discard-threshold</i> to 128. <i>congestive-discard-threshold</i> is an optional command. It is not required, as indicated by the braces {} in the figure.

The congestive discard policy applies only to high-volume conversations that have more than one message in the queue. The discard policy tries to control conversations that would monopolize the link. If an individual conversation queue contains more messages than the congestive discard threshold, that conversation will not have any new messages queued until the content of that queue drops below one-fourth of the congestive discard value.

Note WFQ is used by default on serial interfaces at E1 speeds (2.048 Mbps) and below. WFQ is disabled on serial interfaces using X.25 or compressed PPP. LAN interfaces and serial lines operating at E3 or T3 speeds do not support WFQ.

WFQ Example

This topic describes WFQ being used on a Frame Relay network to enable interactive traffic to flow during times of congestion.

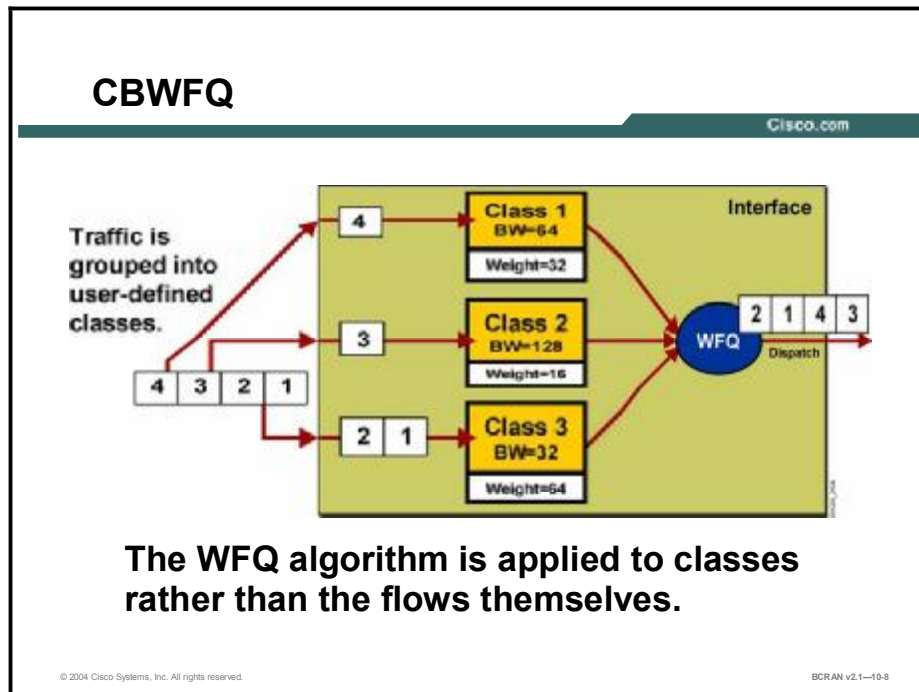


In the figure, interface Serial 1 is attached to a Frame Relay network and is configured to operate at a 56-kbps link speed. The **fair-queue 128** command sets the congestive discard threshold to 128.

Because conversations may not have any new messages queued until the queue content drops below one-fourth of the congestive discard value, a queue must contain fewer than 32 entries (one-quarter of 128).

CBWFQ Operation

This topic describes class-based weighted fair queuing (CBWFQ).



CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. By using CBWFQ, network managers can define traffic classes based on several match criteria, including protocols, ACLs, and input interfaces. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. More than one flow, or conversation, can belong to a class.

After a class has been defined according to its match criteria, you can assign its characteristics. To characterize a class, you assign it bandwidth and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth given to the class during congestion.

CBWFQ assigns a weight to each configured class instead of each flow. This weight is proportional to the bandwidth that is configured for each class ($\text{weight} = \text{interface bandwidth} / \text{class bandwidth}$). Therefore, the larger the bandwidth value of a class, the smaller its weight.

By default, the total amount of bandwidth allocated for all classes must not exceed 75 percent of the available bandwidth on the interface. The other 25 percent is used for control and routing of traffic. However, the maximum-reserved bandwidth can be configured to circumvent this limitation.

You must also specify the queue limit for the class, which is the maximum number of packets allowed to accumulate in the queue for the class. Packets belonging to a class are subject to the bandwidth and queue limits that are configured for the class.

CBWFQ vs. Flow-Based WFQ

This topic describes the benefits of CBWFQ over WFQ.

CBWFQ vs. Flow-Based WFQ

Cisco.com

- **CBWFQ provides for up to 64 classes; flow-based WFQ is limited to 7 classifications, or weights.**
- **CBWFQ allows for coarser granularity. Multiple IP flows can belong to a single class.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-9

CBWFQ offers these benefits over flow-based WFQ:

- **Bandwidth allocation:** CBWFQ allows you to specify the exact amount of bandwidth to be allocated for a specific class of traffic. You can configure up to 64 classes and control distribution among them.

Note This is not the case with flow-based WFQ. Flow-based WFQ applies weights to traffic and classifies traffic into conversations, thus controlling how much bandwidth each conversation is allocated relative to other conversations. For flow-based WFQ, these weights and traffic classifications are limited to the seven IP precedence levels.

- **Finer granularity and scalability:** CBWFQ allows you to define classification based on more criteria. It allows you to use ACLs, protocols, and input interface names to define how traffic will be classified, thereby providing finer granularity. You can configure up to 64 discrete classes in a service policy.

Step 1: Configuring CBWFQ

This topic describes the configuration required to define traffic classes and to specify classification policy.

Step 1: Configuring CBWFQ

Cisco.com

```
Router(config)#class-map class-map-name
Router(config-cmap)#match access-group {access-
    group | name access-group-name}
    or
Router(config-cmap)#match input-interface
    interface-name
    or
Router(config-cmap)#match protocol protocol
    or
Router(config-cmap)#match ip precedence tos
```

- Use only one match command with each class-map.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-10

These are the steps involved in the CBWFQ configuration process:

- Step 1** Define traffic classes to specify the classification policy (class maps).
- Step 2** Associate policies, or class characteristics, with each traffic class (policy map).
 - A: CBWFQ with tail drop
 - or
 - B: CBWFQ with WRED
 - C: Optional: Default Class
- Step 3** Attaching policies to interfaces (service policies).

This process determines how many types of packets are to be differentiated from one another.

To create a class map, use the **class-map** command to specify the name of the class map and enter class map configuration mode. You can use only one **match** command for each class map.

match Command

Command	Description
<i>access-group {access-group name access-group name}</i>	Specifies the name of the ACL against whose contents packets are checked to determine if they belong to the class. CBWFQ supports numbered and named ACLs.
<i>input-interface interface name</i>	Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class.
<i>protocol protocol</i>	Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.
<i>ip precedence tos</i>	Specifies the IP precedence ToS level used as a match criterion against which packets are checked to determine if they belong in this class.

Step 2a: Configuring CBWFQ with Tail Drop

This topic describes configuration of policies built from previously defined classes. This CBWFQ is configured with tail drop rather than WRED. You can implement either one of these options, 2a or 2b, but not both.

Step 2a: Configuring CBWFQ with Tail Drop

Cisco.com

```
Router(config)#policy-map policy-map-name
Router(config-pmap)#class class-name
Router(config-pmap-c)#bandwidth bandwidth-kbps
Router(config-pmap-c)#queue-limit number-of-packets
```

- Use the **queue-limit** command when configuring CBWFQ with tail drop.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10-11

This process entails configuration of policies to be applied to packets belonging to one of the classes previously defined through a class map. For this process, you must configure a policy map that specifies the policy for each traffic class.

Use the **policy-map** command to specify the policy map name and enter the policy map configuration mode. Then, use one or more of the following commands to configure policy for a standard class or the default class:

- **class**
- **bandwidth**
- **fair-queue** (for class-default class only)
- **queue-limit** or **random-detect**

Step 2b: Configuring CBWFQ with WRED

This topic describes configuration of CBWFQ with WRED rather than tail drop. Remember, you can choose this step or the prior one (2a), but not both.

Step 2b: Configuring CBWFQ with WRED

Cisco.com

```
Router(config)#policy-map policy-map-name
Router(config-pmap)#class class-name
                        or
Router(config-pmap-c)#bandwidth bandwidth-kbps
Router(config-pmap-c)#random-detect
Router(config-pmap-c)#random-detect
                        exponential-weighting-constant exponent
                        and/or
Router(config-pmap-c)#random-detect
                        precedence precedence min-threshold max-threshold
                        mark-prob-denominator
```

- Use the random-detect command when configuring CBWFQ with WRED.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10-12

Note If you configure a class in a policy map to use WRED for packet drop instead of tail drop, you must ensure that WRED is not configured on the interface to which you intend to attach that service policy.

class Command

Command	Description
<i>class-name</i>	Specifies the name of a class to be created and included in the service policy
<i>class-default</i>	Specifies the default class so that you can configure or modify its policy

bandwidth Command

Command	Description
<i>bandwidth-kbps</i>	Specifies the amount of bandwidth in kbps (or as a percentage of the link) to be assigned to the class. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.

queue-limit Command

Command	Description
<i>number-of-packets</i>	Specifies the maximum number of packets that can be queued for the class. If this is not specified, the default queue limit is 64 packets.

random-detect Command

Command	Description
<i>Random-detect</i>	Enables WRED. The class policy will drop packets using WRED instead of tail drop.
<i>exponential-weighting-constant exponent</i>	Configures the exponential weight factor that is used in calculating the average queue length.
<i>precedence precedence min-threshold max-threshold mark-prob-denominator</i>	Configures WRED parameters for packets with a specific IP precedence. Repeat this command for each precedence.

You can configure policy for more than one class in the same policy map.

Step 2c: Configuring CBWFQ Default Class (Optional)

This topic describes configuration of a CBWFQ default class. You can use default class with either tail drop (2a) or WRED (2b).

Step 2c: Configuring CBWFQ Default Class (Optional)

Cisco.com

```
Router(config)#policy-map policy-map-name
Router(config-pmap)#class class-default default-class-name
    or
Router(config-pmap-c)#bandwidth bandwidth-kbps
    or
Router(config-pmap-c)#fair-queue [number-of-dynamic queues]
```

- **Configure the default class for tail drop using the queue-limit command.**
- **Configure the default class for WRED using the random-detect command.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-10-13

Optionally, you can modify the policy for IP flows that do not match any of the match criteria of the classes. The **class class-default** command is used to classify traffic that does not fall into one of the defined classes. The class-default class is predefined when you create the policy map. By default, the class-default class is defined as flow-based WFQ.

Configuring the default class with the **bandwidth** policy-map class configuration command disqualifies the default class for flow-based WFQ. If a default class is configured with the **bandwidth** policy-map class configuration command, all unclassified traffic is put into a single FIFO queue and treated according to the configured bandwidth. If a default class is configured with the **fair-queue** command (or if no default class is configured), all unclassified traffic is flow-classified and given best-effort treatment.

fair-queue Command

Command	Description
<i>[number-of-dynamic-queues]</i>	In policy-map class configuration mode, this command specifies the number of dynamic queues to be reserved for use by flow-based WFQ running on the default class. The number of dynamic queues is derived from the bandwidth of the interface.

Step 3: Configuring CBWFQ

This topic describes the configuration for attaching policies to interfaces.


Step 3: Configuring CBWFQ

Cisco.com

```
Router(config-if)#service-policy output policy-map
```

- Use the **service-policy output** command to attach the service policy to an interface and enable CBWFQ.

```
Router(config)#interface s0  
Router(config-if)#service-policy output MYMAP
```



A diagram showing a blue router icon with a red arrow pointing to its top surface. A red line representing a network link extends from the router to the right, labeled 'S0'.

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-14

This process requires that you apply an existing policy map, or service policy, with an interface to associate the particular set of policies for the map to that interface.

Use the **service-policy output** command in interface configuration mode to attach the policy to an interface.

service-policy output Command

Command	Description
<i>output policy-map</i>	Enables CBWFQ and attaches the specified service policy map to the output interface

CBWFQ Example

This topic describes a CBWFQ configuration example.

CBWFQ Example

Cisco.com

```
Router(config)#access-list 101 permit udp host
10.10.10.10 host 10.10.10.20 range 16382 20000
Router(config)#access-list 102 permit udp host
10.10.10.10 host 10.10.10.20 range 53000 56000
Router(config)#class-map class1
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#class-map class2
Router(config-cmap)#match access-group 102
Router(config-cmap)#exit
```

- **Class1** uses access-list 101 to match a UDP port range for voice
- **Class2** uses access-list 102 to match a UDP port range for video

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-10-15

In the configuration example shown in the figure, class1 is defined by referencing access-list 101 with the **match access-group 101** command. Class1 will therefore match UDP traffic from host 10.10.10.10 to host 10.10.10.20 on ports 16382 to 20000.

Class2 is defined by referencing access-list 102 with the **match access-group 102** command. Class2 will therefore match UDP traffic from host 10.10.10.10 to host 10.10.10.20 on ports 53000 to 56000.

CBWFQ Example (Cont.)

Cisco.com

```
Router(config)#policy-map policy1
Router(config-pmap)#class class1
Router(config-pmap-c)#bandwidth 3000
Router(config-pmap-c)#queue-limit 30
Router(config-pmap-c)#exit
Router(config-pmap)#class class2
Router(config-pmap-c)#bandwidth 2000
Router(config-pmap-c)#exit
```

- **Class2 does not specify a queue limit, so the default of 64 packets is assumed.**
- **Tail drop will be used for both classes**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-16

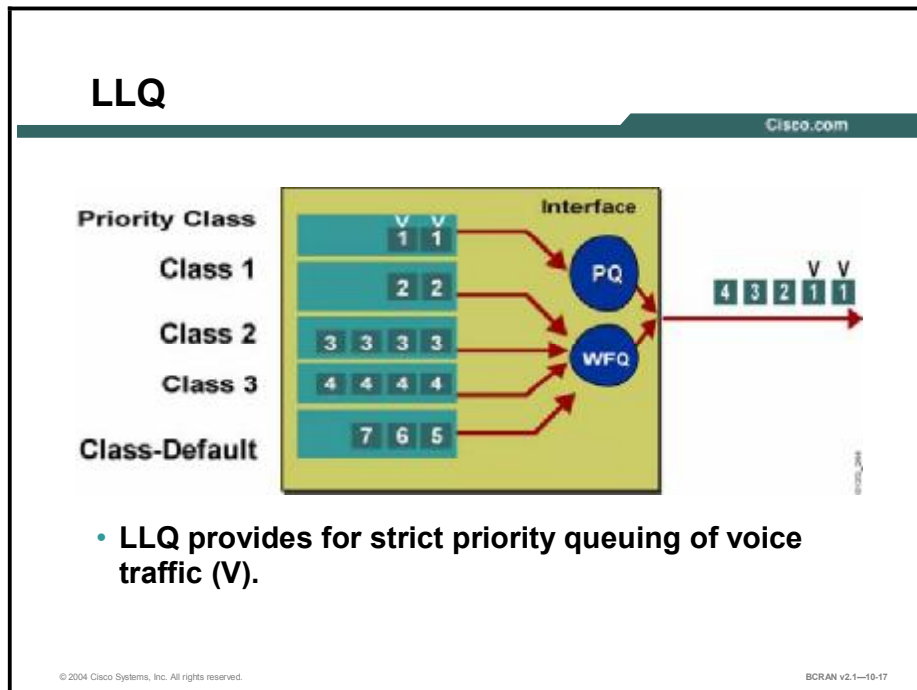
The **policy-map** command creates a policy map. The configuration example in the figure shows that the policy map, policy1, includes two class maps:

- **Class1:** Configured with a bandwidth of 3000 kbps and a queue limit of 30 packets.
- **Class2:** Configured with a bandwidth of 2000 kbps. Because the queue limit is not specified, the default of 64 packets applies.

Since neither class is configured with the **random-detect** command, Cisco IOS software will tail drop packets if their destination queue is full. Use the **random-detect** command to configure WRED.

LLQ Operation

This topic describes the concept of low latency queuing (LLQ).



The LLQ feature provides strict priority queuing (PQ) for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, strict PQ gives delay-sensitive data—such as voice—preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. LLQ is also called PQ/CBWFQ, because it is a combination of the two techniques.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth that you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which the packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice and video traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission, which cause jitter.

To apply a class of traffic to the strict priority queue, you configure the **priority** command for that class of traffic. That class of traffic and others then belong to a policy map. Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes are applied to the same, single, strict priority queue. The multiple classes will contend with each other for bandwidth.

Although it is possible to apply various types of real-time traffic to the strict priority queue, Cisco recommends that you direct only voice traffic to it. This is because voice traffic is well behaved, whereas other types of real-time traffic are not. Moreover, voice traffic requires that delay be nonvariable in order to avoid jitter. Real-time traffic such as video could introduce variation in delay, thereby thwarting the steadiness of delay required for successful voice traffic transmission.

Configuring LLQ

This topic describes the configuration of LLQ.

Configuring LLQ

Cisco.com

```
Router(config)#policy-map policy-map-name
Router(config-pmap)#class class-name
or
Router(config-pmap-c)#priority bandwidth-kbps
```

- **The bandwidth, queue-limit, or random-detect commands cannot be used when configuring a class for LLQ.**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-18

When you specify the **priority** command for a class, it takes a bandwidth argument that gives maximum bandwidth in kilobits per second (kbps). You use this parameter to specify the maximum amount of bandwidth that is allocated for packets belonging to the class. The bandwidth parameter both *guarantees* bandwidth to the priority class and *restrains* the flow of packets from the priority class.

In the event of congestion when the bandwidth is exceeded, policing is used to drop packets. Voice traffic queued to the priority queue is UDP-based and therefore not adaptive to the early packet drop characteristic of WRED. Because WRED is ineffective, you cannot use the WRED **random-detect** command with the **priority** command. In addition, because policing is used to drop packets and a queue limit is not imposed, the **queue-limit** command cannot be used with the **priority** command. The following table explains the **priority** command.

priority Command

Command	Description
<i>bandwidth-kbps</i>	Specifies the amount of bandwidth in kbps to be assigned to the class for PQ. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded. Priority traffic metering has these qualities:

- It is much like the rate-limiting feature of committed access rate (CAR), except that priority traffic metering is only performed under congestion conditions. Whether or not the device is congested, the priority-class traffic is not allowed to exceed its allocated bandwidth. When the device is congested, the priority-class traffic above the allocated bandwidth is discarded.
- It is performed on a per-packet basis, and tokens are replenished as packets are sent. If there are not enough tokens available to send the packet, it is dropped.
- It restrains priority traffic to its allocated bandwidth to ensure that standard traffic, such as routing packets and other data, is not starved.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **WFQ prioritizes traffic into conversations or flows.**
- **For interfaces having 2.048 Mbps or less, WFQ is the default.**
- **Use the fair-queue command to modify flows or to setup WFQ on other interfaces.**
- **Use the class-map CBWFQ command to specify the class map name.**
- **Use the policy-map CBWFQ command to specify the policy map name and configure WRED or tail drop along with optional default class.**
- **Use the service-policy output CBWFQ command in interface configuration mode to attach the policy to an interface.**
- **The LLQ feature provides strict priority queuing for CBWFQ.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-19

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Packet trains are most closely associated with what type of network application?
- A) SNA
 - B) DNS
 - C) Telnet
 - D) FTP
- Q2) The WFQ algorithm cannot discriminate between traffic flows based on _____.
- A) RTP
 - B) source or destination port
 - C) source or destination MAC
 - D) ToS
- Q3) With WFQ, small, low-volume packets are given priority over large, high-volume conversation packets.
- A) true
 - B) false
- Q4) The *congestive-discard-threshold* parameter in the **fair-queue** {*congestive-discard-threshold*} interface configuration command specifies the maximum number of _____ in a conversation held in a queue before messages are discarded.
- A) bytes
 - B) packets
 - C) kilobytes
 - D) streams
- Q5) The weight assigned to a traffic class in CBWFQ is defined as _____.
- A) class bandwidth divided by the interface bandwidth
 - B) class bandwidth
 - C) interface bandwidth divided by the class bandwidth
 - D) interface bandwidth
- Q6) How many priority classifications are possible with flow-based WFQ?
- A) 5
 - B) 6
 - C) 7
 - D) 8

- Q7) After entering policy map configuration mode, all of the following are valid commands except ____.
- A) **class**
 - B) **protocol**
 - C) **bandwidth**
 - D) **queue-limit**
- Q8) The **class class-default** command is used to ____.
- A) classify traffic that does not fall into one of the defined classes
 - B) classify traffic that falls into one of the defined classes
 - C) specify traffic that falls into one of the defined classes
 - D) route traffic to a specific location
- Q9) You can configure a policy for more than one class in the same policy map.
- A) true
 - B) false
- Q10) You can use the **service-policy output** command in interface configuration mode to attach the policy to an interface.
- A) true
 - B) false
- Q11) Low latency queuing is also referred to as PQ/CBWFQ.
- A) true
 - B) false
- Q12) When you are configuring low latency queuing, what measurement of bandwidth is specified in the **priority** command?
- A) bits per second
 - B) bytes per second
 - C) kilobits per second
 - D) kilobytes per second

Quiz Answer Key

- Q1) D
Relates to: WFQ Operation
- Q2) A
Relates to: WFQ Operation
- Q3) A
Relates to: Configuring WFQ
- Q4) B
Relates to: Configuring WFQ
- Q5) C
Relates to: CBWFQ Operation
- Q6) C
Relates to: CBWFQ vs. Flow-Based WFQ
- Q7) B
Relates to: Step 2c: Configuring CBWFQ Default Class (Optional)
- Q8) A
Relates to: Step 2c: Configuring CBWFQ Default Class (Optional)
- Q9) A
Relates to: Step 3: Configuring CBWFQ
- Q10) A
Relates to: Step 3: Configuring CBWFQ
- Q11) A
Relates to: LLQ Operation
- Q12) C
Relates to: Configuring LLQ

Verifying Congestion Management

Overview

This lesson discusses queuing verification.

Relevance

When queuing is configured on routers, proper operation should be verified for assurance that the expected traffic-handling objectives have resulted.

Objectives

Upon completing this lesson, you will be able to:

- Verify queuing operation using the **show queuing** command
- Describe the differences and similarities among flow-based WFQ, CBWFQ, and LLQ

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Verification of Queuing Operation
- Queuing Comparison Summary
- Summary
- Quiz

Verification of Queuing Operation

This topic describes the **show queuing** command.

Verifying Queuing Operation

Cisco.com

```
Router#show queuing int S0
Interface Serial0 queuing strategy: fair
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queuing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
```

- **Displays queuing status on all interfaces**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-10.2

Use the **show queuing** command to display detailed queuing information about all interfaces where fair queuing is enabled.

In this example, serial0 is enabled with WFQ.

You can also use the **show interfaces** command to display queuing information for the interfaces of the router.

Note The word “queuing” is spelled “queueing” in the commands.

Verifying Queuing Operation (Cont.)

Cisco.com

```
branch_6#show policy-map interface s1.1
Serial1.1: DLCI 621 -

Service-policy output: CBWFQ-branch

Class-map: LLQ-102-CLASS (match-all)
2022 packets, 129408 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 102
Weighted Fair Queuing
Strict Priority
Output Queue: Conversation 24
Bandwidth 8 (kbps) Burst 200 (Bytes)
(pkts matched/bytes matched) 390/24960
(total drops/bytes drops) 0/0
Class-map: class-default (match-any)
1641 packets, 74919 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

- Displays counter information on the serial interface queuing.

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1-10-3

The table defines the counters in the figure.

Counters for show policy-map interface Command (in figure)

Counter	Explanation
2022 packets, 129408 bytes	The number of packets matching the criteria of the class. This counter increments whether or not the interface is congested.
(pkts matched/bytes matched) 390/24960	The number of packets matching the criteria of the class when the interface was congested. In other words, the transmit ring of the interface was full, and the driver and the Layer 3 processor system worked together to queue the excess packets in the Layer 3 queues, where the service policy applies. Packets that are process-switched always go through the Layer 3 queuing system and thus increment the "packets matched" counter.
5 minute offered rate 0 bps, drop rate 0 bps	Use the load-interval command to change this value and make it a more instantaneous value. The lowest value is 30 seconds; however, statistics displayed in the show policy-map interface output are updated every ten seconds. Because the command effectively provides a snapshot at a specific moment, the statistics may not reflect a temporary increase in queue size.

Without congestion, there is no need to queue any excess packets. With congestion, packets, including Cisco Express Forwarding (CEF) and fast-switched packets, may go into the Layer 3 queue. Refer back to how the Cisco IOS configuration guide defines congestion: "If you use congestion management features, packets accumulating at an interface are queued until the interface is free to send them; they are then scheduled according to their assigned priority and the queuing mechanism configured for the interface."

Normally, the "packets" counter is much larger than the "pkts matched" counter. If the values of the two counters are nearly equal, then the interface is receiving a large number of process-switched packets or is heavily congested. Both of these conditions should be investigated to ensure optimal packet forwarding.

Verifying Queuing Operation (Cont.)

Cisco.com

```
Router# show policy-map interface e1/1
Ethernet1/1 output : pol
Weighted Fair Queuing
Class class1
  Output Queue: Conversation 264
  Bandwidth 937 (kbps) Max Threshold 64 (packets)
  (total/discards/tail drops) 11548/0/0
Class class2
  Output Queue: Conversation 265
  Bandwidth 937 (kbps) Max Threshold 64 (packets)
  (total/discards/tail drops) 11546/0/0
```

- Displays configuration for classes on the output interface

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-4

For CBWFQ and LLQ, you can use the **show policy-map interface** command to display the configuration of all classes forming part of the specified policy map. The **show policy-map interface** command displays the configuration of all classes configured for all policy maps on the specified interface.

Queuing Comparison Summary

This topic describes the differences and similarities among queuing methods.

Queuing Comparison Summary		
Flow-Based WFQ	Class-Based WFQ	Low Latency Queuing
No classes	Up to 64 classes	Up to 64 classes
Weights IP flows	Weights classes	Prioritizes classes (voice), weights remaining classes
Interactive traffic gets lowest weight	User-defined classes get custom weight	Priority classes served first
File transfer gets balanced access	Highly customizable	Designed to bring prioritize VoIP
Enabled by default	Must configure	Must configure

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10.5

WFQ is enabled by default. It does not use queue lists to determine the preferred traffic on a serial interface. Instead, the fair queue algorithm dynamically sorts traffic into messages that are part of a conversation. The messages are queued with low-volume conversations (usually interactive traffic), and given priority over high-volume, bandwidth-intensive conversations, such as file transfers. When multiple file transfers occur, the transfers are given comparable bandwidth.

CBWFQ allows network managers to customize fair queuing behavior so that user-defined classes of traffic receive guaranteed bandwidth during times of congestion. More than one flow, or conversation, can belong to a user-defined class. LLQ adds strict PQ to CBWFQ operation. LLQ allows you to specify a priority class which will be served first, before any of the other classes of traffic. The PQ with LLQ will not starve the other classes because the PQ is policed whether or not there is congestion.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Use the show queuing command to display detailed queuing information about all interfaces where fair queuing is enabled.**
- **Use the show interfaces command to display queuing information for the router interfaces.**
- **Use the show policy-map interface command to display the configuration of all classes forming part of the specified policy map.**

© 2004 Cisco Systems, Inc. All rights reserved.

BCRAN v2.1—10-6

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) When an interface is cleared to send queued packets, the packets are sent based on their _____.
- A) size
 - B) assigned priority
 - C) mobility
 - D) date
- Q2) Which type of queuing does NOT use queue lists to determine the preferred traffic?
- A) CBWFQ
 - B) LLQ
 - C) WFQ
 - D) WRED
- Q3) Which type of queuing allows you to specify a priority class that will be served first?
- A) CBWFQ
 - B) LLQ
 - C) WFQ
 - D) WRED

Quiz Answer Key

- Q1) B
Relates to: Verification of Queuing Operation
- Q2) C
Relates to: Queuing Comparison Summary
- Q3) B
Relates to: Queuing Comparison Summary

Implementing Link Efficiency

Overview

This lesson discusses how to optimize traffic over the WAN link by compressing data on the link.

Relevance

Managing network performance is crucial for the bandwidth-demanding applications of today. Understanding various compression techniques is important to determine how effective each would be in reducing congestion.

Objectives

Upon completing this lesson, you will be able to:

- Identify the concepts of compression and where compression occurs on a data frame
- Describe link compression and the two algorithms associated with link compression
- Describe payload compression
- Describe TCP/IP header compression
- Describe modem compression, encrypted data, and CPU and memory considerations when selecting compression for a WAN link
- Configure link, payload, and TCP header compression on a WAN interface

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

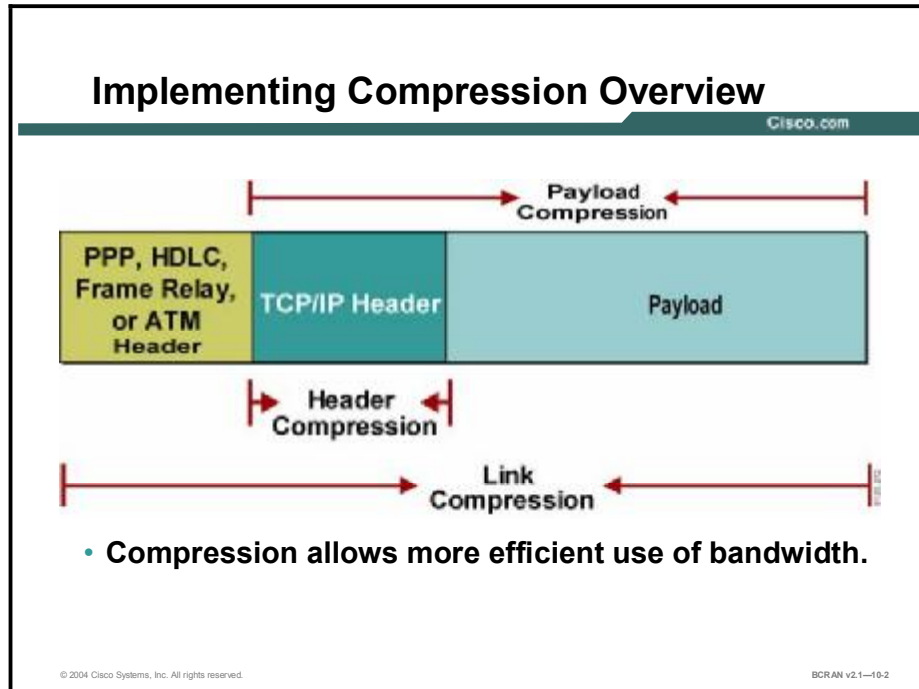
Outline

This lesson includes these topics:

- Overview
- Compression Overview
- Link Compression over a Point-to-Point Connection
- Payload Compression Implementation
- TCP/IP Header Compression
- Microsoft Point-to-Point Compression
- Other Compression Considerations
- Data Compression
- Summary
- Quiz

Compression Overview

This topic describes the general concepts of compression.



Cisco IOS software offers a number of features that optimize WAN links to ease the WAN bandwidth bottleneck. One of the more effective methods of WAN optimization is compression of the data that travels across the WAN link.

The various types of data compression that Cisco equipment supports are as follows:

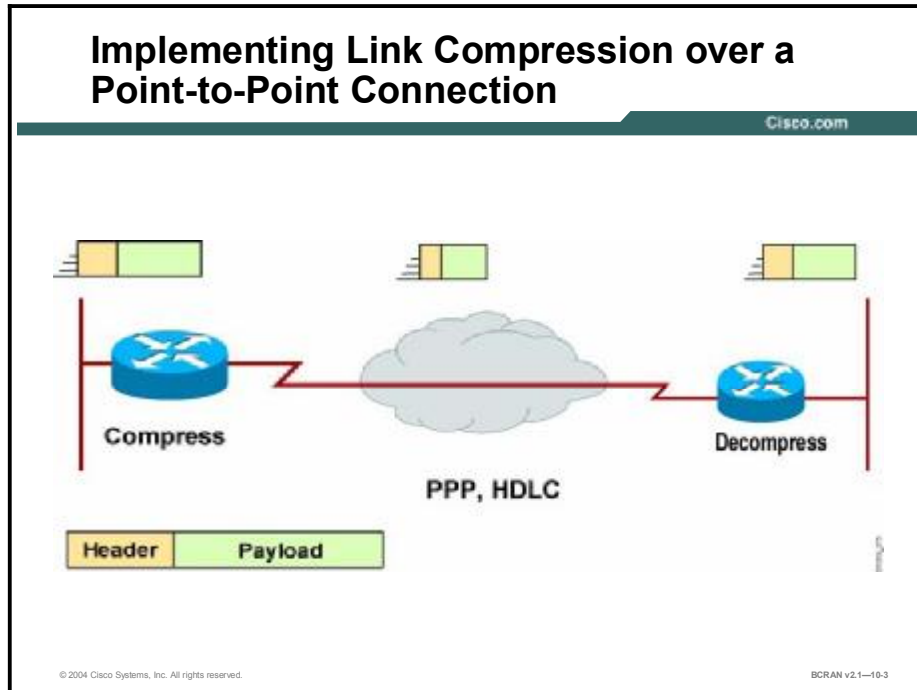
- Link compression (also known as per-interface compression)
- Payload compression (also known as per-virtual circuit compression)
- TCP/IP header compression
- Microsoft Point-to-Point Compression (MPPC)
- Other compression considerations

Note The default method of transmitting data across a serial link is uncompressed. This method allows headers to be used in the normal switching operation, but can consume valuable bandwidth. This section discusses software compression features on Cisco devices. A hardware compression card is available on some Cisco devices. This section does not cover hardware compression features.

Note Compression (header or data) is only one method of link efficiency. The other method of fragmentation and interleaving involves Multilink PPP (MLP), which was discussed earlier in the "Configuring PPP Features" module.

Link Compression over a Point-to-Point Connection

This topic describes link compression and the two algorithms that are associated with link compression.



Link compression (or per-interface compression) involves compressing both the header and payload sections of a data stream. Unlike header compression, link compression is protocol independent.

The link compression algorithm uses Predictor or STAC to compress the traffic into another link layer, such as PPP or Link Access Procedure, Balanced (LAPB), to ensure error correction and packet sequencing. Cisco High-Level Data Link control (HDLC) uses STAC compression only. The link compression algorithms are:

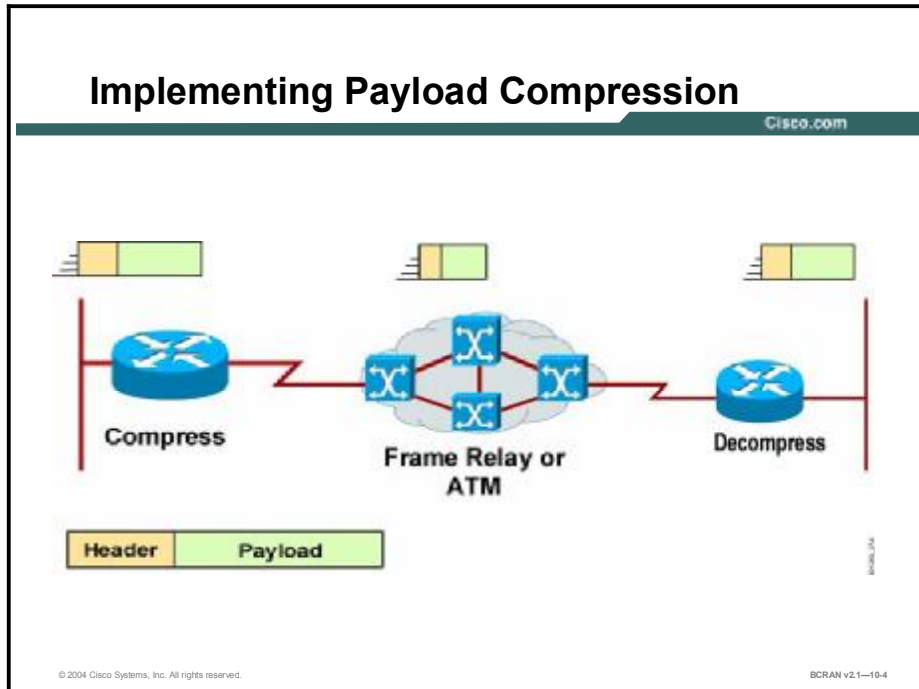
- **Predictor:** Predicts the next sequence of characters in the data stream by using an index to look up a sequence in a compression dictionary. It then examines the next sequence in the data stream to see if it matches. If so, that sequence replaces the looked-up sequence in a maintained dictionary. If not, the algorithm locates the next character sequence in the index and the process begins again. The index updates itself by hashing a few of the most recent character sequences from the input stream.
- **STAC:** Developed by STAC Electronics, STAC is a Lempel-Ziv (LZ)-based compression-based algorithm. It searches the input data stream for redundant strings and replaces them with a "token," which is shorter than the original redundant data string.

If the data flow moves across a point-to-point connection, use link compression. In a link compression environment, the complete packet is compressed and the switching information in the header is not available for WAN switching networks. Therefore, the best applications for

link compression are point-to-point environments with a limited hop path. Typical examples are leased lines or ISDN.

Payload Compression Implementation

This topic describes payload compression.



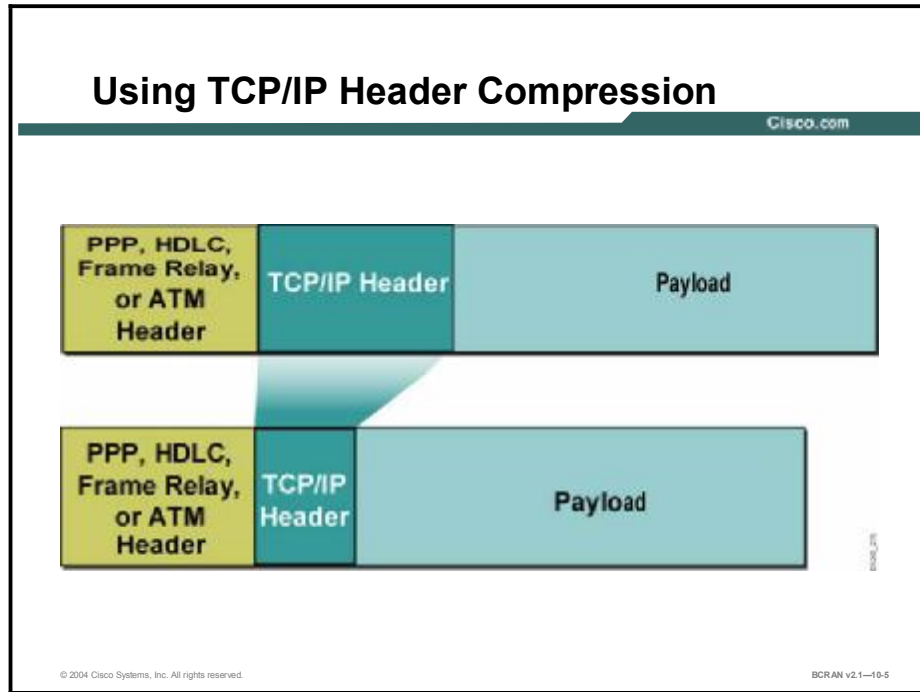
Payload compression (or per-virtual circuit compression) compresses only the data portion of the data stream. The header is left intact.

When designing an internetwork, the customer cannot assume that an application will be transmitted over point-to-point lines. If link compression is used rather than payload compression, the header may not be readable at a particular hop.

Note When using payload compression, the header is left unchanged and packets can be switched through a WAN packet network. Payload compression is appropriate for virtual network services such as Frame Relay and ATM. It uses the STAC compression method discussed earlier.

TCP/IP Header Compression

This topic describes TCP/IP header compression.

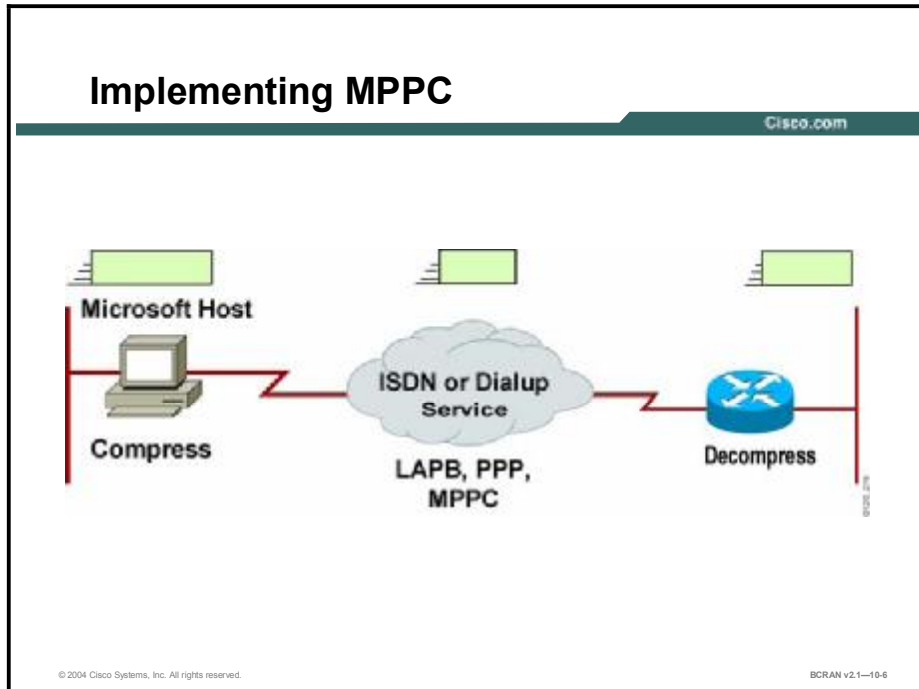


TCP/IP header compression subscribes to the Van Jacobson algorithm defined in RFC 1144. It lowers the overhead generated by disproportionately large TCP/IP headers as they are transmitted across the WAN. TCP/IP header compression is protocol-specific and only compresses the TCP/IP header. The Layer 2 header is still intact and a packet with a compressed TCP/IP header can still travel across a WAN link.

Note TCP/IP header compression is beneficial on small packets with few bytes of data, such as Telnet. Cisco header compression supports Frame Relay and dial-on-demand WAN link protocols. Due to processing overhead, header compression is generally used at lower speeds, such as 64-kbps links.

Microsoft Point-to-Point Compression

This topic describes Microsoft Point-to-Point Compression (MPPC).



The MPPC protocol (RFC 2118) allows Cisco routers to exchange compressed data with Microsoft clients. MPPC uses an LZ-based compression mechanism. Use MPPC when exchanging data with a host using MPPC across a WAN link.

Other Compression Considerations

This topic describes modem compression, encrypted data, and CPU and memory considerations when you are selecting compression for a WAN link.

Other Compression Considerations

Cisco.com

- **Modem compression**
- **Encrypted data**
- **CPU cycles versus memory**

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-10-7

Other considerations when selecting a compression algorithm to optimize your WAN utilization include:

- **Modem compression:** In dialup environments, compression can occur in the modem. Two common modem compression standards are Microcom Networking Protocol-5 (MNP-5) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) V.42*bis*. MNP-5 and V.42*bis* offer up to two times and four times compression, respectively. The two specifications are not compatible. The modems at both ends of the connection negotiate the standard to use. If compression occurs at the modem, do not configure the router to run compression.
- **Encrypted data:** Compression is a Layer 2 function and encryption occurs at Layer 3. When a data stream is encrypted by the client application, it is then passed onto the router for routing or compression services or both. When the compression engine receives the encrypted data stream, which by definition has no repetitive patterns, the data expands and will not compress. LZ will then compare the before and after images to determine which is the smallest and send the uncompressed data as it was originally received if expansion occurred. If data is encrypted, do not compress the encrypted data using a Layer 2 compression algorithm.
- **CPU cycles versus memory:** The amount of memory that a router must have and that the network manager must plan on varies. The amount of memory that is required varies according to the protocol being compressed, the compression algorithm, and the number of concurrent circuits on the router. Memory requirements will be higher for Predictor than for STAC, and payload will use more memory than link compression. Likewise, link compression uses more CPU cycles.

Data Compression

This topic describes the configuration steps for compression on a WAN interface.

Configuring Compression

Cisco.com

```
Router(config-if)#compress [ predictor | stac | mppc ]
```

- Configures software compression for LAPB, PPP, and HDLC for a link

```
Router(config-if)#frame-relay payload-compress
```

- Enables payload compression on a specified interface or subinterface

```
Router(config-if)#ip rtp header-compression [ passive ]
```

- Specified that headers for RTP traffic will be compressed

```
Router(config-if)#ip tcp header-compression [ passive ]
```

- Specified that headers for TCP traffic will be compressed

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—10-8

Use the **compress** [*predictor* | *stac* | *mppc*] command to configure point-to-point software compression for an LAPB, PPP, or HDLC link. Data compression schemes that are used in internetworking devices are referred to as lossless compression algorithms. These schemes reproduce the original bit streams exactly, with no degradation or loss. This feature is required by routers and other devices to transport data across the network. If you have a point-to-point link and are using PPP encapsulation, you can also use the **ppp compress** [*predictor* | *stac*] interface configuration command (not shown) instead of the **compress** command.

Use the **frame-relay payload-compress** command to enable STAC compression on a specified Frame Relay point-to-point interface or subinterface.

Use the **ip rtp header-compression** command to enable compressed Real-Time Transport Protocol (cRTP) header compression for serial encapsulations, HDLC, or PPP. If you include the *passive* keyword, the software compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you use the command without the *passive* keyword, the software compresses all RTP traffic.

Use the **ip tcp header-compression** command to enable TCP/IP header compression. The *passive* keyword compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If *passive* is not specified, the router will compress all traffic.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Link compression involves compressing the header and payload sections of a data stream.**
- **Payload compression only compresses the payload portion of a data stream.**
- **Use the `compress [predictor | stac | mppc]` command to configure point-to-point software compression for an LAPB, PPP, or HDLC link.**
- **Use the `frame-relay payload-compress` command to enable STAC compression on a specified Frame Relay point-to-point interface or subinterface.**
- **Use the `ip rtp header-compression` command to enable CRTP header compression for serial encapsulations, HDLC, or PPP.**
- **Use the `ip tcp header-compression` command to enable TCP/IP header compression.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—10-9

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 10-1: Managing Network Performance Using CBWFQ and LLQ

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the best method for optimizing data across a WAN link?
- A) WFQ
 - B) LLQ
 - C) FIFO
 - D) compression
- Q2) Link compression will compress the _____.
- A) payload
 - B) header
 - C) payload and header
 - D) none of the above
- Q3) Applications that require the IP header to be intact should use _____.
- A) link compression
 - B) payload compression
 - C) header compression
 - D) link and header compression
- Q4) TCP/IP header compression requires very minimal processing and should be used on high-speed WAN links.
- A) true
 - B) false
- Q5) Which implementation of compression allows Cisco routers to compress communications with Microsoft clients?
- A) STAC
 - B) Predictor
 - C) MPPC
- Q6) Compression and encryption should be used together to maximize WAN links.
- A) true
 - B) false

Q7) Which of the following is NOT a valid keyword for the **compress** command?

- A) **predictor**
- B) **stac**
- C) **mppc**
- D) **lz**

Quiz Answer Key

- Q1) D
Relates to: Compression Overview
- Q2) C
Relates to: Link Compression over a Point-to-Point Connection
- Q3) B
Relates to: Payload Compression Implementation
- Q4) B
Relates to: TCP/IP Header Compression
- Q5) C
Relates to: Microsoft Point to Point Compression
- Q6) B
Relates to: Other Compression Considerations
- Q7) D
Relates to: Data Compression

Using AAA to Scale Access Control

Overview

This module describes the Cisco Secure Access Control Server (ACS) software features. It also describes how to configure a router to access the Cisco Secure ACS and use authentication, authorization, and accounting (AAA).

Objectives

Upon completing this module, you will be able to:

- Describe Cisco Secure ACS features and operation
- Configure a router with AAA commands
- Use a configured AAA server to control access in a remote access network

Outline

The module contains these lessons:

- Identifying Cisco Access Control Solutions
- Defining and Configuring AAA

Identifying Cisco Access Control Solutions

Overview

This lesson contains an overview of Cisco access control solutions.

Relevance

Network administrators require the ability to authenticate users, authorize access, and log significant events (accounting) on network resources. The Cisco Systems solution to this requirement is the Cisco Secure ACS.

Objectives

Upon completing this lesson, you will be able to:

- Identify the security features of the Cisco Secure ACS server
- Identify the three components of the Cisco Secure ACS server
- Describe the security features of the Cisco Secure ACS server components
- Describe the features of the Cisco Secure ACS server administrator client

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- Cisco Access Control Solutions Overview
- Basic Security Devices and Router Security
- Cisco Security Options Overview
- Cisco Secure ACS Overview
- Cisco Secure ACS Components
- Cisco Secure ACS Administrator GUI Client
- Summary
- Quiz

Cisco Access Control Solutions Overview

This topic describes Cisco access control solutions.

Cisco Access Control Solutions Overview

Cisco.com

- Cisco security control solutions
- Security options
- Cisco Secure ACS function and components
- Cisco Secure ACS administrative clients

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—11-2

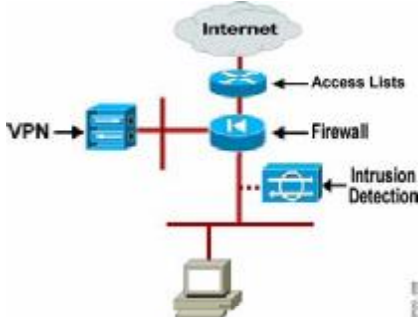
The Cisco Secure ACS is a high-performance, highly scalable, centralized user access control framework. The Cisco Secure ACS offers centralized command and control for all user AAA from a web-based graphical interface and distributes those controls to hundreds or thousands of access gateways in your network.

Basic Security Devices and Router Security

This topic discusses basic security methods.

Basic Security Devices and Router Security

Cisco.com



- Router security services to be used:
 - Access lists
 - Service password encryption
 - AAA
- Router services to be examined for security impacts:
 - IP source route
 - HTTP server
 - Bootp
 - CDP
 - Small servers

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-1.3

In a remote access network it is important to secure data and the network infrastructure. Although this course does not analyze different security methods in depth, it does focus on AAA and Virtual Private Networks (VPNs). Other security measures must also be considered when constructing a remote access network.

Popular security devices include:

- **Cisco PIX Firewall:** Firewalls separate network segments and inspect packets to determine if they are part of a permitted protocol, IP address, or conversation. The Cisco PIX Firewall can actually examine conversations to determine if an internal user properly solicited inbound traffic on the network.
- **Intrusion Detection System (IDS):** You can install IDS at various points within a network to examine passing traffic and determine if the traffic patterns show certain anomalies. These irregular traffic signatures can alert the network administrator of a network attack.
- **VPN concentrator:** Concentrators can encrypt data in network traffic and allow this data to be shared confidentially over a network infrastructure.
- **Routers:** Routers offer many security features that are also available in dedicated security devices. These features include the ability to encrypt traffic as a VPN concentrator and the ability to run access lists that prevent unauthorized traffic from accessing interfaces. In addition, routers can run a Cisco IOS Firewall feature set that prevents unauthorized traffic. While simultaneously inspecting traffic conversations in a manner similar to the Cisco PIX Firewall.

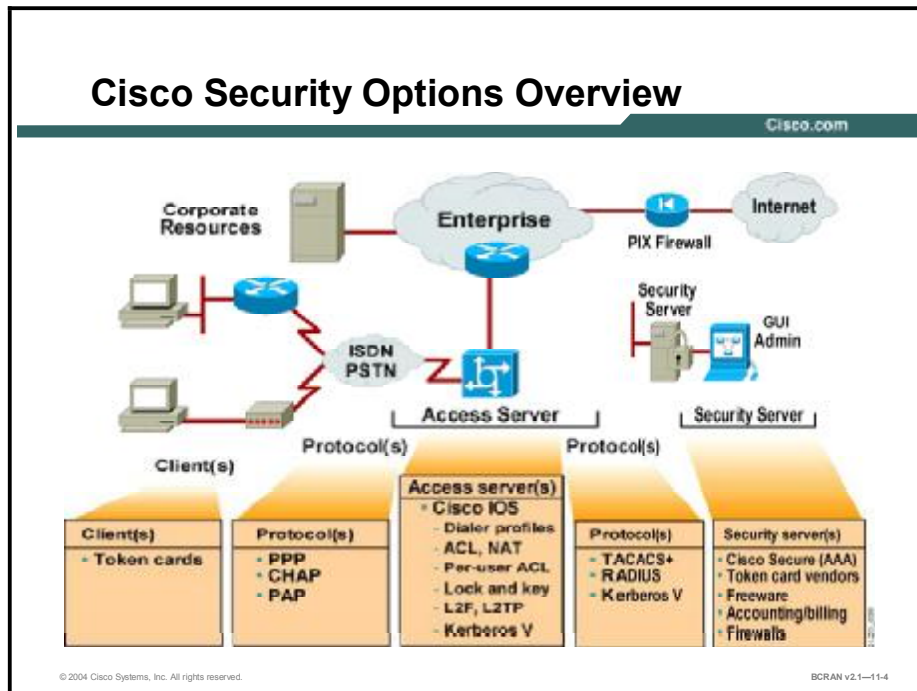
Although routers offer security features, many of the services that help the administrator manage the network can also leave the network vulnerable to attack. For example, Cisco routers generally have a web browser configuration interface, but it is recommended that administrators remove this HTTP functionality and configure using the command-line interface (CLI) in Cisco IOS software.

Other helpful services (such as Cisco Discovery Protocol [CDP]) can also be taken advantage of by a dishonest user trying to map a network. It is therefore important for a network administrator to know which users have access to the network and how to protect it from attacks.

Cisco Secure ACS implementation of AAA can be an extremely valuable tool available for administrators to use in protecting the network

Cisco Security Options Overview

This topic describes Cisco access control solutions.

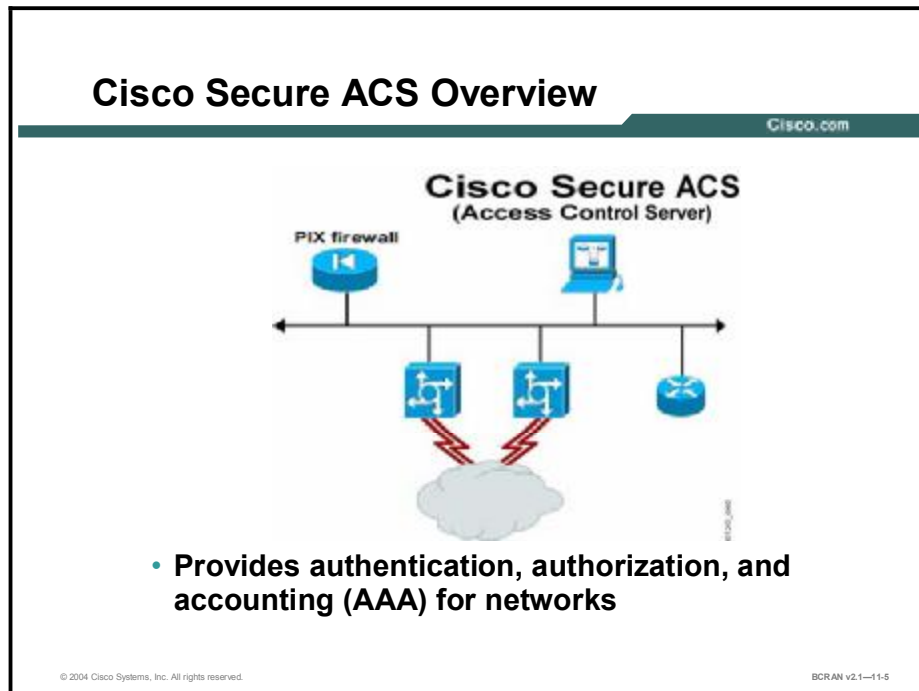


Cisco provides the following security solutions:

- **Clients:** Dialup clients can use token cards for secure dialup. Token cards such as RSA Data Security, Enigma, and Cryptocard are supported.
- **Protocols (client):** The Cisco IOS software supports PPP, Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP) for dialup security. Using PPP with CHAP authentication is recommended.
- **Access servers:** The Cisco IOS software supports the following protocols to provide a secure means for dialup access: dialer profiles, access control lists (ACLs), per-user ACLs, lock and key, Layer 2 Forwarding (L2F) protocol, Layer 2 Tunneling Protocol (L2TP), and Kerberos V.
- **Protocols (central site):** For security verification between the network access server and the network security server, the network access server supports the TACACS+, RADIUS, and Kerberos V protocols.
- **Security servers:** The Cisco Secure ACS is the umbrella under which Cisco Systems has a variety of security server solutions. Both the Cisco Secure ACS for UNIX and the Cisco Secure ACS for Windows software provide networks with AAA capabilities.

Cisco Secure ACS Overview

This topic describes Cisco Secure Access Control Server (ACS).



The Cisco Secure ACS helps centralize access control, accounting, and client access management.

The Cisco Secure ACS software incorporates a multiuser, web-based Java configuration and management tool that simplifies server administration and enables multiple system administrators to simultaneously manage security services from multiple locations. The graphical user interface (GUI) supports Microsoft and Netscape web browsers and provides multiplatform compatibility.

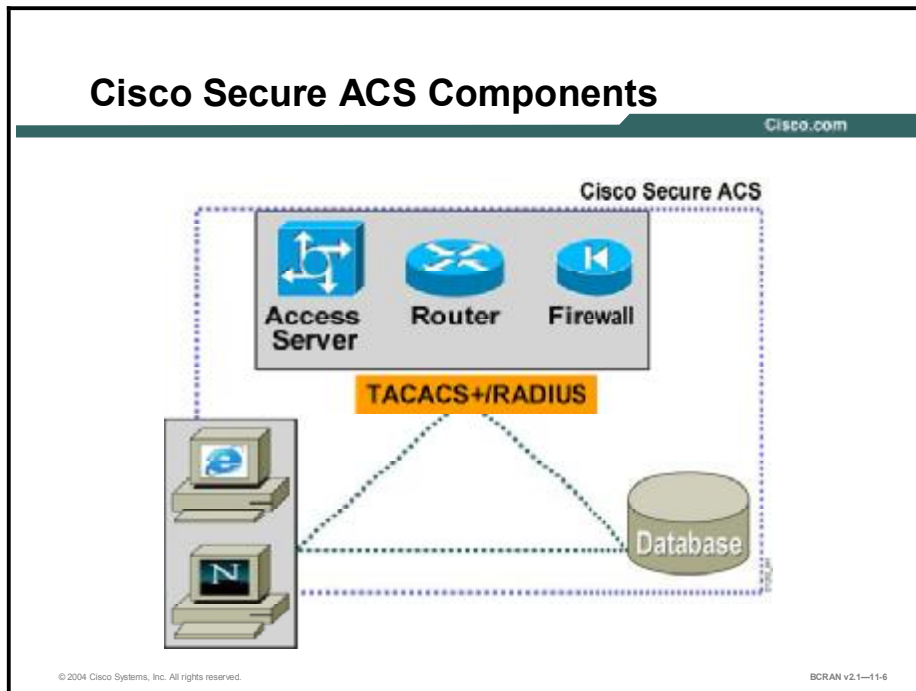
Various methods of authentication are supported on the Cisco Secure ACS, such as manual password entry, CHAP, and one-time passwords, including token cards. Token cards are considered the strongest method used to authenticate connecting users and to prevent unauthorized users from accessing proprietary information.

Management of group and user information takes place on a database configured to work with the Cisco Secure ACS. To simplify management of group and user information, the Cisco Secure ACS supports internal Windows, Open DataBase Connectivity (ODBC), Lightweight Directory Access Protocol (LDAP), Novell Directory Services (NDS), and many token server databases.

Additional features included in the Cisco Secure ACS are the ability to automatically disable accounts for prevention of brute force attacks and limitations on the number of login sessions.

Cisco Secure ACS Components

This topic describes Cisco Secure ACS components.



The Cisco Secure ACS has three major components:

- AAA server (Cisco Secure ACS)
- AAA clients
- User database

The AAA server gathers authentication information from an AAA configured client and verifies this information with a database. The Cisco Secure ACS then returns information to the AAA clients, permitting or denying user access. When the user authenticates successfully, the Cisco Secure ACS determines the authorization attributes to give the AAA client. Authorization attributes may include IP address pool, the type of protocol connection, or an ACL. The AAA client then begins forwarding accounting information to the Cisco Secure ACS.

AAA clients include a variety of Cisco products such as firewalls, routers, switches, and VPN Concentrators. These clients have software that allows them to communicate with the Cisco Secure ACS using either the TACACS+ or RADIUS protocols.

Cisco Secure ACS allows network administrators to easily administer accounts and globally change levels of services that are available for entire groups of users. The administrator can affect individual users or groups of users as they are configured in a specified database. This database may be a Windows NT or 2000, LDAP, NDS, ODBC, or many other token server databases.

Note Cisco Secure ACS operates successfully with Oracle version 7.3, Sybase SQL Server version 11, and Sybase SQLAnywhere by means of ODBC.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- The Cisco Secure ACS is a high-performance, highly scalable, centralized user access control framework.
- The Cisco Secure ACS incorporates a multiuser, Web-based Java configuration and management tool.
- The major components of Cisco Secure TACACS+ are the AAA server, the AAA client, and the user database.

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—1-8

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which services can be used with the Cisco Secure ACS?
- A) encryption
 - B) hashing
 - C) authentication
- Q2) Which security features can be implemented on a Cisco router?
- A) AAA
 - B) access lists
 - C) VPN
 - D) all of the above
- Q3) Which of the following is NOT a feature of the Cisco Secure ACS?
- A) AAA server
 - B) GUI interface
 - C) token card server
 - D) firewall function
- Q4) Which is the strongest method used to authenticate users dialing in and to prevent unauthorized users from accessing proprietary information?
- A) password verification
 - B) encryption
 - C) token cards
 - D) hashing
- Q5) The three components of the Cisco Secure ACS are the AAA server, AAA client, and _____.
- A) modems
 - B) user database
 - C) Visual Basic
 - D) firewall packet inspection
- Q6) Either a Netscape or a Microsoft Windows browser may be used as the Cisco Secure ACS GUI.
- A) true
 - B) false

Quiz Answer Key

- Q1) C
Relates to: Cisco Access Control Solutions Overview
- Q2) D
Relates to: Basic Security Devices and Router Security
- Q3) D
Relates to: Cisco Security Options Overview
- Q4) C
Relates to: Cisco Secure ACS Overview
- Q5) B
Relates to: Cisco Secure ACS Components
- Q6) A
Relates to: Cisco Secure ACS Administrator GUI Client

Defining and Configuring AAA

Overview

This lesson provides an overview of authentication, authorization, and accounting (AAA) and how to configure AAA.

Relevance

AAA is an invaluable tool for the network administrator. Understanding how, what, and when to use this tool is important to effectively control network access.

Objectives

Upon completing this lesson, you will be able to:

- Describe how AAA operates
- Describe the three components of AAA
- Describe the AAA router access modes
- Describe how to enable AAA and identify the Cisco Secure ACS
- Describe how to configure AAA authentication
- Configure AAA authentication
- Configure character mode login using AAA authentication
- Describe how to enable AAA authorization
- Configure character mode authorization
- Describe how to use AAA accounting commands
- Configure AAA accounting

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course
- All knowledge presented in the *Interconnecting Cisco Network Devices* (ICND) course

Outline

This lesson includes these topics:

- Overview
- AAA Definitions
- AAA Overview and Configuration
- Router Access Modes
- AAA Protocols
- AAA and the Cisco Secure ACS
- AAA Authentication Commands
- Character Mode Login Example
- AAA Authorization Commands
- Character Mode with Authorization
- Packet Mode Example
- AAA Accounting Commands
- AAA Accounting Example
- Summary
- Quiz

AAA Definitions

This topic describes the three components of AAA.

AAA Definition

Cisco.com

- 1. Authentication**
 - Who are you?
- 2. Authorization**
 - What can you do?
- 3. Accounting**
 - What did you do and how long did you do it?

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1—11.2

The three parts of AAA are defined as follows:

1. Authentication

- Authentication examines the identity of users and determines whether they should be allowed access to the network. Authentication allows network managers to bar intruders from their networks.

2. Authorization

- Authorization allows network managers to limit the network services available to a user. Authorization also helps restrict the exposure of the internal network to outside callers. Authorization allows mobile users to connect to the closest local connection and still have access privileges as though they were directly connected to their local networks. You can also use authorization to specify which commands a new system administrator can issue on specific network devices.

3. Accounting

- System administrators might need to bill departments or customers for connection time or resources that are used on the network (for example, bytes transferred). Accounting tracks this kind of information. You can also use the accounting syslog to track suspicious connection attempts and trace malicious activity.

AAA Overview and Configuration

This topic explains the configuration of AAA.

AAA Overview and Configuration

Cisco.com

- AAA definition
- AAA operation
- Router access modes

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—1-3

Configuring the Cisco Secure ACS server is the first part of a two-part process to develop an operational access control system that implements AAA. The second process involves configuring the network access server so that it functions properly with the Cisco Secure ACS server. These steps are critical and must be completed with extreme precision. Failure to configure the network access server properly may result in being locked out of the router.

You must understand router port types and access methods before you configure your network.

Router Access Modes

This topic describes the AAA router access modes.

Router Access Modes		
Modes	Router Ports	AAA Command Element
Character mode (line mode or interactive login)	tty, vty, aux, con	login, exec, nasi connection, enable, command
Packet mode (interface mode or link protocol session)	async, group-async, BRI, PRI, serial, dialer profiles, dialer rotaries	ppp, network

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-11.4

Understanding router access modes is the key to understanding the AAA commands and how they work to secure your network access server.

With the exception of the **aaa accounting system** command, all the AAA commands apply to either character mode or packet mode. The mode refers to the format of the packets requesting AAA. If the query is presented as Service-Type = Exec-User, it is presented in character mode. If the request is presented as Service-Type = Framed-User and Framed-Type = PPP, it is presented in packet mode.

Character mode allows a network administrator with a large number of routers in the network to authenticate one time as the user, and then access all the routers configured in this method. The figure shown here can help you decode the meaning of an AAA command by associating the AAA command element with the connection mode to the router.

Primary applications for the Cisco Secure ACS include securing dialup access to a network and securing the management of routers within a network. Both applications have unique AAA requirements.

With the Cisco Secure ACS, system administrators can select a variety of authentication methods, each providing a set of authorization privileges. These router ports must be secured using the Cisco IOS software and a Cisco Secure ACS server.

AAA Protocols

This topic describes the most popular AAA protocols.

The image shows a slide titled "AAA Protocols" with the Cisco.com logo in the top right corner. It features a comparison table between TACACS+ and RADIUS. The table has three rows and three columns. The first column lists the comparison criteria: "AAA Protocols", "Layer 3 Protocol", "Encryption", and "Standard". The second column lists the features for TACACS+, and the third column lists the features for RADIUS. The table is styled with a dark green header and alternating light and dark green rows.

AAA Protocols	TACACS+	RADIUS
Layer 3 Protocol	TCP/IP	UDP/IP
Encryption	Entire Body	Password Only
Standard	Cisco	Open/IETF

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—11-5

The best-known and best-used types of AAA protocols are TACACS+ and RADIUS. TACACS+ supersedes older versions of TACACS and XTACACS. TACACS+ and RADIUS have different features that make them suitable for different situations.

For example, RADIUS is maintained by a standard that was created by the Internet Engineering Task Force (IETF); TACACS+ is a proprietary Cisco Systems technology that encrypts data. Another key difference is that TACACS+ runs in TCP while RADIUS operates in User Datagram Protocol (UDP).

TACACS+ provides many benefits for configuring Cisco devices to use AAA for management and terminal services. TACACS+ can control the authorization level of users, while RADIUS cannot. Also, because TACACS+ separates authentication and authorization, it is possible to use TACACS+ authorization and accounting while using another method of authentication such as Kerberos.

AAA and the Cisco Secure ACS

This topic describes how to enable AAA and identify the Cisco Secure ACS.

Enabling AAA and Identifying the Server

Cisco.com

TACACS+ or RADIUS

```
router(config)# aaa new-model
router(config)# tacacs-server host 192.168.229.76
                    single-connection
router(config)# tacacs-server key shared1
```

OR

```
router(config)# aaa new-model
router(config)# radius-server host 192.158.229.76
router(config)# radius-server key shared1
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-11-6

The first steps in configuring the network access server are as follows:

- Globally enable AAA to allow the use of all AAA elements. This step is a prerequisite for all other AAA commands.
- Specify the Cisco Secure ACS that will provide AAA services for the network access server.
- Configure the encryption key that will be used to encrypt the data transfer between the network access server and the Cisco Secure ACS.

The table shows commonly used AAA configuration commands and what the commands enable.

Commonly Used AAA Commands

Command	Description
aaa new-model	Enables AAA on the router. Prerequisite for all other AAA commands.
tacacs-server host <i>ip-address</i> single-connection	Indicates the address of the Cisco Secure ACS server and specifies use of the TCP single-connection feature of Cisco Secure ACS. This feature improves performance by maintaining a single TCP connection for the life of the session between the network access server and the Cisco Secure ACS server, rather than opening and closing TCP connections for each session (the default).
tacacs-server key <i>key</i>	Establishes the shared secret encryption key between the network access server and the Cisco Secure ACS server.
radius-server host <i>ip-address</i>	Specifies a RADIUS AAA server.
radius-server key <i>key</i>	Specifies an encryption key to be used with the RADIUS AAA server.


AAA Authentication Commands

This topic describes how to configure AAA authentication.

AAA Authentication Commands

Cisco.com

```
router(config)#aaa authentication login
[default | list-name]
group [group-name | radius | tacacs+]
[method2 [method3 [method4]]]
```



```
enable
group
krb5
line
local
local-case
none
```

Example:

```
router(config)#aaa authentication login default group tacacs+
local line
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-11.7

The **authentication login** command in global configuration mode enables the AAA authentication process, as follows:

- **default:** This command creates a default that is automatically applied to *all* lines and interfaces, specifying the method or sequence of methods for authentication.
- **list-name:** This command creates a list, with a name of your choosing, that is applied explicitly to a line or interface using the method or methods specified. This defined list overrides the default when applied to a specific line or interface.
- **group {group-name | radius | tacacs+}:** This method specifies the use of an AAA server. The **group radius**, **group tacacs+** method refers to previously defined RADIUS or TACACS+ servers. The group-name string allows the use of a predefined group of RADIUS or TACACS+ servers for authentication (created with the **aaa group server radius** or **aaa group server tacacs+** command).
- **[method2 [method3 [method4]]]:** This command executes authentication methods in the listed order. If an authentication method returns an error, such as a timeout, the Cisco IOS software attempts to execute the next method. If the authentication fails, access is denied. You can configure up to four methods for each operation. The method must be supported by the authentication operation specified. A general list of methods includes:
 - **enable:** Uses the enable password for authentication
 - **group:** Uses server-group
 - **krb5:** Uses Kerberos Version 5 for authentication
 - **line:** Uses the line password for authentication
 - **local:** Uses the local username and password database for authentication
 - **local-case:** Uses case-sensitive local username authentication
 - **none:** Uses no authentication

Character Mode Login Example

This topic provides an example of how to configure character mode login using AAA authentication.

Character Mode Login Example

Cisco.com

```
router(config)#aaa authentication login default group
tacacs+ local
router(config)#aaa authentication login my_list group
tacacs+
router(config)line con 0
router(config-line)#login authentication my_list
router(config-line)#line 1 48
router(config-line)#login authentication my_list
router(config-line)#line vty 0 4 (this implies "default" list)
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-11-8

This table describes how to configure AAA authentication using TACACS+.

AAA Authentication Commands

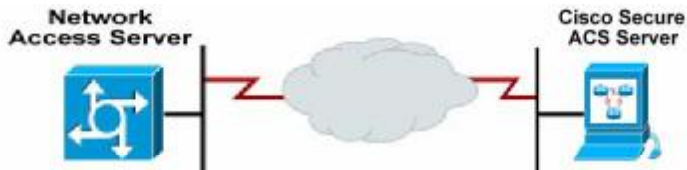
Command	Description
aaa authentication login default group tacacs+ local	The default login is TACACS+ server. If no response from the server, then use the local username and password database.
aaa authentication login my_list group tacacs+	Used for character mode username and password challenge. A new list name, my_list , is defined, and the only method is TACACS+.
line con 0	Enters console configuration mode.
login authentication my_list	Configures the console line to use the AAA list name my_list , which has been previously defined to use only TACACS+.
line 1 48 login authentication my_list	Configures lines 1 through 48 to use the AAA list name my_list , which has been previously defined to use only TACACS+.
line vty 0 4	On lines vty 0 through 4, the default list is used, which in this case specifies the aaa authentication login default tacacs+ local command.

AAA Authorization Commands

This topic describes how to enable AAA authorization.

AAA Authorization Commands

Cisco.com



The diagram illustrates the connection between a Network Access Server (NAS) and a Cisco Secure ACS Server. The NAS is represented by a blue square with a white circular arrow icon. The ACS Server is represented by a blue laptop icon. A red lightning bolt symbol indicates a network connection between the two servers, passing through a central grey cloud representing the network.

```
router(config)#aaa authorization
{network | exec | commands level | config-commands | reverse-
access} [default|list-name] method1 [method2..]
```

Example:

```
router(config)#aaa authorization exec default group radius
local none
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-11.9

You can configure the access server to restrict the user to perform certain functions only after successful authentication. Use the **aaa authorization** command in global configuration mode to select the function authorized and the method of authorization, as shown in the table.

AAA Authorization Commands

Command	Description
network	All network services, including Serial Line Internet Protocol (SLIP), PPP, and AppleTalk Remote Access Protocol (ARA Protocol).
exec	EXEC process.
commands level	All EXEC commands at the specified level (0–15).
config-commands	For configuration mode commands.
reverse-access	For reverse Telnet connections.
if-authenticated	It allows the user to use the requested function if the user is authenticated.
local	Uses the local database for authorization (with the username password commands).
none	Performs no authorization.
group radius	Uses RADIUS for authorization.
group tacacs+	Uses TACACS+ for authorization.

Character Mode with Authorization

This topic illustrates an example of how to configure character mode authorization.

Character Mode with Authorization Example

Cisco.com

```
router(config)# username admin password cisco
router(config)# aaa new-model
router(config)# aaa authentication login default local
router(config)# aaa authentication enable default
                group tacacs+ enable
router(config)# aaa authorization exec default
                group tacacs+ local
router(config)# aaa authorization command 1 default
                group tacacs+ local
router(config)# aaa authorization command 15 default
                group tacacs+ local
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1-11-10

Character mode with authorization commands are shown in the table.

Example of AAA Command Usage

Command	Description
aaa authentication enable default group tacacs+ enable	Determines if the user can access the enabled command level. If authentication via TACACS+ server is unavailable, then use the enable password.
aaa authorization exec default group tacacs+ local	Determines if the user is allowed access to an EXEC shell and, if so, which shell attributes are permitted or denied. The method is TACACS+. If there is no response from the TACACS+ server, then the method is local, using the local username and password database.
aaa authorization command <i>n</i> default group tacacs+ local	Runs authorization for all commands at the specified privilege level (<i>n</i>). It is possible to have every line entered by a user authorized by TACACS+.

Packet Mode Example

This topic illustrates an example of how to configure packet mode authorization.

Packet Mode Example

Cisco.com

```
router(config)#username admin password xxxx
router(config)#aaa authentication ppp default if-needed
                    group tacacs+
router(config)#aaa authentication ppp user if-needed
                    group tacacs+
router(config)#aaa authorization network default
                    group tacacs+ if-authen
router(config)#interface group-async1
router(config-if)#ppp authentication chap (default list implied)
router(config-if)#interface async16
router(config-if)#ppp authentication chap user
router(config-if)#line 1 16
```

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—11-11

The table contains descriptions of the commands that are used in the example configuration.

Example of AAA Packet Mode Command Usage

Command	Description
username admin password password	Creates or adds to the local database a username of admin and the specified password.
aaa authentication ppp user if-needed group tacacs+	Used for packet mode username /password challenge. Creates a list called user that specifies the first method as if-needed and the second as TACACS+. If the user has already been authenticated on a tty line, the first method, if needed, uses that as proof of authentication. If the user has not already been authenticated, TACACS + is used.
aaa authorization network default group tacacs+ if-authenticated	Determines if the user is permitted to make packet mode connections. If so, specifies what packet mode attributes are permitted or denied. Method is TACACS+. If no response from TACACS+, checks if user has been authenticated.
interface async16 ppp authentication chap user	On line async16, uses list user for CHAP authentication.
line 1 16	On lines 1 to 16, uses default list.

AAA Accounting Commands

This topic describes how to use AAA accounting commands.

AAA Accounting Commands

Cisco.com

```
router(config)#aaa accounting
{command level | connection | exec | network | system}
(default | list-name) {start-stop | stop-only |
wait-start} group {tacacs+ | radius}
```

© 2004 Cisco Systems, Inc. All rights reserved.
BCRAN v2.1-11-12

Use the **aaa accounting** command in global configuration mode for auditing and billing purposes, as shown in the following table.

Example of AAA Accounting Command Usage

Command	Description
command level	Audits all commands at the specified privilege level (0–15).
connection	Audits all outbound connections such as Telnet, rlogin.
exec	Audits the EXEC process.
network	Audits all network service requests, such as SLIP, PPP, and ARAP.
system	Audits all system-level events, such as reload.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice has been received by the accounting server.
stop-only	Sends a stop accounting notice at the end of the requested user process.
wait-start	As in start-stop , sends both a start and a stop accounting notice to the accounting server. With the wait-start keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.
group {tacacs+ radius}	Uses TACACS+ for accounting, or enables RADIUS-style accounting.

AAA Accounting Example

This topic provides an example of how to configure AAA accounting.

Accounting Example

Cisco.com

Typical Output:

```
Wed Dec 4 04:47:46 2002
NAS -IP-Address = "172.16.24.127"
NAS -Port = 5
User-Name = "jdoe"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed -IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Input-Octets = 3075
Acct-Output-Octets = 167
Acct-Input-Packets = 33
Acct-Output-Packets = 9
Acct-Session-Time = 171
Acct-Delay-Time = 0
User-Id = "jdoe"
NAS-Identifier = "172.16.24.127"
```

© 2004 Cisco Systems, Inc. All rights reserved.BCRAN v2.1-11-13

The Cisco Secure ACS serves as a central repository for accounting information by completing the access control functionality. Accounting essentially tracks events occurring on the network.

Each session that is established through the Cisco Secure ACS can be fully accounted for and stored on the server. This stored information can be very helpful for management, security audits, capacity planning, and network usage billing.

The table contains the descriptions of commands that are used in the example configuration.

AAA Accounting Commands

Command	Description
aaa accounting network default start-stop group tacacs+	Runs start-stop accounting for all packet mode service requests and uses the TACACS+ server
aaa accounting exec default start-stop group tacacs+	Runs start-stop accounting for all character mode service requests and uses the TACACS+ server
aaa accounting command 15 default start-stop group tacacs+	Runs start-stop accounting for all commands at privilege level 15
aaa accounting connection default start-stop group tacacs+	Runs start-stop accounting for all outbound Telnet and rlogin sessions
aaa accounting system default start-stop group tacacs+	Runs start-stop accounting for all system-level events not associated with users, such as configuration changes and reloads

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Authentication, authorization, and accounting are used to effectively control network access.**
- **Authentication determines the identity of users and whether they should be allowed to access the network.**
- **Authorization allows network managers to limit the network services available to each user.**
- **Accounting keeps track of connection time and resources used on the network.**

© 2004 Cisco Systems, Inc. All rights reserved. BCRAN v2.1—11-14

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 11-1: Using AAA to Scale Access Control

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which process in AAA identifies a user?
- A) authentication
 - B) authorization
 - C) accounting
- Q2) In a remote access network, where should you configure AAA to authenticate incoming traffic to the central site?
- A) on the remote nodes
 - B) on the central site router
 - C) on the AAA server between the central site and the remote sites
 - D) only on the TACACS+ or RADIUS server
- Q3) Which part of the packet does TACACS+ encrypt?
- A) username
 - B) password
 - C) authentication services
 - D) all of the above
- Q4) Which command is required to implement AAA on a Cisco router?
- A) **aaa accounting**
 - B) **aaa new-model**
 - C) **aaa authorization**
 - D) **tacacs-server host**
- Q5) Which command enables the authentication process?
- A) **aaa new-model**
 - B) **aaa authentication login**
 - C) **radius-server key**
 - D) **aaa authenticate**
- Q6) The command **line con 0** is used to enter the console configuration mode.
- A) true
 - B) false

- Q7) What does the **aaa authorization** command allow you to do?
- A) authorize which users can log in
 - B) bypass authentication for a user
 - C) specify who can establish a Telnet session on the router
 - D) specify which commands a user may use
- Q8) It is impossible to have every line entered by a user authorized by TACACS+.
- A) true
 - B) false
- Q9) In which command mode is the **line 1 16** command issued?
- A) router(config)#
 - B) router(config-if)#
 - C) router#
 - D) router>
- Q10) Which **aaa accounting** keyword will audit Telnet traffic?
- A) **exec**
 - B) **network**
 - C) **system**
 - D) **connection**
- Q11) Which command will run start-stop accounting for all character mode service requests?
- A) **aaa accounting network default start-stop group tacacs+**
 - B) **aaa accounting exec default start-stop group tacacs+**
 - C) **aaa accounting connection default start-stop group tacacs+**

Quiz Answer Key

- Q1) A
Relates to: AAA Definitions
- Q2) B
Relates to: Router Access Modes
- Q3) D
Relates to: AAA Protocols
- Q4) B
Relates to: AAA and the Cisco Secure ACS
- Q5) B
Relates to: AAA Authentication Commands
- Q6) A
Relates to: Character Mode Login Example
- Q7) D
Relates to: AAA Authorization Commands
- Q8) B
Relates to: Character Mode with Authorization
- Q9) A
Relates to: Packet Mode Example
- Q10) D
Relates to: AAA Accounting Commands
- Q11) B
Relates to: AAA Accounting Example

BCRAN

Course Glossary

The Course Glossary for *Building Cisco Remote Access Networks* (BCRAN) v2.1 highlights and defines key terms and acronyms used throughout this course. Many of these terms are also described in the Cisco Internetworking Terms and Acronyms resource, available via <http://www.cisco.com>.

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
802.x		IEEE standards that define LAN protocols	A set of IEEE standards for the definition of LAN protocols.	ITA/Jan 2003
A&B bit signaling		T1 transmission facilities in which each of the 24 T1 subchannels devotes 1 bit of every sixth frame to signaling	Procedure used in T1 transmission facilities in which each of the 24 T1 subchannels devotes 1 bit of every sixth frame to the carrying of supervisory signaling information. Also called 24th channel signaling.	ITA/Jan 2003
AAA	authentication, authorization, and accounting	authentication, authorization, and accounting	Pronounced "triple A." In security, authentication is the verification of the identity of a person or a process. Authorization is The method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of protocols such as IP and telnet. Accounting is responsible for collecting network data relating to resource usage.	ITA/Jan 2003
Access-Accept		RADIUS server notifying the access server that the user is authenticated	Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.	ITA/Jan 2003
Access-Challenge		RADIUS server requesting that the user supply additional information	Response packet from the RADIUS server requesting that the user supply additional information before being authenticated.	ITA/Jan 2003
Access-Request		Request for authentication sent to the RADIUS server	Request packet sent to the RADIUS server by the access server requesting authentication of the user.	ITA/Jan 2003
Acknowledgment		Notification that some event occurred	Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message). Sometimes abbreviated ACK. Compare to NAK.	ITA/Jan 2003
ACL	access list	A list used to permit or deny access or other services	A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).	ITA/Jan 2003
Activation		process of enabling a subscriber device for network access and privileges	The process of enabling a subscriber device for network access and privileges on behalf of a registered account.active discovery packet. The type of packet used by PPPoE during the discovery stage.	ITA/Jan 2003
address		Data structure used to identify a unique entity	Data structure or logical convention used to identify a unique entity, such as a particular process or a network device.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
address mask		Bit combination that describes which address parts refer to the network and the host	A bit combination used to describe which part of an address refers to the network or the subnet and which part refers to the host. Sometimes referred to simply as mask.	ITA/Jan 2003
address resolution		Method for resolving differences between computer addressing schemes	Generally, a method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network layer (Layer 3) addresses to data-link layer (Layer 2) addresses.	ITA/Jan 2003
ADM	add/drop multiplexer	Digital multiplexing equipment that provides interfaces between different signals in a network.	Digital multiplexing equipment that provides interfaces between different signals in a network.	ITA/Jan 2003
administrative distance		Rating of the trustworthiness of a routing information source	Rating of the trustworthiness of a routing information source. Administrative distance often is expressed as a numerical value between 0 and 255. The higher the value, the lower the trustworthiness rating.	ITA/Jan 2003
ADSL	asymmetric digital subscriber line	One of four DSL technologies.	One of four DSL technologies. ADSL is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. Downstream rates range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair. See also HDSL, SDSL, and VDSL.	ITA/Jan 2003
ADTS	automated digital terminal system			BCRAN Mod6
AES	Advanced Encryption Standard		A new symmetric encryption algorithm selected by NIST in a public process. AES is set to replace DES mainly because of its longer keys and smaller computing resources needed. It is already available in a number of VPN products.	BCRAN Mod5
aggressive mode		Connection mode that eliminates several steps during IKE authentication	The connection mode that eliminates several steps during IKE authentication negotiation (phase 1) between two or more IPSec peers. Aggressive mode is faster than main mode but not as secure.	ITA/Jan 2003
AH	Authentication Header	Security protocol that provides data authentication using fields embedded in the datagram	A security protocol that provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
AIS	alarm indication signal	An all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity for T1	In a T1 transmission, an all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity and to indicate to the receiving terminal that there is a transmission fault that is located either at, or upstream from, the transmitting terminal. See also T1.	ITA/Jan 2003
AMI	alternate mark inversion	Line-code type used on T1 and E1 circuits.	Line-code type used on T1 and E1 circuits. In AMI, zeros are represented by 01 during each bit cell, and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary coded alternate mark inversion. Compare with bipolar 8-zero substitution. See also ones density.	ITA/Jan 2003
ANSI	American National Standards Institute	Organization that helps develop international and U.S. standards relating to, among other things, communications and networking	A voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking.	ITA/Jan 2003
antenna		A device for transmitting or receiving a radio frequency (RF).	A device for transmitting or receiving a radio frequency (RF). Antennas are designed for specific and relatively tightly defined frequencies and are quite varied in design. An antenna for a 2.5 GHz (MMDS) system does not work for a 28 GHz (LMDS) design.	ITA/Jan 2003
Antenna Site		The location of main receiving antennas for broadcast and satellite reception.	The location of main receiving antennas for broadcast and satellite reception.	BCRAN Mod11
application		Program that performs a function directly for a user	A program that performs a function directly for a user. FTP and Telnet clients are examples of network applications.	ITA/Jan 2003
area		Logical set of network segments and their attached devices	A logical set of network segments (OSPF-based) and their attached devices. Areas usually are connected to other areas via routers, making up a single autonomous system. See also autonomous system.	ITA/Jan 2003
ARP	Address Resolution Protocol	Protocol used to map an IP address to a MAC address	Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
ARPA	Advanced Research Projects Agency Network			BCRAN Mod6
assigned numbers		RFC that documents the currently assigned values from several series of numbers used in network protocol implementations	RFC [STD2] documents the currently assigned values from several series of numbers used in network protocol implementations. This RFC is updated periodically, and current information can be obtained from the IANA. If you are developing a protocol or an application that requires the use of a link, a socket, a port, a protocol, and so on, contact the IANA to receive a number assignment.	ITA/Jan 2003
asynchronous transmission		Digital signals that are transmitted without precise clocking	Term describing digital signals that are transmitted without precise clocking. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and the end of each character. Compare with isochronous transmission, plesiochronous transmission, and synchronous transmission.	ITA/Jan 2003
ATM	Asynchronous Transfer Mode	Standard that conveys multiple service types in fixed-length cells	The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.	ITA/Jan 2003
authentication		In security, verification of the identity of a person or a process	In security, the verification of the identity of a person or a process.	ITA/Jan 2003
autonomous system		Networks under a common administration that share a routing strategy	A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA. Sometimes abbreviated as AS.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
B8ZS	binary 8-zero substitution	Line-code type, used on T1 and E1 circuits, in which a special code is substituted whenever eight consecutive zeros are sent over the link.	Line-code type, used on T1 and E1 circuits, in which a special code is substituted whenever eight consecutive zeros are sent over the link. This code then is interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream. Sometimes called bipolar 8-zero substitution. Compare with AMI. See also ones density.	ITA/Jan 2003
B channel	Bearer channel	DS0 time slot that carries analog voice or digital data over ISDN	DS0 time slot that carries analog voice or digital data over ISDN. In ISDN, a full-duplex, 64-kbps channel used to send user data.	ITA/Jan 2003
backbone		Part of a network that acts as the primary path for traffic	Part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.	ITA/Jan 2003
bandwidth		Difference between the highest and lowest frequencies for network signals	The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.	ITA/Jan 2003
baseband		Characteristic of a network technology where only one carrier frequency is used	Characteristic of a network technology where only one carrier frequency is used. Ethernet is an example of a baseband network. Also called narrowband. Contrast with broadband.	ITA/Jan 2003
baud		Unit of signaling speed where each signal element represents exactly 1 bit	Unit of signaling speed equal to the number of discrete signal elements transmitted per second. Baud is synonymous with bits per second (bps) if each signal element represents exactly 1 bit.	ITA/Jan 2003
Bc	committed burst	Maximum amount of data in a Frame Relay network committed to accept and transmit	Negotiated tariff metric in Frame Relay internetworks. The maximum amount of data (in bits) that a Frame Relay internetwork is committed to accept and transmit at the CIR.	ITA/Jan 2003
Be	excess burst	Number of bits that a Frame Relay network transmits after Bc	Negotiated tariff metric in Frame Relay internetworks. The number of bits that a Frame Relay internetwork attempts to transmit after Bc is accommodated. Be data, in general, is delivered with a lower probability than Bc data because Be data can be marked as DE by the network.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
BECN	backward explicit congestion notification	Bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path.	Bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path. DTE receiving frames with the BECN bit set can request that higher-level protocols take flow control action as appropriate. Compare with FECN. Cisco routers can respond to BECN notifications	ITA/Jan 2003 and BCRA Mod7
BER	bit error rate	Ratio of received bits that contain errors.	Ratio of received bits that contain errors.	ITA/Jan 2003
BERT	bit error rate tester	Device that determines the BER on a given communications channel	Device that determines the BER on a given communications channel. See also BER (bit error rate).	ITA/Jan 2003
best-effort delivery		A network system that does not use a sophisticated acknowledgment system for delivery of information.	Describes a network system that does not use a sophisticated acknowledgment system to guarantee reliable delivery of information.	ITA/Jan 2003
BISDN	Broadband ISDN	ITU-T communication standards designed to handle high-bandwidth applications, such as video.	ITU-T communication standards designed to handle high-bandwidth applications, such as video. BISDN currently uses ATM technology over SONET-based transmission circuits to provide data rates from 155 to 622 Mbps and beyond. Contrast with N-ISDN. See also BRI, ISDN, and PRI.	ITA/Jan 2003
bit-oriented protocol		Class of data link layer communication protocols that can transmit frames regardless of frame content	Class of data link layer communication protocols that can transmit frames regardless of frame content. Unlike byte-oriented protocols, bit-oriented protocols provide full-duplex operation and are more efficient and reliable. Compare with byte-oriented protocol.	ITA/Jan 2003
blocking		A situation in which one activity or path cannot begin or be used until capacity is returned.	In a switching system, a condition in which no paths are available to complete a circuit. The term also is used to describe a situation in which one activity cannot begin until another is completed.	ITA/Jan 2003
BOC	Bell operating company	Phone companies formed by the breakup of AT&T	The several local phone companies formed by the breakup of AT&T. See also RBOC.	ITA/Jan 2003
BPDU	bridge protocol data unit	Spanning-Tree Protocol hello packet used when exchanging information among bridges	Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.	WIP/June 2002
BPV	bipolar violation	A one (1) in a bipolar signal that has the same polarity as the preceding one.	A one (1) in a bipolar signal that has the same polarity as the preceding one. See also coding violation.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
BRI	Basic Rate Interface	ISDN interface composed of two B channels and one D channel	ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data.	ITA/Jan 2003
bridge		Device that connects network segments that use the same protocol	Device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data-link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame.	ITA/Jan 2003
bridge static filtering		Process in which a bridge maintains a filtering database	The process in which a bridge maintains a filtering database consisting of static entries. Each static entry equates a MAC destination address with a port that can receive frames with this MAC destination address and a set of ports on which the frames can be transmitted. Defined in the IEEE 802.1 standard.	ITA/Jan 2003
Broadband		Refers to the ability to frequency-division multiplex (FDM) many signals in a wide RF bandwidth over an HFC network, and the ability to handle vast amounts of information.	Refers to the ability to frequency-division multiplex (FDM) many signals in a wide RF bandwidth over an HFC network, and the ability to handle vast amounts of information.	BCRAN Mod11
broadband		Transmission system that multiplexes multiple independent signals onto one cable having a bandwidth greater than a voice-grade channel (4 kHz).	1. Describes facilities or services that operate at the DS3 rate and above. For example, a Broadband DCS makes cross-connections at the DS3, STS-1, and STS-Nc levels. Similarly, Broadband ISDN provides about 150 Mb/s per channel of usable bandwidth. 2. Transmission system that multiplexes multiple independent signals onto one cable. 3. Telecommunications terminology: Any channel having a bandwidth greater than a voice-grade channel (4 kHz). 4. LAN terminology: A coaxial cable on which analog signaling is used. An RF system with a constant data rate at or above 1.5 Mbps. Also called wideband. Contrast with baseband.	ITA/Jan 2003
broadcast		Data packets that are sent to all nodes on a network	Data packets that are sent to all nodes on a network. Broadcasts are identified by a broadcast address.	ITA/Jan 2003
broadcast address		Special address reserved for sending a message to all stations	A special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
broadcast domain		All devices that receive broadcast frames originating from any device within the set	Set of all devices that receive broadcast frames originating from any device within the set. Broadcast domains typically are bounded by routers because routers do not forward broadcast frames.	ITA/Jan 2003
broadcast storm		Network event where many broadcasts are sent simultaneously across all network segments	An undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.	ITA/Jan 2003
burst		Sequence of signals counted as one unit based on a specific measure	In data communications, a sequence of signals counted as one unit in accordance with some specific criterion or measure.	ITA/Jan 2003
bursty traffic		An uneven pattern of data transmission	A data communications term referring to an uneven pattern of data transmission.	ITA/Jan 2003
CA certificate	Certificate of Authority certificate	Certificate of Authority certificate	[Digital] certificate for one CA issued by another CA.	ITA/Jan 2003
cable		Transmission medium of copper wire or optical fiber wrapped in a protective cover.	Transmission medium of copper wire or optical fiber wrapped in a protective cover.	ITA/Jan 2003
cable modem		Modem that at subscriber locations to convey data communications on a cable television system.	Modulator-demodulator device that is placed at subscriber locations to convey data communications on a cable television system.	ITA/Jan 2003
cable router		Router optimized for data-over-CATV hybrid fiber-coaxial	Modular chassis-based router optimized for data-over-CATV hybrid fiber-coaxial (HFC) applications.	ITA/Jan 2003
call		An attempted connection between remote systems	An attempted connection between remote systems, such as a telephone call through the PSTN.	ITA/Jan 2003
CAP	carrierless amplitude/ phase	An earlier and more easily implemented modulation used on many of the early installations of ADSL.	An earlier and more easily implemented modulation used on many of the early installations of ADSL.	BCRAN Mod11
CATV	Cable TV	Originally an acronym for community antenna television; today the term is generally accepted to mean cable TV. A system where multiple channels of programming material are transmitted to homes using broadband coaxial cable	A communication system where multiple channels of programming material are transmitted to homes using broadband coaxial cable. Formerly called Community Antenna Television.	ITA/Jan 2003 and BCRAN Mod11

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
cause codes		The coded reason for ISDN call failure or completion.	Code that indicates the reason for ISDN call failure or completion.	ITA/Jan 2003
CBDS	Connectionless Broadband Data Service.	European high-speed, packet-switched, datagram-based WAN networking technology.	European high-speed, packet-switched, datagram-based WAN networking technology.	ITA/Jan 2003
CBWFQ	class-based weighted fair queuing	Defines traffic classes (typically using ACLs) and then applies parameters, such as bandwidth and queue-limits to these classes.	The bandwidth assigned to a class is used to calculate the "weight" of that class. The weight of each packet that matches the class criteria is also calculated from this. WFQ is then applied to the classes (which can include several flows) rather than the flows themselves.	BCRAN Mod9
CCITT	Consultative Committee for International Telegraph and Telephone	International organization responsible for the development of communications standards. Now called the ITU-T.	International organization responsible for the development of communications standards. Now called the ITU-T. See also ITU-T.	ITA/Jan 2003
CD	Carrier Detect	A signal that indicates whether an interface is active	A signal that indicates whether an interface is active. Also, a signal generated by a modem indicating that a call has been connected.	ITA/Jan 2003
CDP	Cisco Discovery Protocol	Cisco protocol that allows a device to advertise its existence and receive information about other devices	Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.	ITA/Jan 2003
CET	Cisco Encryption Technology		40- and 56-bit DES network layer encryption available since Cisco IOS Software Release 11.2.	BCRAN Mod5
channel		Communication path	<p>1. Communication path wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments.</p> <p>2. In IBM, the specific path between large computers (such as mainframes) and attached peripheral devices.</p> <p>3. Specific frequency allocation and bandwidth. Downstream channels are used for television in the United States are 6 MHz wide.</p>	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
channelized E1		Access link operating at 2.048 Mbps that is subdivided into 30 B-channels and 1 D-channel	Access link operating at 2.048 Mbps that is subdivided into 30 B-channels and 1 D-channel. Supports DDR, Frame Relay, and X.25. Compare with channelized T1	ITA/Jan 2003
channelized T1		Access link operating at 1.544 Mbps that is subdivided into 24 channels (23 B channels and 1 D channel) of 64 kbps each.	Access link operating at 1.544 Mbps that is subdivided into 24 channels (23 B channels and 1 D channel) of 64 kbps each. The individual channels or groups of channels connect to different destinations. Supports DDR, Frame Relay, and X.25. Also called fractional T1.	ITA/Jan 2003
CHAP	Challenge Handshake Authentication Protocol	Security feature supported on lines using PPP encapsulation	Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.	ITA/Jan 2003
chat script		String of text that defines the login "conversation" that occurs between modems.	String of text that defines the login "conversation" that occurs between two systems. Consists of expect-send pairs that define the string that the local system expects to receive from the remote system and what the local system should send as a reply.	ITA/Jan 2003
checksum		Method for checking the integrity of transmitted data using an integer value	Method for checking the integrity of transmitted data. A checksum is an integer value computed from a sequence of octets taken through a series of arithmetic operations. The value is recomputed at the receiving end and is compared for verification.	ITA/Jan 2003
Cipher		Cryptographic algorithm for encryption and decryption.	Cryptographic algorithm for encryption and decryption.	ITA/Jan 2003
Ciphertext		Data encrypted so that its meaning is no longer intelligible or directly available	Data that has been transformed by encryption so that its semantic information content (that is, its meaning) is no longer intelligible or directly available	ITA/Jan 2003
CIR	committed information rate	Rate at which a Frame Relay network agrees to transfer information	The rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. CIR, measured in bits per second, is one of the key negotiated tariff metrics.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
Cisco IOS		Software that provides common functionality for Cisco products	Cisco Systems software that provides common functionality, scalability, and security for all Cisco products. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while ensuring support for a wide variety of protocols, media, services, and platforms.	ITA/Jan 2003
CLI	command-line interface	Interface that allows the user to interact with the operating system	An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.	ITA/Jan 2003
CLID	calling line ID	Information about the telephone number from which a call originated.	Information about the billing telephone number from which a call originated. The CLID value might be the entire phone number, the area code, or the area code plus the local exchange. Also known as Caller ID.	ITA/Jan 2003
CM	cable modem	Device used to connect a PC to a local cable TV line	Device used to connect a PC to a local cable TV line and receive data at much higher rates than ordinary telephone modems or ISDN. A cable modem can be added to or integrated with a set-top box, thereby enabling Internet access via a television set. In most cases, cable modems are furnished as part of the cable access service and are not purchased directly and installed by the subscriber.	ITA/Jan 2003
CMI	coded mark inversion	ITU-T line coding technique specified for STS-3c transmissions	ITU-T line coding technique specified for STS-3c transmissions. Also used in DS-1 systems. See also DS-1 and STS-3c.	ITA/Jan 2003
CMTS	cable modem termination system	Any DOCSIS-compliant headend cable router	A cable modem termination system, such as a router or a bridge, typically located at the cable headend. Any DOCSIS-compliant headend cable router, such as the Cisco uBR7246.	ITA/Jan 2003
CNR	Carrier-to-noise	The difference in amplitude between the desired RF carrier and the noise in a defined bandwidth.	The difference in amplitude between the desired RF carrier and the noise in a defined bandwidth.	BCRAN Mod11
CO	central office	Local telephone company office to which all local loops in an area connect	The local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.	ITA/Jan 2003
coaxial cable		The principal physical media with which CATV systems are built.	Coaxial cable is used to transport RF signals. Coaxial cable signal loss (attenuation) is a function of the diameter of the cable, dielectric construction, ambient temperature, and operating frequency (f).	BCRAN Mod11

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
codec	coder-decoder	Device that transforms analog signals into a digital bit stream and digital signals back into analog signals.	<p>1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.</p> <p>2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.</p>	ITA/Jan 2003
collision		In Ethernet, result of two nodes transmitting simultaneously	In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.	ITA/Jan 2003
collision domain		Network area within which frames that have collided are propagated	In Ethernet, the network area within which frames that have collided are propagated. Repeaters and hubs propagate collisions; LAN switches, bridges, and routers do not.	ITA/Jan 2003
communications line		Physical link that connects devices to other devices	Physical link (such as wire or a telephone circuit) that connects one or more devices to one or more other devices.	ITA/Jan 2003
configuration register		User-configurable value that determines how a Cisco router initializes	In Cisco routers, a 16-bit, user-configurable value that determines how the router functions during initialization. The configuration register can be stored in hardware or software. In hardware, the bit position is set using a jumper. In software, the bit position is set by specifying a hexadecimal value using configuration commands.	ITA/Jan 2003
connectionless		Data transfer without a virtual circuit	Term used to describe data transfer without the existence of a virtual circuit.	ITA/Jan 2003
connection-oriented		Data transfer that requires a virtual circuit	Term used to describe data transfer that requires the establishment of a virtual circuit.	ITA/Jan 2003
core router		Router that is part of the backbone in a star topology	In a packet-switched star topology, a router that is part of the backbone and that serves as the single pipe through which all traffic from peripheral networks must pass on its way to other peripheral networks.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
CPE	customer premises equipment	Equipment at customer sites, connected to the telephone company network	Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.	ITA/Jan 2003
cps	cells per second	Unit of measure used for ATM switch volumes.	Unit of measure used for ATM switch volumes.	ITA/Jan 2003
cRTP	compressed Real-Time Transport Protocol		cRTP, RFC 1889, provides bandwidth efficiency over low-speed links by compressing the UDP/RTP/IP header when transporting voice. With cRTP, the header for VoIP traffic can be reduced from 40 bytes to approximately 2 to 5 bytes. cRTP is supported over Frame Relay, ATM, PPP, MLP, and HDLC encapsulated interfaces.	
cryptographic algorithm		Algorithm that employs the science of cryptography	Algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.	ITA/Jan 2003
cryptographic key		Input parameter that varies the transformation performed by a cryptographic algorithm.	Usually shortened to just "key." Input parameter that varies the transformation performed by a cryptographic algorithm.	ITA/Jan 2003
CSU	Channel service unit	Digital interface device that connects end-user equipment to the local digital telephone loop	Digital interface device that connects end-user equipment to the local digital telephone loop. Often referred to together with DSU, as CSU/DSU. See also DSU.	ITA/Jan 2003
CTS	Clear To Send	Clear To Send	Circuit in the EIA/TIA-232 specification that is activated when DCE is ready to accept data from a DTE.	ITA/Jan 2003
custom queuing		Reserves a percentage of bandwidth for specified protocols	Up to 16 output queues can be configured for normal data and an additional queue can be created for system messages such as LAN keepalives. Each queue is serviced sequentially, by transmitting a configurable percentage of traffic and then moving on to the next queue	BCRAN Mod9
D channel	data channel	Full-duplex, 16-kbps (BRI), or 64-kbps (PRI) ISDN channel	Full-duplex, 16-kbps (BRI), or 64-kbps (PRI) ISDN channel.	ITA/Jan 2003
D4 framing		Super Frame	See SF	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
data circuit-terminating equipment		See DCE	See DCE. Also known as data communications equipment	ITA/Jan 2003
data-link layer		Layer 2 of the OSI reference model.	Layer 2 of the OSI reference model. Provides reliable transit of data across a physical link. The data-link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes simply called link layer. Roughly corresponds to the data-link control layer of the SNA model.	ITA/Jan 2003
data terminal equipment		See DTE	See DTE	ITA/Jan 2003
datagram		Logical grouping of information sent as a network layer unit	Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.	ITA/Jan 2003
DCE	data circuit-terminating equipment (ITU-T expansion)	Network connections that comprise the network end of the user-to-network interface	Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.	ITA/Jan 2003
DDR	dial-on-demand routing	Technique whereby a router automatically initiates and closes a circuit-switched session	Technique whereby a router can automatically initiate and close a circuit-switched session as transmitting stations demand. The router spoofs keepalives so that end stations treat the session as active. DDR permits routing over ISDN or telephone lines using an external ISDN terminal adaptor or modem.	ITA/Jan 2003
DE	discard eligible	Traffic that can be dropped if the network is congested	If the network is congested, DE traffic can be dropped to ensure the delivery of higher priority traffic.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
DEA	Data Encryption Algorithm	Symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard	Symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.	ITA/Jan 2003
decrypt		Restore ciphertext to the plaintext form	Cryptographically restore ciphertext to the plaintext form it had before encryption.	ITA/Jan 2003
decryption		Reverse application of an encryption algorithm to encrypted data	Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state. See also encryption.	ITA/Jan 2003
dedicated LAN		Network segment allocated to a single device	Network segment allocated to a single device. Used in LAN switched network topologies.	ITA/Jan 2003
dedicated line		Communications line that is indefinitely reserved for transmissions	Communications line that is indefinitely reserved for transmissions, rather than switched as transmission is required. See also leased line.	ITA/Jan 2003
default route		Routing table entry that directs frames without a next hop in the routing table	Routing table entry that is used to direct frames for which a next hop is not explicitly listed in the routing table.	ITA/Jan 2003
DEK	data encryption key	encryption of message text and for the computation of signatures	Used for the encryption of message text and for the computation of message integrity checks (signatures).	ITA/Jan 2003
delay		Time between a sender transaction and the first response received by the sender	The time between the initiation of a transaction by a sender and the first response received by the sender. Also, the time required to move a packet from source to destination over a given path.	ITA/Jan 2003
demarc		Demarcation point between carrier equipment and CPE	Demarcation point between carrier equipment and CPE.	ITA/Jan 2003
demodulation		Returning a modulated signal to its original form	Process of returning a modulated signal to its original form. Modems perform demodulation by taking an analog signal and returning it to its original (digital) form.	ITA/Jan 2003
demodulator		Device for assembling signals after they have been received by an antenna.	Device for assembling signals after they have been received by an antenna. A demodulator is typically the first major device downstream from an antenna receiving system and exists on the block diagram prior to various Cisco devices. The corresponding device on the transmission side of a system is a modulator.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
demultiplexing		Separating of multiple input streams from a common physical signal back into multiple output streams	Separating of multiple input streams that were multiplexed into a common physical signal back into multiple output streams. See also multiplexing.	ITA/Jan 2003
demux	demultiplexer	Device that separates two or more signals that previously were combined by a compatible multiplexer	Device used to separate two or more signals that previously were combined by a compatible multiplexer and are transmitted over a single channel.	ITA/Jan 2003
DES	Data Encryption Standard	Standard cryptographic algorithm from the U.S. National Bureau of Standards.	Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.	ITA/Jan 2003
designated bridge		Bridge that incurs the lowest path cost when forwarding a frame to the root bridge	Bridge that incurs the lowest path cost when forwarding a frame from a segment to the root bridge.	ITA/Jan 2003
designated router		OSPF router that generates link-state advertisements for a multi-access network	OSPF router that generates link-state advertisements for a multi-access network and has other special responsibilities in running OSPF. Each multi-access OSPF network that has at least two attached routers has a designated router that is elected by the OSPF Hello protocol. The designated router enables a reduction in the number of adjacencies required on a multi-access network, which in turn reduces the amount of routing protocol traffic and the size of the topological database.	ITA/Jan 2003
destination address		Address of a network device that is receiving data	Address of a network device that is receiving data.	ITA/Jan 2003
D-H	Diffie-Hellman	The algorithm in the first system to utilize "public-key" or "asymmetric" cryptographic keys	The Diffie-Hellman algorithm, introduced by Whitfield Diffie and Martin Hellman in 1976, was the first system to utilize "public-key" or "asymmetric" cryptographic keys. Today Diffie-Hellman is part of the IPsec standard. A protocol known as OAKLEY uses Diffie-Hellman, as described in RFC 2412. OAKLEY is used by the Internet Key Exchange (IKE) protocol (see RFC 2401), which is part of the overall framework called Internet Security Association and Key Management Protocol (ISAKMP; see RFC 2408).	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
dial backup		Feature that provides protection against WAN downtime by allowing the network administrator to configure a backup serial line through a circuit-switched connection.	Feature that provides protection against WAN downtime by allowing the network administrator to configure a backup serial line through a circuit-switched connection.	BCRAN Mod6
dial-up line		Communications over a switched-circuit connection using the telephone company network	Communications circuit that is established by a switched-circuit connection using the telephone company network.	ITA/Jan 2003
Dialer interface		logical entity that uses a per-destination dialer profile.	logical entity that uses a per-destination dialer profile.	BCRAN Mod6
Dialer profiles		separate the "logical" configuration from the interface receiving or making calls.	. Profiles can define encapsulation, access control lists, minimum or maximum calls, and turn features on or off	BCRAN Mod6
Diffie-Hellman key exchange		A public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels	A public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange. Cisco IOS software supports 768-bit and 1024-bit Diffie-Hellman groups.	ITA/Jan 2003
digital certificate		Certificate document to which is appended a computed digital signature value	Certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.	ITA/Jan 2003
digital envelope		a combination of encrypted content data and the content encryption key in an encrypted form	Digital envelope for a recipient is a combination of (a) encrypted content data (of any kind) and (b) the content encryption key in an encrypted form that has been prepared for the use of the recipient.	ITA/Jan 2003
digital signature		Value computed with a cryptographic algorithm and appended to a data object to verify the data's origin and integrity	Value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
distance vector routing algorithm		Routing algorithms that use the number of hops to find a shortest-path spanning tree	Class of routing algorithms that iterate on the number of hops in a route to find a shortest-path spanning tree. Distance vector routing algorithms call for each router to send its entire routing table in each update, but only to its neighbors. Distance vector routing algorithms can be prone to routing loops, but are computationally simpler than link-state routing algorithms. Also called Bellman-Ford routing algorithm.	ITA/Jan 2003
Distribution network		In a classic tree-and-branch cable system, trunk and feeder cables comprise the distribution network.	The trunk is the backbone. The trunk distributes signals throughout the community being served. Typically uses 0.750-inch (19 mm) diameter coaxial cable. The feeder branches off of the trunk, and passes all of the homes in the service area. Typically uses 0.500-inch (13 mm) diameter coaxial cable.	BCRAN Mod11
DLCI	data-link connection identifier	Value that specifies a PVC or an SVC in a Frame Relay network	Value that specifies a PVC or an SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant. (Connected devices might use different values to specify the same connection.) In the LMI extended specification, DLCIs are globally significant (DLCIs specify individual end devices).	ITA/Jan 2003
DMT	discrete multitone	The official ANSI and ITU standard for ADSL.	The official ANSI and ITU standard for ADSL.	BCRAN Mod11
DNS	Domain Name System	System used on the Internet for translating names of network nodes into addresses.	System used on the Internet for translating names of network nodes into addresses.	ITA/Jan 2003
DOCSIS	Data-over-Cable Service Interface Specifications	Defines specific bandwidths for data signals (200kHz, 400kHz, 800kHz, 1.6Mh and 3.2MHz), which the cable operator can use.	Defines technical specifications for equipment at both subscriber locations and cable operators' headends. Adoption of DOCSIS will accelerate the deployment of data-over-cable services and will ensure interoperability of equipment throughout system operators' infrastructures.	ITA/Jan 2003 and BCRAN Mod11
DOCSIS CM	DOCSIS cable modem	DOCSIS cable modem	DOCSIS CMs obtain boot configuration using DHCP, Time, and TFTP client implementations.	ITA/Jan 2003
DOCSIS CMTS	DOCSIS cable modem termination system	DOCSIS cable modem termination system	The Cisco 7246 or 7223 router is a leading router implementation of a DOCSIS CMTS	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
DOCSIS configuration file		File containing configuration parameters for a DOCSIS cable modem	File containing configuration parameters for a DOCSIS cable modem. The cable modem obtains this file at boot time using the TFTP protocol.	ITA/Jan 2003
dot address		Common notation for IP addresses in the form <i>n.n.n.n</i>	Refers to the common notation for IP addresses in the form <i>n.n.n.n</i> where each number <i>n</i> represents, in decimal, 1 byte of the 4-byte IP address. Also called dotted notation and four-part dotted notation.	ITA/Jan 2003
dotted decimal notation		Representation of IP addresses on the Internet	Syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. Used to represent IP addresses on the Internet, as in 192.67.67.20. Also called dotted quad notation.	ITA/Jan 2003
DS	downstream	RF signal flow from headend toward subscribers. Also called forward path.	RF signal flow from headend toward subscribers. Also called forward path.	BCRAN Mod1
DS0	digital service zero (0)	Single timeslot on a DS1 (also known as T1) digital interface	Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.	ITA/Jan 2003
DS-0	digital signal level 0	Framing for digital signals over a single channel at 64-kbps on a T1 facility.	Framing specification used in transmitting digital signals over a single channel at 64-kbps on a T1 facility. Compare with DS-1 and DS-3.	ITA/Jan 2003
DS1	digital service 1	Interface with a 1.544-Mbps data rate that often carries voice interface connections on a PBX	Interface with a 1.544-Mbps data rate that often carries voice interface connections on a PBX. Each DS1 (also known as T1) has 24 DS0 channels framed together so that each DS0 timeslot can be assigned to a different type of trunk group, if desired.	ITA/Jan 2003
DS-1	digital signal level 1	Framing for digital signals at 1.544-Mbps on a T1 facility (in the US) or at 2.108-Mbps on an E1 facility (in Europe).	Framing specification used in transmitting digital signals at 1.544-Mbps on a T1 facility (in the United States) or at 2.108-Mbps on an E1 facility (in Europe). Compare with DS-0 and DS-3. See also E1 and T1.	ITA/Jan 2003
DS-3	digital signal level 3	Framing for digital signals at 44.736 Mbps on a T3 facility.	Framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. Compare with DS-0 and DS-1. See also E3 and T.120.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
DSL	digital subscriber line.	Public network technology that delivers high bandwidth over conventional copper wiring at limited distances.	There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.	ITA/Jan 2003
DSLAM	digital subscriber line access multiplexer	A device for multiplexing the DSL traffic onto one or more network trunk lines	A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.	ITA/Jan 2003
DSn	digital signal level n	A classification of digital circuits.	A classification of digital circuits. The DS technically refers to the rate and the format of the signal, whereas the T designation refers to the equipment providing the signals. In practice, DS and T are used synonymously; for example, DS1 and T1, DS3 and T3.	ITA/Jan 2003
DSR	data set ready	EIA/TIA-232 interface circuit that is activated when DCE is powered up and ready for use.	EIA/TIA-232 interface circuit that is activated when DCE is powered up and ready for use.	ITA/Jan 2003
DSU	data service unit	data service unit	Device used in digital transmission that adapts the physical interface on a DTE device to a transmission facility, such as T1 or E1. The DSU also is responsible for such functions as signal timing. Often referred to together with CSU, as CSU/DSU.	ITA/Jan 2003
DTE	data terminal equipment	Device at the user end of a user-network interface that serves as a data source, destination, or both.	Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes such devices as computers, protocol translators, and multiplexers. Compare with DCE .	ITA/Jan 2003
DTR	data terminal ready	data terminal ready	EIA/TIA-232 circuit that is activated to let the DCE know when the DTE is ready to send and receive data.	ITA/Jan 2003
dynamic routing		Routing that adjusts automatically to network topology changes	Routing that adjusts automatically to network topology or traffic changes. Also called adaptive routing.	ITA/Jan 2003
E1		Wide-area digital transmission scheme operating at 2.048 Mbps	Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
E3		European WAN transmission scheme that carries data at a rate of 34.368 Mbps	Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers. Compare with T.120. See also DS-3.	ITA/Jan 2003
EIA	Electronic Industries Alliance	Group that specifies electrical transmission standards	Group that specifies electrical transmission standards. The EIA and the TIA have developed numerous well-known communications standards, including EIA/TIA-232 and EIA/TIA-449. See also TIA.	ITA/Jan 2003
EIA/TIA-232		Common physical layer interface standard for signal speeds of up to 64 kbps	Common physical layer interface standard, developed by EIA and TIA that supports unbalanced circuits at signal speeds of up to 64 kbps. Closely resembles the V.24 specification. Formerly called RS-232.	ITA/Jan 2003
EIGRP	Enhanced Interior Gateway Routing Protocol	Advanced version of IGRP that provides superior convergence and efficiency	Advanced version of IGRP developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link-state protocols with those of distance vector protocols.	ITA/Jan 2003
encapsulation		Wrapping of data in a particular protocol header	Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data-link layer protocol of the other network.	ITA/Jan 2003
encoder		Device that modifies information into the required transmission format.	Device that modifies information into the required transmission format.	ITA/Jan 2003
encryption		Altering the appearance of the data making it incomprehensible to those who are not authorized to see the information	Application of a specific algorithm to data so as to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information. See also decryption.	ITA/Jan 2003
encryption certificate		Public-key certificate that contains a public key	Public-key certificate that contains a public key that is intended to be used for encrypting data, rather than for verifying digital signatures or performing other cryptographic functions.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
end-to-end encryption		Continuous encryption protection of data that flows between two points in a network,	Continuous protection of data that flows between two points in a network, provided by encrypting data when it leaves its source, leaving it encrypted while it passes through any intermediate computers (such as routers), and decrypting only when the data arrives at the intended destination.	ITA/Jan 2003
enterprise network		Large and diverse network connecting most major points in a company or other organization	Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.	ITA/Jan 2003
ephemeral key		A public key or a private key that is relatively short-lived.	A public key or a private key that is relatively short-lived.	ITA/Jan 2003
ESP	Encapsulating Security Payload		Security protocol that provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected.	
Ethernet		Networks that use CSMA/CD and run over different cable types	Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.	ITA/Jan 2003
EXEC		Interactive command processor of Cisco IOS	Interactive command processor of Cisco IOS.	ITA/Jan 2003
Fast Ethernet		100-Mbps Ethernet specification	Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.	ITA/Jan 2003
FCS	frame check sequence	Extra characters added to a frame for error control purposes	Extra characters added to a frame for error control purposes. Used in HDLC, Frame Relay, and other data-link layer protocols.	ITA/Jan 2003
FDDI	Fiber Distributed Data Interface	Standard specifying a 100-Mbps token-passing network using fiber-optic cable	LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber-optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
FDM	frequency-division multiplexing	An RF transmission method in which a number of transmitters share a transmission medium. Each transmitter occupies a different frequency.	An RF transmission method in which a number of transmitters share a transmission medium. Each transmitter occupies a different frequency.	BCRAN Mod11
FEC	forward error correction	In data transmission, a process by which additional data is added that is derived from the payload by an assigned algorithm.	. It allows the receiver to determine if certain classes of errors have occurred in transmission and, in some cases, allows other classes of errors to be corrected.	BCRAN Mod11
FECN	forward explicit congestion notification	Bit set by a Frame Relay network to inform the receiving DTE of network congestion	Bit set by a Frame Relay network to inform the DTE receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow-control action as appropriate.	ITA/Jan 2003
FIFO	First-in, first-out	Queuing is the classic algorithm for packet transmission.	With FIFO, transmission occurs in the same order as messages are received	BCRAN Mod9
FIPS	Federal Information Processing Standards		A government security measurement standard that specifies four increasing levels (from "Level 1" to "Level 4") of requirements to cover a wide range of potential applications and environments. The requirements address such issues as basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference and electromagnetic compatibility (EMI/EMC), and self-testing. NIST and the Canadian Communication Security Establishment jointly certify modules.	
firewall		A buffer device separating any connected public networks and a private network	Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
flash memory		Special type of EEPROM that can be erased and reprogrammed	A special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can be updated easily if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.	ITA/Jan 2003
flow control		Technique for ensuring that a transmitting entity does not overwhelm a receiving entity with data.	Technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed. In IBM networks, this technique is called pacing.	ITA/Jan 2003
forwarding		Sending a frame toward its end destination using an internetworking device	Process of sending a frame toward its ultimate destination by way of an internetworking device.	ITA/Jan 2003
frame		Logical grouping of information sent as a data-link layer unit	Logical grouping of information sent as a data-link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control that surround the user data contained in the unit.	ITA/Jan 2003
Frame Relay		Switched data-link layer protocol that handles multiple virtual circuits	Industry-standard, switched data-link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it generally is considered a replacement.	ITA/Jan 2003
FRF.5		Function that allows Frame Relay traffic over an ATM network	Frame Relay-to-ATM Service Interworking. Allows Frame Relay traffic to be transported through an ATM network.	
FRF.8		Function that allows Frame Relay and ATM networks to exchange data	Frame Relay-to-ATM Service Interworking. Allows Frame Relay and ATM networks to exchange data despite differing network protocols.	ITA/Jan 2003
FRTS	Frame Relay traffic shaping	Queueing method that uses queues on a Frame Relay network to limit surges that can cause congestion.	Data is buffered and sent into the network in regulated amounts to ensure that the traffic can fit within the promised traffic envelope for the particular connection.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
FTP	File Transfer Protocol	A standard protocol in the TCP/IP suite of protocols used to transfer files from one device to another	A standard protocol in the TCP/IP suite of protocols used to transfer files from one device to another	BCRAN Mod9
full duplex		Simultaneous data transmission between sending and receiving stations	Capability for simultaneous data transmission between a sending station and a receiving station.	ITA/Jan 2003
full mesh		Network topology, with each network node having either a physical circuit or a virtual circuit connecting it to every other network node.	Term describing a network in which devices are organized in a mesh topology, with each network node having either a physical circuit or a virtual circuit connecting it to every other network node. A full mesh provides a great deal of redundancy but because it can be prohibitively expensive to implement, it usually is reserved for network backbones.	ITA/Jan 2003
half duplex		Capability for data transmission in only one direction at a time	Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.	ITA/Jan 2003
HDB3	high density binary 3	Line code type used on E1 circuits	1. Zero suppression line coding used on E1 links. 2. Line code type used on E1 circuits.	ITA/Jan 2003
HDLC	high-level data link control	Bit-oriented synchronous data-link layer protocol	Bit-oriented synchronous data-link layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.	ITA/Jan 2003
HDSL	high-data-rate digital subscriber line	One of four DSL technologies. HDSL delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs.	Because HDSL provides T1 speed, telephone companies have been using HDSL to provision local access to T1 services whenever possible. The operating range of HDSL is limited to 12,000 feet (3658.5 meters), so signal repeaters are installed to extend the service	ITA/Jan 2003
headend		Somewhat analogous to a central office of a telephone company.	A facility where signals are received, processed, formatted, and combined for transmission on the distribution network.	BCRAN Mod11
header		Control information placed before data during encapsulation	Control information placed before data when encapsulating that data for network transmission.	ITA/Jan 2003
HFC	hybrid fiber-coaxial	Cable technology using a combination of fiber optics and traditional coaxial cable	Technology being developed by the cable TV industry to provide two-way, high-speed data access to the home using a combination of fiber optics and traditional coaxial cable.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
hierarchical addressing		Addressing scheme that uses a logical hierarchy to determine location	Scheme of addressing that uses a logical hierarchy to determine location. For example, IP addresses consist of network numbers, subnet numbers, and host numbers, which IP routing algorithms use to route the packet to the appropriate location.	ITA/Jan 2003
hierarchical routing		Network hierarchy that solves the problem of routing on large networks	The complex problem of routing on large networks can be simplified by reducing the size of the networks. This is accomplished by breaking a network into a hierarchy of networks, where each level is responsible for its own routing.	ITA/Jan 2003
HMAC	Hash-based Message Authentication Code	A mechanism for message authentication using cryptographic hash functions	HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, for example, MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.	ITA/Jan 2003
HMAC-MD5	Hashed Message Authentication Codes with MD5	A keyed version of MD5 based on RFC 2104	A keyed version of MD5 based on RFC 2104 that enables two parties to validate transmitted information using a shared secret.	ITA/Jan 2003
hop		Passage of a data packet between two network nodes	Passage of a data packet between two network nodes (for example, between two routers).	ITA/Jan 2003
hop count		Routing metric that measures the distance between a source and a destination	Routing metric used to measure the distance between a source and a destination. RIP uses hop count as its sole metric.	ITA/Jan 2003
host		Computer system on a network	Computer system on a network. Similar to node, except that host usually implies a computer system, whereas node generally applies to any networked system, including access servers and routers.	ITA/Jan 2003
host name		Name given to a machine	Name given to a machine.	ITA/Jan 2003
HTTP	Hypertext Transfer Protocol	The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.	The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.	ITA/Jan 2003
hybrid encryption		Combination of two or more encryption algorithms	Application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
ICMP	Internet Control Message Protocol	Network layer protocol that reports IP packet processing errors	Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.	ITA/Jan 2003
IDS	Intrusion Detection System		An IDS is a security countermeasure. It monitors traffic and events looking for signs of intruders. A host-based IDS monitors system events, log files, and so on. A network-based IDS monitors network traffic, usually promiscuously. Being replaced with IPS, Intrusion Protection System.	BCRAN Mod11
IEEE	Institute of Electrical and Electronics Engineers	Professional organization that develops network standards	Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.	ITA/Jan 2003
IEEE 802.1		Specification of an algorithm that prevents bridging loops by creating a spanning tree	IEEE specification that describes an algorithm that prevents bridging loops by creating a spanning tree. The algorithm was invented by Digital Equipment Corporation. The Digital algorithm and the IEEE 802.1 algorithm are not exactly the same, nor are they compatible.	ITA/Jan 2003
IEEE 802.3		LAN protocol that specifies the physical and MAC sublayers of the data-link layer	IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data-link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet.	ITA/Jan 2003
IETF	Internet Engineering Task Force	Internet standards task force	Task force consisting of over 80 working groups responsible for developing Internet standards.	ITA/Jan 2003
IGP	Interior Gateway Protocol	Protocol used to exchange routing information within an autonomous system	Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.	ITA/Jan 2003
IGRP	Interior Gateway Routing Protocol	Protocol that addresses routing issues in large, heterogeneous networks	IGP developed by Cisco to address the issues associated with routing in large, heterogeneous networks.	ITA/Jan 2003
IKE	Internet Key Exchange	A shared security policy of authenticated key exchanges for IPSec	IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
Ingress noise		Over-the-air signals that are coupled into the nominally closed coaxial cable distribution system, generally via damaged cable or other network components, poorly shielded TVs and VCRs. Difficult to track down and intermittent in nature.	Over-the-air signals that are coupled into the nominally closed coaxial cable distribution system, generally via damaged cable or other network components, poorly shielded TVs and VCRs. Difficult to track down and intermittent in nature.	BCRAN Mod11
internet		Short for internetwork	Short for internetwork. Not to be confused with the Internet.	ITA/Jan 2003
Internet		Largest global internetwork	Largest global internetwork, connecting tens of thousands of networks worldwide and having a "culture" that focuses on research and standardization based on real-life use. Many leading-edge network technologies come from the Internet community. The Internet evolved in part from ARPANET. At one time, called the DARPA Internet.	ITA/Jan 2003
internetwork		Collection of networks that functions as a single network	Collection of networks interconnected by routers and other devices that functions (generally) as a single network. Sometimes called an internet, which is not to be confused with the Internet.	ITA/Jan 2003
internetworking		Term that refers to connecting networks together	General term used to refer to the industry devoted to connecting networks together. The term can refer to products, procedures, and technologies.	ITA/Jan 2003
Inverse ARP	Inverse Address Resolution Protocol	Method of building dynamic routes in a network	Method of building dynamic routes in a network. Allows an access server to discover the network address of a device associated with a virtual circuit.	ITA/Jan 2003
IP	Internet Protocol	Protocol that offers a connectionless internetwork service	Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
IP address		32-bit address assigned to hosts using TCP/IP	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.	ITA/Jan 2003
IP spoofing		IP spoofing attack where an attacker outside your network pretends to be a trusted user	IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.	ITA/Jan 2003
IPCP	IP Control Protocol	Protocol controlling IP over PPP	Protocol that establishes and configures IP over PPP. See also IP and PPP.	ITA/Jan 2003
IPSec	IP Security	Open standards that provides data confidentiality, data integrity, and data authentication between participating peers.	A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.	ITA/Jan 2003
IPSO	IP Security Option	Specification that defines an optional security field in the IP packet header	U.S. government specification that defines an optional field in the IP packet header that defines hierarchical packet security levels on a per interface basis.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
IPv6	IP version 6		Replacement for IP version 4. IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).	BCRAN Mod10
IPX	Internetwork Packet Exchange		NetWare network layer (Layer 3) protocol used for transferring data from servers to workstations. IPX is similar to IP and XNS.	ITA/Jan 2003
ISAKMP	Internet Security Association and Key Management Protocol	Internet IPSec protocol [RFC 2408] that negotiates, establishes, modifies, and deletes security associations	Internet IPSec protocol [RFC 2408] that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.	ITA/Jan 2003
ISDN	Integrated Services Digital Network	Protocol that permits telephone networks to carry data, voice, and other traffic	Communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.	ITA/Jan 2003
IS-IS	Intermediate System-to-Intermediate System	Routing protocol whereby routers exchange information based on a single metric	OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric to determine network topology.	ITA/Jan 2003
ISL	Inter-Switch Link	Protocol that maintains VLAN information between switches and routers	Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.	ITA/Jan 2003
ISP	Internet service providers	Company that provides Internet access to other companies and individuals.	Company that provides Internet access to other companies and individuals.	ITA/Jan 2003
ITU	International Telecommunication Union	UN organization that sets international telecommunications standards	An organization established by the United Nations to set international telecommunications standards and to allocate frequencies for specific uses.	ITA/Jan 2003
ITU-T	International Telecommunication Union Telecommunication Standardization Sector	The process for sending data over a public data network	Defines the process for sending data over a public data network.	BCRAN Mod7
jitter		Interpacket delay variance	The interpacket delay variance; that is, the difference between interpacket arrival and departure. Jitter is an important QoS metric for voice and video applications.	ITA/Jan 2003
kbps	kilobits per second	Bit rate expressed in thousands of bits per second.	A bit rate expressed in thousands of bits per second.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
keepalive interval		Time between expected keepalive message	Period of time between each keepalive message sent by a network device.	ITA/Jan 2003
keepalive message		Message to show that a virtual circuit between the two devices is still active.	Message sent by one network device to inform another network device that the virtual circuit between the two is still active.	ITA/Jan 2003
key distribution		Delivery of a generated cryptographic key to the locations where it is used	<p>Process that delivers a cryptographic key from the location where it is generated to the locations where it is used in a cryptographic algorithm.</p> <p>key establishment (algorithm or protocol)</p> <p>Process that combines the key generation and key distribution steps needed to set up or install a secure communication association.</p>	ITA/Jan 2003
key pair		Set of mathematically related keys	Set of mathematically related keys—a public key and a private key—that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key.	ITA/Jan 2003
key recovery		Learning the value of a cryptographic key that previously was used	<p>1. Process for learning the value of a cryptographic key that previously was used to perform some cryptographic operation.</p> <p>2. Techniques that provide an intentional, alternate (that is, secondary) means to access the key used for data confidentiality service in an encrypted association.</p>	ITA/Jan 2003
LAN	local-area network	High-speed, low-error data network covering a small geographic area	High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data-link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.	ITA/Jan 2003
LAN switch		High-speed switch that forwards packets between data-link segments	High-speed switch that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches often are categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multilayer switches are an intelligent subset of LAN switches.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
LAPB	Link Access Procedure, Balanced	Data link layer protocol in the X.25 protocol stack	LAPB is a bit-oriented protocol derived from HDLC.	ITA/Jan 2003
LAPD	Link Access Procedure on the D channel	ISDN data link layer protocol for the D channel.	LAPD was derived from the LAPB protocol and is designed primarily to satisfy the signaling requirements of ISDN basic access. Defined by ITU-T Recommendations Q.920 and Q.921.	ITA/Jan 2003
latency		Delay between the time a device requests network access and the time it is granted permission to transmit.	1. Delay between the time a device requests access to a network and the time it is granted permission to transmit. 2. Delay between the time a device receives a frame and the time that frame is forwarded out the destination port.	ITA/Jan 2003
LCP	link control protocol	Protocol that establishes, configures, and tests PPP connections	Protocol that establishes, configures, and tests data-link connections for use by PPP.	ITA/Jan 2003
LCV	line code violation	WAN line error event	Occurrence of a BPV or EXZ error event.	ITA/Jan 2003
learning bridge		Bridge that performs MAC address learning	Bridge that performs MAC address learning to reduce traffic on the network. Learning bridges manage a database of MAC addresses and the interfaces associated with each address.	ITA/Jan 2003
leased line		Transmission line reserved for the private use of a customer	Transmission line reserved by a communications carrier for the private use of a customer. A leased line is a type of dedicated line.	ITA/Jan 2003
LFI	Link Fragmentation and Interleaving		On low-speed serial links, a large packet can cause latency for smaller packets, such as voice packets. Developed primarily for links running at 768 kbps or less, link-level fragmentation can prevent increased latency (and jitter) by dividing the large data packets into smaller pieces and interleaving voice packets within those fragments. Link Fragmentation and Interleaving for MLP has the same benefits as FRF.12 except over links running PPP encapsulation. The feature complies with RFC 1717.	BCRAN Mod10
line card		Any I/O card that can be inserted in a modular chassis	Any I/O card that can be inserted in a modular chassis.	ITA/Jan 2003
line code type		Coding schemes used on serial lines to maintain data integrity and reliability	One of a number of coding schemes used on serial lines to maintain data integrity and reliability. The line code type used is determined by the carrier service provider. See also AMI, B8ZS, and HDB3.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
link-state routing algorithm		Routing algorithm where each router broadcasts information about each neighbor to all network nodes	Routing algorithm in which each router broadcasts or multicasts information regarding the cost of reaching each of its neighbors to all nodes in the internetwork. Link-state algorithms create a consistent view of the network and therefore are not prone to routing loops; however, they achieve this at the cost of relatively greater computational difficulty and more widespread traffic (compared with distance vector routing algorithms).	ITA/Jan 2003
LLQ	Low Latency Queuing	LLQ provides strict priority queuing for Class-Based Weighted Fair Queuing (CBWFQ), reducing jitter in voice conversations.	Strict priority queuing gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. Low Latency Queuing is also called PQ/CBWFQ because it is a combination of the two techniques.	BCRAN Mod9
LMDS	Local Multipoint Distribution Service		A relatively low-power license for broadcasting voice, video, and data. There are typically two licenses granted in three frequencies, each to separate entities within a BTA. These licenses are known as Block A or Block B licenses. Block A licenses operate from 27.5 to 28.35 GHz, 29.10 to 29.25 GHz, and 31.075 to 31.225 GHz for a total of 1.159 MHz of bandwidth. Block B licenses operate from 31.00 to 31.075 GHz and 31.225 to 31.300 for a total of 150 MHz of bandwidth. LMDS systems have a typical maximum transmission range of approximately 3 miles as opposed to the transmission range of an MMDS system, which is typically 25 miles. This difference in range is primarily a function of physics and FCC-allocated output power rates.	ITA/Jan 2003
LMI	Local Management Interface	Frame Relay feature that supports keepalive, multicast, and status mechanisms	Set of enhancements to the basic Frame Relay specification. LMI includes support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which provides the network server with its local DLCI and the multicast DLCI; global addressing, which gives DLCIs global rather than local significance in Frame Relay networks; and a status mechanism, which provides an on-going status report on the DLCIs known to the switch.	ITA/Jan 2003
local loop		Line from phone subscriber to the central office.	Line from the premises of a telephone subscriber to the telephone company CO.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
LOF	loss of frame	loss of frame on a WAN signal for a given interval	LOF is a generic term with various meanings depending on the signal standards domain in which it's being used. A SONET port status indicator that activates when an LOF defect occurs and does not clear for an interval of time equal to the alarm integration period, which is typically 2.5 seconds.	ITA/Jan 2003
LOS	loss of signal	A loss of signal indicated by consecutive zeros	A loss of signal occurs when n consecutive zeros is detected on an incoming signal.	ITA/Jan 2003
LSA	link-state advertisement	Link-state broadcast packet with information about neighbors and path costs	Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.	ITA/Jan 2003
MAC	Media Access Control	Lower sublayer of the data-link layer defined by the IEEE	Lower of the two sublayers of the data-link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.	ITA/Jan 2003
MAC address		Data-link layer address required for every port or device on a LAN	Standardized data-link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, and physical address.	ITA/Jan 2003
MAC address learning		Service in which the source MAC address of each received packet is stored	Service that characterizes a learning bridge, in which the source MAC address of each received packet is stored so that future packets destined for that address can be forwarded only to the bridge interface on which that address is located. Packets destined for unrecognized addresses are forwarded out every bridge interface. This scheme helps minimize traffic on the attached LANs. MAC address learning is defined in the IEEE 802.1 standard.	ITA/Jan 2003
MAN	metropolitan-area network	Network that spans a metropolitan area.	Network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN. Compare with LAN and WAN.	ITA/Jan 2003
man-in-the-middle		Active wiretapping attack in which the attacker intercepts and selectively modifies communicated data	Form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
map class		defines specific characteristics for a call to a specified dial string.	defines specific characteristics for a call to a specified dial string.	BCRAN Mod6
Mbps	megabits per second	Bit rate expressed in millions of binary bits per second	A bit rate expressed in millions of binary bits per second.	
MD5	Message Digest 5	One-way hashing algorithm that produces a 128-bit hash	A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. See also SNMP2.	ITA/Jan 2003
mesh		Topology in which devices are organized with many, often redundant, interconnections	Network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections strategically placed between network nodes. See also full mesh and partial mesh.	ITA/Jan 2003
MICA	Modem ISDN channel aggregation	Modem module and card used in the Cisco AS5300 universal access servers.	Modem module and card used in the Cisco AS5300 universal access servers. A MICA modem provides an interface between an incoming or outgoing digital call and an ISDN telephone line; the call does not have to be converted to analog as it does with a conventional modem and an analog telephone line. Each line can accommodate, or aggregate, up to 24 (T1) or 30 (E1) calls.	ITA/Jan 2003
MLP	Multilink PPP	Protocol that splits, recombines, and sequences datagrams	This protocol is a method of splitting, recombining, and sequencing datagrams across multiple logical data links.	ITA/Jan 2003
MMDS	Multichannel Multipoint Distribution Service		MMDS is composed of as many as 33 discrete channels, which are transmitted in a pseudorandom order between the transmitters and the receivers. The FCC-allocated two bands of frequencies for each BTA are 2.15 to 2.161 GHz and 2.5 to 2.686 GHz.	ITA/Jan 2003
modem	modulator-demodulator	Device that converts digital and analog signals	Device that converts digital and analog signals. At the source, a modem converts digital signals to a form suitable for transmission over analog communication facilities. At the destination, the analog signals are returned to their digital form. Modems allow data to be transmitted over voice-grade telephone lines.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
modem eliminator		Connection of two DTE devices without modems	Device allowing the connection of two DTE devices without modems.	ITA/Jan 2003
modulation		Process to transform electrical signals to represent information	Process by which the characteristics of electrical signals are transformed to represent information. Types of modulation include AM, FM, and PAM. See also AM, FM, and PAM.	ITA/Jan 2003
MPPC	Microsoft Point-to-Point Compression	Allows Cisco routers to exchange compressed data with Microsoft clients	MPPC uses an LZ-based compression mechanism. Use MPPC when exchanging data with a host using MPPC across a WAN link.	BCRAN Mod9
MSO	Multiple system operators	Big companies that operate multiple systems	Big companies that operate multiple systems	BCRAN Mod11
multilayer switch		Switch that filters and forwards packets based on MAC network addresses	Switch that filters and forwards packets based on MAC addresses and network addresses. A subset of LAN switch.	ITA/Jan 2003
multiplexing		Multiple logical signals transmitted simultaneously across a single physical channel.	Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel. Compare with demultiplexing.	ITA/Jan 2003
name server		Server that resolves network names into network addresses	Server connected to a network that resolves network names into network addresses.	ITA/Jan 2003
NAT	Network Address Translation	Mechanism that reduces the need for globally unique IP addresses	Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.	ITA/Jan 2003
NBMA	nonbroadcast multiaccess	Multiaccess network that does not support broadcasting	Term describing a multi-access network that either does not support broadcasting (such as X.25) or in which broadcasting is not feasible (for example, an SMDS broadcast group or an extended Ethernet that is too large).	ITA/Jan 2003
NBS	National Bureau of Standards		Organization that was part of the U.S. Department of Commerce. Now known as NIST. See also NIST .	ITA/Jan 2003
NCP	Network Control Protocol	Protocols that establish and configure different network layer protocols	Series of protocols for establishing and configuring different network layer protocols, such as for AppleTalk over PPP.	ITA/Jan 2003
neighboring routers		In OSPF, two routers that have interfaces to a common network	In OSPF, two routers that have interfaces to a common network. On multi-access networks, neighbors are discovered dynamically by the OSPF Hello protocol.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
network address		Network layer address referring to a logical network device	Network layer address referring to a logical, rather than a physical, network device.	ITA/Jan 2003
network management		Systems or actions that help maintain or troubleshoot a network	Generic term used to describe systems or actions that help maintain, characterize, or troubleshoot a network.	ITA/Jan 2003
NIC	network interface card	Board that provides network communication with a computer system	Board that provides network communication capabilities to and from a computer system. Also called an adapter.	ITA/Jan 2003
NIST	National Institute of Standards and Technology		U.S. government organization that supports and catalogs a variety of standards. Formerly the NBS. See also NBS .	
N-ISDN	Narrowband ISDN	ISDN standard for 64-kbps B channels and 16- or 64-kbps D channels.	Communication standards developed by the ITU-T for baseband networks. Based on 64-kbps B channels and 16- or 64-kbps D channels. Contrast with BISDN. See also BRI, ISDN, and PRI.	ITA/Jan 2003
NNI	Network-to-Network Interface	Describes how the ATM and Frame Relay networks of different service providers connect to each other	Describe how the ATM and Frame Relay networks of different service providers connect to each other.	BCRAN Mod7
nonce		Random or non-repeating value	Random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks.	ITA/Jan 2003
NT-1	network termination 1	An ISDN device interfacing customer premises equipment and central office equipment.	In ISDN, a device that provides the interface between customer premises equipment and central office switching equipment.	ITA/Jan 2003
NTSC	National Television Systems Committee.	North American TV technical standard, named after the organization that created it in 1941.	Uses a 6-MHz-wide modulated signal.	BCRAN Mod11
NVRAM	nonvolatile RAM	RAM that retains its contents when the power is off	RAM that retains its contents when a unit is powered off.	ITA/Jan 2003
OAKLEY		Key establishment protocol	Key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
OIR	online insertion and removal	Feature that permits the card replacement without interrupting the power	Feature that permits the addition, the replacement, or the removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown. Sometimes called hot swapping or power-on servicing.	ITA/Jan 2003
one-way encryption		Irreversible transformation of plaintext to ciphertext	Irreversible transformation of plaintext to ciphertext, such that the plaintext cannot be recovered from the ciphertext by other than exhaustive procedures even if the cryptographic key is known.	ITA/Jan 2003
ones density		Scheme that allows a CSU/DSU to recover the data clock reliably	Scheme that allows a CSU/DSU to recover the data clock reliably. The CSU/DSU derives the data clock from the data that passes through it. To recover the clock, the CSU/DSU hardware must receive at least one 1 bit value for every 8 bits of data that pass through it. Also called pulse density.	ITA/Jan 2003
OSI reference model	Open System Interconnection reference model	Network architectural model developed by ISO and ITU-T	Network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are implemented in hardware and software whereas the upper five layers are implemented only in software. The highest layer (the application layer) is closest to the user.	ITA/Jan 2003
OSPF	Open Shortest Path First	Link-state, hierarchical IGP routing algorithm	Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.	ITA/Jan 2003
packet		Information that includes a header with control information	Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data.	ITA/Jan 2003
packet switching		Method in which nodes share bandwidth with each other	Networking method in which nodes share bandwidth with each other by sending packets. Compare with circuit switching and message switching.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
PAL	Phase Alternating Line.	This TV system is used in most of Europe, Asia, Africa, Australia, Brazil, and Argentina.	The color difference signals alternate phase at the horizontal line rate. Utilizes a 6 MHz, 7 MHz or 8 MHz wide modulated signal, depending on PAL version.	BCRAN Mod11
PAP	Password Authentication Protocol	Authentication protocol between PPP peers	Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines.	ITA/Jan 2003
partial mesh		Network where some nodes are in a full mesh and some are connected to one or two other nodes	Network in which devices are organized in a mesh topology with some network nodes organized in a full mesh but others that are connected only to one or two other nodes in the network. A partial mesh does not provide the level of redundancy of a full mesh topology but is less expensive to implement. Partial mesh topologies generally are used in the peripheral networks that connect to a fully meshed backbone.	
password		Secret data value for authentication	Secret data value, usually a character string that is used as authentication information.	ITA/Jan 2003
password sniffing		Passive wiretapping to get passwords	Passive wiretapping, usually on a local-area network, to gain knowledge of passwords.	ITA/Jan 2003
PAT	port address translation	Translation method that allows source ports to be translated	Translation method that allows the user to conserve addresses in the global address pool by allowing source ports in TCP connections or UDP conversations to be translated. Different local addresses then map to the same global address, with port translation providing the necessary uniqueness.	ITA/Jan 2003
PCM	pulse code modulation	pulse code modulation	Technique of encoding analog voice into a 64-kbit data stream by sampling with eight-bit resolution at a rate of 8000 times per second.	ITA/Jan 2003
PGP	Pretty Good Privacy	Public-key encryption application	Public-key encryption application that allows secure file and message exchanges. There is some controversy over the development and the use of this application, in part due to U.S. national security concerns.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
ping	packet internet groper	Utility used to test the reachability of a network device	ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.	ITA/Jan 2003
ping of death		Attack that sends an improperly large ping	Attack that sends an improperly large ICMP [R0792] echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.	ITA/Jan 2003
ping sweep		Attack that sends pings to a range of IP addresses	Attack that sends ICMP [RFC 0792] echo requests ("pings") to a range of IP addresses with the goal of finding hosts that can be probed for vulnerabilities.	ITA/Jan 2003
PKCS	Public-Key Cryptography Standards	data structures and algorithm usage for asymmetric cryptography	Series of specifications published by RSA Laboratories for data structures and algorithm usage for basic applications of asymmetric cryptography.	ITA/Jan 2003
PKI	public-key infrastructure	set of security-management functions for a community of users for asymmetric cryptography.	System of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.	ITA/Jan 2003
poison reverse updates		Routing updates that used to defeat large routing loops	Routing updates that explicitly indicate that a network or a subnet is unreachable, rather than implying that a network is unreachable by not including it in updates. Poison reverse updates are sent to defeat large routing loops.	ITA/Jan 2003
port		Interface on an internetworking device	Interface on an internetworking device (such as a router).	ITA/Jan 2003
POTS	plain old telephone service	Traditional variety of telephone networks and services in place worldwide.	Public switched telephone network. General term referring to the variety of telephone networks and services in place worldwide.	ITA/Jan 2003
PPP	Point-to-Point Protocol	Protocol that provides router-to-router and host-to-network connections	Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.	ITA/Jan 2003
PPPoA	Point-to-Point Protocol over ATM	The CPE is routing the packets from the PC of the end user over ATM to an aggregation router.	The PPP session is established between the CPE and the aggregation router. PPP over ATM requires no host-based software like PPPoE.	BCRAN Mod11

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
PPPoE	Point-to-Point Protocol over Ethernet	PPPoE is also a bridged solution similar to RFC 1483/2684 bridging.	The CPE is bridging the Ethernet frames from the PC of the end user to an aggregation router over ATM like RFC 1483/2684 bridging. But in this case, the Ethernet frame is carrying a PPP frame inside it. The PPP session is established between the end-user PC (PPPoE Client) and the aggregation router.	BCRAN Mod11
PQ/CBWFQ	priority queueing /class-based weighted fair queueing	Strict priority queueing added to class-based weighted fair queueing	Feature that brings strict priority queueing to CBWFQ. Strict priority queueing allows delay-sensitive data, such as voice, to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.	ITA/Jan 2003
presared key		Shared secret key	Shared secret key that is used during IKE authentication.	ITA/Jan 2003
PRI	Primary Rate Interface	ISDN interface to primary rate access	ISDN interface to primary rate access. Primary rate access consists of a single 64-kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.	ITA/Jan 2003
Priority Queuing		defines four priorities of traffic--high, normal, medium, and low on a given interface.	As traffic comes into the router, it is assigned to one of the four output queues. Packets on the highest-priority queue are transmitted first. Packets on the next highest-priority queue are transmitted second, and so on.	BCRAN Mod9
private key		Secret component of a pair of cryptographic keys	Secret component of a pair of cryptographic keys used for asymmetric cryptography.	ITA/Jan 2003
privilege		Authorization to perform security-relevant functions	Authorization or set of authorizations to perform security-relevant functions, especially in the context of a computer operating system.	ITA/Jan 2003
protected checksum		Checksum 7 protected against active attacks for match changes made to the data object.	Checksum that is computed for a data object by means that protect against active attacks that would attempt to change the checksum to make it match changes made to the data object.	ITA/Jan 2003
protocol		Rules and conventions that govern how network devices exchange information	Formal description of a set of rules and conventions that govern how devices on a network exchange information.	ITA/Jan 2003
PSTN	Public switched telephone network.	General term referring to the variety of telephone networks and services in place worldwide.	General term referring to the variety of telephone networks and services in place worldwide.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
PTT	Post, Telephone, and Telegraph	Government agency that provides telephone services	Government agency that provides telephone services. PTTs exist in most areas outside North America and provide both local and long-distance telephone services.	ITA/Jan 2003
public key		Publicly disclosable component of a pair of cryptographic keys	Publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography.	ITA/Jan 2003
public-key certificate		Certificate that attests to the ownership of a public key.	Digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally signed data structure that attests to the ownership of a public key.	ITA/Jan 2003
PVC	permanent virtual circuit (or connection)	Virtual circuit that is permanently established	Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.	ITA/Jan 2003
PVST+	per-VLAN spanning tree	Dot1q trunks that map multiple spanning trees to a single spanning tree	Support for Dot1q trunks to map multiple spanning trees to a single spanning tree.	ITA/Jan 2003
QAM	Quadrature amplitude modulation	A digital modulation method in which the phase and amplitude of an RF carrier are varied to transmit data.	Typical QAM types are 16-QAM (4 bits per symbol), 64-QAM (6 bits per symbol), and 256-QAM (8 bits per symbol).	BCRAN Mod11
QoS	quality of service		Measure of performance for a transmission system that reflects its transmission quality and service availability.	BCRAN Mod4
QPSK	quadrature phase shift keying	A digital modulation method in which the phase of the RF carrier is varied to transmit data. There are 2 bits per symbol.	A digital modulation method in which the phase of the RF carrier is varied to transmit data. There are 2 bits per symbol.	BCRAN Mod11
RA	registration authority	Optional public-key infrastructure (PKI) entity	Optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions.	ITA/Jan 2003
RADIUS	Remote Authentication Dial-In User Service	Database for authenticating connections	Database for authenticating modem and ISDN connections and for tracking connection time.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
RAM	random-access memory	Volatile memory that can be read and written by a microprocessor	Volatile memory that can be read and written by a microprocessor.	ITA/Jan 2003
random early detection		Congestion avoidance algorithm	Congestion avoidance algorithm in which a small percentage of packets are dropped when congestion is detected and before the queue in question overflows completely.	ITA/Jan 2003
rcp	remote copy protocol	Protocol used to copy files to and from a network file system	Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.	ITA/Jan 2003
RED	Random Early Detection	Larger-scale networks employ algorithms, such as RED, so they can proactively discard packets earlier to prevent (or delay) tail drops.	RED directs one TCP session at a time to slow down. This allows for fuller utilization of the bandwidth and can prevent the crests and troughs of traffic from global TCP synchronization.	BCRAN Mod9
redundant system		System that contains two or more of the most important subsystems	Computer, router, switch, or other system that contains two or more of each of the most important subsystems, such as two disk drives, two CPUs, or two power supplies.	ITA/Jan 2003
rekey		Change the value of a cryptographic key	Change the value of a cryptographic key that is being used in an application of a cryptographic system.	ITA/Jan 2003
reliability		Total number of system failures	Total number of system failures, regardless of whether a given failure results in system down time.	ITA/Jan 2003
remote system		End system or router that is attached to a remote access network	End system or router that is attached to a remote access network and that is either the initiator or the recipient of a call.	ITA/Jan 2003
Request To Send		Request To Send	Request To Send	ITA/Jan 2003
RF	radio frequency	Generic term referring to frequencies that correspond to radio transmissions, that is wireless communications with frequencies below 300 GHz.	Cable TV and broadband networks use RF technology.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
RF Carrier		An electromagnetic signal on which another, lower-frequency signal (usually base band, such as analog audio, analog video or digital data) is modulated in order to transport the lower-frequency signal to another location	An electromagnetic signal on which another, lower-frequency signal (usually base band, such as analog audio, analog video or digital data) is modulated in order to transport the lower-frequency signal to another location	BCRAN Mod11
RFC	Request For Comments	Documents that communicate information about the Internet	Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.	ITA/Jan 2003
RIP	Routing Information Protocol	Routing protocol that uses hop count as a routing metric	IGP supplied with UNIX BSD systems. The most common IGP in the Internet. RIP uses hop count as a routing metric.	ITA/Jan 2003
RJ connector	registered jack connector	registered jack connector	registered jack connector. Standard connectors originally used to connect telephone lines. RJ connectors are now used for telephone connections and for 10BaseT and other types of network connections. RJ-11, RJ-12, and RJ-45 are popular types of RJ connectors.	ITA/Jan 2003
RMON	remote monitoring	Defines functions for the remote monitoring of networked devices	MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.	ITA/Jan 2003
ROM	read-only memory	Nonvolatile memory that can be read, but not written	Nonvolatile memory that can be read, but not written, by the microprocessor.	ITA/Jan 2003
root bridge		Bridge that exchanges topology information with designated bridges	Exchanges topology information with designated bridges in a spanning-tree implementation to notify all other bridges in the network when topology changes are required. This prevents loops and provides a measure of defense against link failure.	ITA/Jan 2003
root certificate		Certificate for which the subject is a root.	Certificate for which the subject is a root. Hierarchical PKI usage: The self-signed public-key certificate at the top of a certification hierarchy.	ITA/Jan 2003
root key		Public key with matching private key held by a root.	Public key for which the matching private key is held by a root.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
route		Path through an internetwork	Path through an internetwork.	ITA/Jan 2003
route summarization		Consolidation of advertised addresses in OSPF and IS-IS	Consolidation of advertised addresses in OSPF and IS-IS. In OSPF, this causes a single summary route to be advertised to other areas by an area border router.	ITA/Jan 2003
routed protocol		Protocol that can be routed by a router	Protocol that can be routed by a router. A router must be able to interpret the logical internetwork as specified by that routed protocol. Examples of routed protocols include AppleTalk, DECnet, and IP.	ITA/Jan 2003
router		Network device that forwards packets from one network to another	Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated).	ITA/Jan 2003
routing		Process of finding a path to a destination host	Process of finding a path to a destination host. Routing is very complex in large networks because of the many potential intermediate destinations a packet might traverse before reaching its destination host.	ITA/Jan 2003
routing domain		Group of systems operating under a set of administrative rules	Group of end systems and intermediate systems operating under the same set of administrative rules. Within each routing domain is one or more areas, each uniquely identified by an area address.	ITA/Jan 2003
routing metric		Method used to determine that one route is better than another	Method by which a routing algorithm determines that one route is better than another. This information is stored in routing tables. Metrics include bandwidth, communication cost, delay, hop count, load, MTU, path cost, and reliability. Sometimes referred to simply as a metric.	ITA/Jan 2003
routing protocol		Protocol uses a specific routing algorithm to route packets	Protocol that accomplishes routing through the implementation of a specific routing algorithm. Examples of routing protocols include IGRP, OSPF, and RIP.	ITA/Jan 2003
routing table		Table stored in a router that tracks routes and metrics	Table stored in a router or some other internetworking device that keeps track of routes to particular network destinations and, in some cases, metrics associated with those routes.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
routing update		Message sent from a router to indicate network reachability and cost	Message sent from a router to indicate network reachability and associated cost information. Routing updates typically are sent at regular intervals and after a change in network topology.	ITA/Jan 2003
RS-232		Popular physical layer interface	Popular physical layer interface. Now known as EIA/TIA-232. See also EIA/TIA-232.	ITA/Jan 2003
RSA	Rivest, Shamir, and Adleman	Public-key cryptographic system	Acronym stands for Rivest, Shamir, and Adleman, the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.	ITA/Jan 2003
RSVP	Resource Reservation Protocol		Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams that they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol. See also IPv6 .	
RTP	Real-Time Transport Protocol	Used to carry multimedia application traffic, including packetized audio and video, over an IP network.	Used to carry multimedia application traffic, including packetized audio and video, over an IP network.	BCRAN Mod9
RTS	Request To Send	EIA/TIA-232 control signal	EIA/TIA-232 control signal that requests a data transmission on a communications line.	ITA/Jan 2003
SA	security association	Instance of security policy and keying material	Instance of security policy and keying material applied to a data flow. See also Security Association.	ITA/Jan 2003
Satellite Communication		Use of orbiting satellites to relay data between multiple earth-based stations.	Satellite communications offer high bandwidth and a cost that is not related to distance between earth stations, long propagation delays, or broadcast capability.	ITA/Jan 2003
SDSL	single-line digital subscriber line	One of four DSL technologies. SDSL delivers 1.544 Mbps	One of four DSL technologies. SDSL delivers 1.544 Mbps both downstream and upstream over a single copper twisted pair. The use of a single twisted pair limits the operating range of SDSL to 10,000 feet (3048.8 meters). Compare with ADSL, HDSL, and VDSL.	ITA/Jan 2003
SECAM	Sequential Couleur avec Memoire.	TV system used in France and some former Soviet bloc countries	Utilizes an 8 MHz wide modulated signal.	BCRAN Mod11

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
Secure Shell Protocol		Protocol that provides a secure remote connection to a router	Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.	ITA/Jan 2003
security association		An instance of security policy and keying material applied to a data flow.	An instance of security policy and keying material applied to a data flow. Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPSec. A user also can establish IPSec SAs manually. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are identified uniquely by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).	ITA/Jan 2003
security parameter index		A number that, together with a destination IP address and a security protocol, uniquely identifies a particular security association.	This is a number that, together with a destination IP address and a security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is specified manually for each security association.	ITA/Jan 2003
segment		Section of a network that is bounded by network devices	Section of a network that is bounded by bridges, routers, or switches.	ITA/Jan 2003
serial transmission		Data transmission where bits are transmitted sequentially	Method of data transmission in which the bits of a data character are transmitted sequentially over a single channel.	ITA/Jan 2003
SF	Super Frame	Common framing type used on T1 circuits.	Common framing type used on T1 circuits. SF consists of 12 frames of 192 bits each, with the 193rd bit providing error checking and other functions. SF is superseded by ESF but is still widely used. Also called D4 framing. See also ESP.	ITA/Jan 2003
SHA-1	Secure Hash Algorithm 1	Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest	Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
SLIP	Serial Line Internet Protocol	Protocol for point-to-point serial connections that is the predecessor of PPP	Standard protocol for point-to-point serial connections using a variation of TCP/IP. Predecessor of PPP. See also CSI and PPP.	ITA/Jan 2003
SMTP	Simple Mail Transfer Protocol	Internet protocol providing e-mail services.	Internet protocol providing e-mail services.	ITA/Jan 2003
SN	Signal noise	Similar to C/N but relates to a base band signal.	Similar to C/N but relates to a base band signal.	BCRAN Mod11
SNA	Systems Network Architecture	Large, complex, feature-rich network architecture developed in the 1970s by IBM	Similar in some respects to the OSI reference model but with a number of differences. SNA essentially is composed of seven layers	ITA/Jan 2003
SNMP	Simple Network Management Protocol	Network management protocol used in TCP/IP networks	Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.	ITA/Jan 2003
SOHO	small office, home office	Network for small office, home office	Networking solutions and access technologies for offices that are not directly connected to large corporate networks.	ITA/Jan 2003
source address		Address of a network device that is sending data	Address of a network device that is sending data.	ITA/Jan 2003
spanning tree		Loop-free subset of a network topology	Loop-free subset of a network topology.	ITA/Jan 2003
spanning-tree algorithm		Algorithm used to create a spanning tree	Algorithm used by the Spanning-Tree Protocol to create a spanning tree.	ITA/Jan 2003
Spectrum Reuse		CATVs most fundamental concept is spectrum reuse.	Historically, the over-the-air spectrum has been assigned to many uses: two-way radio, broadcasting, cellular phones, and pagers. Much of the spectrum is therefore not available for the carriage of just TV. The result is an inadequate supply of spectrum to serve viewers' needs. Cable operators can reuse spectrum that is "sealed" in their networks' coaxial cables.	BCRAN Mod11
SPF	shortest path first algorithm	Routing algorithm that determines a shortest-path spanning tree	Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
SPI	security parameter index	A number that, together with a destination IP address and security protocol, uniquely identifies a particular security association.	This is a number that, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association.	ITA/Jan 2003
split-horizon updates		Routing technique that prevents routing loops	Routing technique in which information about routes is prevented from exiting the router interface through which that information was received. Split-horizon updates are useful in preventing routing loops.	ITA/Jan 2003
spoofing		Scheme used by routers to cause a host to treat an interface as if it were up and supporting a session	<p>1. Scheme used by routers to cause a host to treat an interface as if it were up and supporting a session. The router spoofs replies to keepalive messages from the host in order to convince that host that the session still exists. Spoofing is useful in routing environments, such as DDR, in which a circuit-switched link is taken down when there is no traffic to be sent across it in order to save toll charges. See also DDR.</p> <p>2. The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms, such as filters and access lists.</p>	ITA/Jan 2003
SSH	Secure Shell	A secure application used for logging into a remote device, executing commands on a remote device, and moving files from remote device to remote device	A secure application used for logging into a remote device, executing commands on a remote device, and moving files from remote device to remote device	BCRAN Mod9
SSL	Secure Socket Layer	Encryption technology for the Web	Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.	ITA/Jan 2003
static route		Route that is explicitly configured in the routing table	Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.	ITA/Jan 2003
STDM	Statistical time division multiplexing	Technique whereby information from multiple logical channels can be transmitted across a single physical channel.	multiplexing dynamically allocates bandwidth only to active input channels, making better use of available bandwidth and allowing more devices to be connected than with other multiplexing techniques.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
STP	Spanning-Tree Protocol	Protocol that enables a learning bridge to work around loops	Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.	ITA/Jan 2003
stub network		Network that has a single connection to a router	Network that has only a single connection to a router.	ITA/Jan 2003
subinterface		Virtual interface on a single physical interface	One of a number of virtual interfaces on a single physical interface.	ITA/Jan 2003
subnet address		Portion of an IP address specified as the subnetwork	Portion of an IP address that is specified as the subnetwork by the subnet mask.	ITA/Jan 2003
subnet mask		32-bit address mask used to indicate the of IP address bits used for the subnet address	32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address. Sometimes referred to simply as mask.	ITA/Jan 2003
subnetwork		Network sharing a particular subnet address	In IP networks, a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks.	ITA/Jan 2003
Subscriber drop		Connection between feeder portion of distribution network and subscriber terminal (TV set, VCR, and so forth).	Includes coax, typically 59-series or 6-series coaxial cable; hardware; passive devices; set-top box (STB).	BCRAN Mod11
superencryption		Encryption operation on output from a previous encryption	Encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
SVC	switched virtual circuit	Virtual circuit dynamically established on demand	Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. See also virtual circuit. Called a switched virtual connection in ATM terminology.	ITA/Jan 2003
switch		Network device that filters, forwards, and floods frames to a destination address	Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data-link layer of the OSI model.	ITA/Jan 2003
switched LAN		LAN implemented with LAN switches	LAN implemented with LAN switches.	ITA/Jan 2003
switching		Process of delivering an incoming frame from one interface through another	Process of taking an incoming frame from one interface and delivering it through another interface. Routers use Layer 3 switching to route a packet, and Layer 2 switches use Layer 2 switching to forward frames.	ITA/Jan 2003
symmetric key		Key used in a symmetric cryptographic algorithm	Cryptographic key that is used in a symmetric cryptographic algorithm.	ITA/Jan 2003
synchronous transmission		Digital signals that are transmitted with precise clocking	Term describing digital signals that are transmitted with precise clocking. Such signals have the same frequency, with individual characters encapsulated in control bits (called start bits and stop bits) that designate the beginning and the end of each character.	ITA/Jan 2003
T1		Digital WAN carrier facility operating at 1.544 Mbps	Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding.	ITA/Jan 2003
T3		Digital WAN carrier facility operating at 44.736 Mbps	Digital WAN carrier facility. T3 transmits DS-3-formatted data at 44.736 Mbps through the telephone switching network.	ITA/Jan 2003
TACACS	Terminal Access Controller Access Control System	Authentication protocol, developed by the DDN community	Authentication protocol, developed by the DDN community that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution. See also TACACS+ in the "Cisco Systems Terms and Acronyms" section	ITA/Jan 2003
T-carrier		TDM transmission method	TDM transmission method usually referring to a line or a cable carrying a DS-1 signal.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
TCP/IP	Transmission Control Protocol/Internet Protocol	Suite of protocols that support the construction of worldwide internetworks	Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.	ITA/Jan 2003
TDM	time-division multiplexing	Technique in which information from multiple channels can be allocated bandwidth on a single wire based on pre-assigned time slots.	Technique in which information from multiple channels can be allocated bandwidth on a single wire based on pre-assigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit. Compare with ATDM, FDM, and statistical multiplexing.	ITA/Jan 2003
TE	terminal equipment	Any ISDN-compatible device that can be attached to the network	Any ISDN-compatible device that can be attached to the network, such as a telephone, a fax, or a computer.	ITA/Jan 2003
TEI	terminal endpoint identifier	Address that identifies a device on an ISDN interface	Field in the LAPD address that identifies a device on an ISDN interface. See also TE .	ITA/Jan 2003
Telnet		Standard TCP/IP terminal emulation protocol	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.	ITA/Jan 2003
terminal		Simple device at which data is entered or retrieved from a network	Simple device at which data can be entered or retrieved from a network. Generally, terminals have a monitor and a keyboard, but no processor or local disk drive.	ITA/Jan 2003
terminal adapter		Device used to connect ISDN BRI connections to existing interfaces	Device used to connect ISDN BRI connections to existing interfaces, such as EIA/TIA-232. Essentially, an ISDN modem.	ITA/Jan 2003
terminal emulation		Network application that makes a terminal appear to a remote host as directly attached	Network application in which a computer runs software that makes it appear to a remote host as a directly attached terminal.	ITA/Jan 2003
terminal server		Communications processor that connects asynchronous devices to a network	Communications processor that connects asynchronous devices, such as terminals, printers, hosts, and modems, to any LAN or WAN that uses TCP/IP, X.25, or LAT protocols. Terminal servers provide the internetwork intelligence that is not available in the connected devices.	ITA/Jan 2003
TFTP	Trivial File Transfer Protocol	Simple file transfer protocol without use of authentication	Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
throughput		Rate of information arriving at a particular point in a network	Rate of information arriving at, and possibly passing through, a particular point in a network system.	ITA/Jan 2003
TIA	Telecommunications Industry Alliance	Telecommunications Industry Alliance standards organization	Telecommunications Industry Alliance. Organization that develops standards relating to telecommunications technologies. Together, the TIA and the EIA have formalized standards, such as EIA/TIA-232, for the electrical characteristics of data transmission. See also EIA.	ITA/Jan 2003
token storage key		Cryptography key	Cryptography key used to protect data that is stored on a security token.	ITA/Jan 2003
topology		Physical arrangement of network nodes and media	Physical arrangement of network nodes and media within an enterprise networking structure.	ITA/Jan 2003
traceroute		Program that traces the path a packet takes to a destination	Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.	ITA/Jan 2003
traffic shaping		Use of queues to limit (shape) surges that can congest a network	Use of queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that the traffic fits within the promised traffic envelope for the particular connection. Traffic shaping is used in ATM, Frame Relay, and other types of networks. Also known as metering, shaping, and smoothing.	ITA/Jan 2003
transform		The list of operations done on a dataflow to provide data authentication, data confidentiality, and data compression.	The list of operations done on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.	ITA/Jan 2003
trunk		Physical and logical connection between two switches	Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.	ITA/Jan 2003
trust-file PKI	Trust-file public-key infrastructure	Non-hierarchical public-key infrastructure used for security checking	Non-hierarchical PKI in which each certificate user has a local file (which is used by application software) of public-key certificates that the user trusts as starting points (that is, roots) for certification paths.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
tunnel		Secure communication path between two peers	Secure communication path between two peers, such as two routers.	ITA/Jan 2003
tunneling		Architecture that provides services used to implement point-to-point encapsulation	Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.	ITA/Jan 2003
U interface	User-interface	The DSL interface between the telco and the user	The interface between the telco and the user, also known as the local digital subscriber line (DSL) loop.	ITA/Jan 2003
uBR	Universal Broadband Router	Cisco Broadband Cable Device-- Universal Broadband Router	The uBR7246 and uBR7223 are DOCSIS-compliant cable modem termination systems (CMTSs). The uBR900, uBR904, and uBR924 are DOCSIS-certified cable modems.	ITA/Jan 2003
UDP	User Datagram Protocol	Connectionless transport layer protocol in the TCP/IP protocol stack.	UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.	ITA/Jan 2003
U-NII	Unlicensed National Information Infrastructure		Term coined by federal regulators to describe the access of information for citizens and business. Equivalent to the term "information superhighway," it does not describe system architecture or topology.	ITA/Jan 2003
US	Upstream	RF signal flow from the subscribers to the headend. Also called the return or reverse path.	RF signal flow from the subscribers to the headend. Also called the return or reverse path.	BCRAN Mod11
V.35	V.35	ITU-T standard describing a synchronous, physical layer protocol	ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe, and is recommended for speeds up to 48 kbps.	ITA/Jan 2003
VDSL	very-high-data-rate digital subscriber line	One of four DSL technologies. VDSL delivers 13 to 52 Mbps downstream and 1.5 to 2.3 Mbps upstream over a single twisted copper pair.	The operating range of VDSL is limited to 1,000 to 4,500 feet (304.8 to 1,372 meters).	ITA/Jan 2003
virtual circuit		Logical circuit that ensures reliable communication between two network devices	Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
VLAN	virtual LAN	Group of devices on separate LANs that communicate as if they were attached to the same wire	Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.	ITA/Jan 2003
VLSM	variable length subnet mask	Capability to specify a different subnet mask for the same network number on different subnets	Capability to specify a different subnet mask for the same network number on different subnets. VLSM can help optimize available address space.	ITA/Jan 2003
VoIP	Voice over IP		The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which are then stored in groups of two within voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.	ITA/Jan 2003
VPDN	Virtual private dial-up network	Cisco standard that enables a private network dial-in service to span across to remote access servers.	Cisco standard that enables a private network dial-in service to span across to remote access servers.	BCRAN Mod11
VPN	Virtual Private Network	Tunneling that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another	Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.	ITA/Jan 2003
vty	virtual type terminal	Virtual type terminal commonly used as virtual terminal lines	Virtual type terminal commonly used as virtual terminal lines.	ITA/Jan 2003
WAN	wide-area network	Data network that serves users across a broad geographic area	Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.	ITA/Jan 2003

Acronym or Term	Expansion of Acronym	Short Definition for Mouseover	Definition of Acronym or Term	Source for Definition
WFQ	weighted fair queuing	<p>1. WFQ provides traffic priority management that dynamically sorts traffic into conversations, or flows, based on Layer 3 or 4 information.</p> <p>2. Congestion management algorithm</p>	<p>1. Weighted fair queuing can prioritize traffic based on flows (flow-based weighted fair queuing) or user-defined classes (class-based weighted fair queuing).</p> <p>2. Congestion management algorithm that identifies conversations (in the form of traffic streams), separates packets that belong to each conversation, and ensures that capacity is shared fairly between these individual conversations. WFQ is an automatic way of stabilizing network behavior during congestion and results in increased performance and reduced retransmission.</p>	BCRAN Mod9 and ITA/Jan 2003
WIC	WAN interface card	Card that connects a device to the WAN link service provider	Connects the system to the WAN link service provider.	ITA/Jan 2003
wideband		See broadband.	See broadband.	ITA/Jan 2003
wildcard mask		Value that determines which bits in an IP address to ignore with access lists	A 32-bit quantity used in conjunction with an IP address to determine which bits in an IP address should be ignored when comparing that address with another IP address. A wildcard mask is specified when setting up access lists.	ITA/Jan 2003
WRED	weighted random early detection	<p>Queueing method</p> <p>Extends RED functions by permitting more granular RED drop profiles for different types of traffic</p>	<p>Queueing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.</p> <p>WRED combines RED with IP Precedence values or with Differentiated Services Code Point (DSCP) values.</p>	ITA/Jan 2003 and BCRAN Mod9
xDSL	X Digital Subscriber Link	Group term used to refer to ADSL, HDSL, SDSL, and VDSL.	Group term used to refer to ADSL, HDSL, SDSL, and VDSL. All are emerging digital technologies using the existing copper infrastructure provided by the telephone companies. xDSL is a high-speed alternative to ISDN.	ITA/Jan 2003

BCRAN

Building Cisco Remote Access Networks

Version 2.1

Lab Guide

Text Part Number: 97-1855-01

Copyright © 2004, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe



Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)

Lab Guide

Overview

Use the exercises here to complete the lab exercises for this course. The solutions information is found in the Lab Exercise Answer Key.

Outline

This Lab Guide includes these exercises:

- Lab Exercise 1-1: Using the BCRAN Lab Equipment
- Lab Exercise 2-1: Configuring Asynchronous Connections with Modems
- Lab Exercise 3-1: Configuring and Verifying PPP Operations
- Lab Exercise 4-1: E-Lab: Simulation for Configuring a Cisco 827 Router for NAT with PPPoA
- Lab Exercise 5-1: Configuring a Site-to-Site IPSec VPN Using Preshared Keys
- Lab Exercise 6-1: Using ISDN and DDR to Enhance Remote Connectivity
- Lab Exercise 7-1: Using Dialer Profiles to Enhance DDR
- Lab Exercise 8-1: Establishing a Dedicated Frame Relay Connection and Controlling Traffic Flow
- Lab Exercise 9-1: Enabling a Backup to a Primary Connection
- Lab Exercise 10-1: Managing Network Performance Using CBWFQ and LLQ
- Lab Exercise 11-1: Using AAA to Scale Access Control
- Super Lab

Lab Exercise 1-1: Using the BCRAN Lab Equipment

Complete this lab exercise to practice what you learned in the related module.

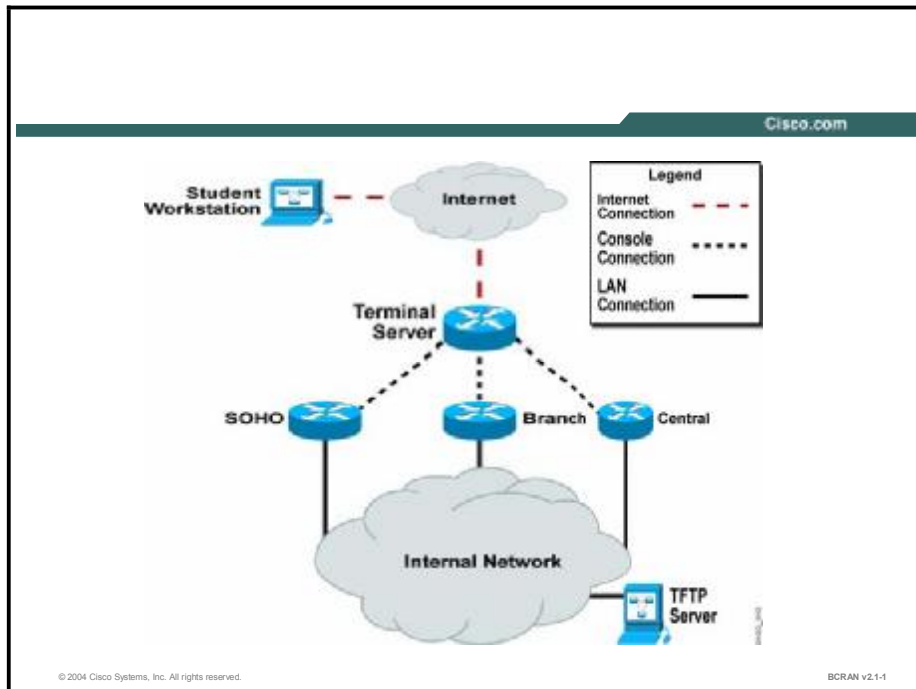
Exercise Objectives

In this exercise you will complete the following tasks:

- Establish a telnet session onto the BCRAN remote equipment pods
- Establish and terminate console connections to the remote routers
- Configure the central, branch, and SOHO routers with the preconfiguration lab files from the TFTP server

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
clsX	Clears an existing console connection where X is the connection number (1 = central, 2 = branch, 3 = SOHO)
Ctrl-Shift-6 and then x	Pressing this key combination suspends a console session and returns you to the terminal server menu
copy tftp startup-config	Copies a configuration from the TFTP server to the startup configuration
exit	Exits the terminal server and terminates all console sessions

Note The **clsX** command is not a Cisco IOS command but is an alias to the Cisco IOS **clear line** command that has been configured at the terminal server for ease of use in this course.

Scenario

You will familiarize yourself with the usage of the BCRAN remote lab equipment and configure your routers to accept the lab preconfiguration files.

Setup

Gather the information shown in these tables prior to starting this lab.

Remote Equipment Comm Server	Information Required	Example	Write in your remote comm server information
BCRAN terminal server	IP address	10.1.1.254	
BCRAN terminal server	Username	BCRAN	
BCRAN terminal server	Password	Cisco	

Pod Number _____ (Assigned by your instructor)	Information Required	Example (X is your pod number; all subnet masks are 255.255.255.0;	Write in the information for your pod
Central router	LAN interface IP	10.X.0.1	
Central router	LAN interface type	Ethernet0/0	
Central router	Preconfiguration file	pXcL	
Branch router	LAN interface IP	10.X.10.2	
Branch router	LAN interface type	FastEthernet0	
Branch router	Preconfiguration file	pXbL	
SOHO router	LAN interface IP	10.X.100.3	
SOHO router	LAN interface type	FastEthernet0	
SOHO router	Preconfiguration file	pXsL	
TFTP server for central	IP address	10.X.0.200	
TFTP server for branch	IP address	10.X.10.200	
TFTP server for SOHO	IP address	10.X.100.200	

Verify that your workstation has Internet connectivity.

Verify that you have established a Telnet session on the BCRAN communication server from your workstation.

Note Different pods could be equipped with different models and modules. For example, some pods may have a Cisco 3640 router, while other pods may consist of a Cisco 2600 Series router. Some pods will be using Ethernet interfaces, while other pods may use FastEthernet interfaces. Ask your instructor for further information about the differences within your equipment pods.

Task 1: Run Telnet to Connect to BCRAN Remote Lab

To begin the lab exercises, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

Exercise Procedure

Complete these steps:

Step 1 From the Microsoft Windows Start Menu, choose **Run**. The Run window displays.

Step 2 In the Open field, enter the **telnet** command followed by the IP address for your terminal server, provided by your instructor. For example, if the terminal server address your instructor provided is 10.1.1.254, you would enter the following:

```
telnet 10.1.1.254
```

If your Telnet session connects successfully to the terminal server, you should see the following authentication:

```
User Access Verification
```

```
Username:
```

Step 3 Enter the username **student** and the password given to you by your instructor.

Step 4 On successful login, you should see a menu similar to the following:

```
***** BCRAN-v2 Main Menu *****
Welcome authorized users to the
Cisco Systems Internet Learning Solutions Group BCRAN-v2
Lab.
Unauthorized access to or use of this lab is prohibited.
Type "exit" at any time while in the menu to disconnect.
*****
***
ITEM#          DEVICE NAME
-----
1             Connect to pod1
2             Connect to pod2
3             Connect to pod3
4             Connect to pod4
5             Connect to pod5
6             Connect to pod6
7             Connect to pod7
8             Connect to pod8
9             Exit
```

Please select menu item:

- Step 5** The term “pod” refers to the group of routers that you will be using to complete your lab exercises for this course. At the Please Select Menu Item prompt, enter the pod number assigned to you by your instructor and press **Return**. Your output should look similar to the following:

```
***** BCRAN-v2 pod9 *****
To exit telnet session and return to the menu press
"CTRL+SHIFT+6" then "x". If need be you can clear
connections by typing cls#
(where # = the menu item#, ie, cls2)
Type "exit" at any time while in the menu to disconnect.
*****
ITEM#      DEVICE NAME
-----
1          Connect to central 9
2          Connect to branch 9
3          Connect to soho 9
4          Return to main menu
```

Please enter selection:

- Step 6** The menu shown in Step 5 is the router selection menu. Your pod number is on the top line, and the display lists the routers in your pod. This example is for pod 9.

- Step 7** From the router selection menu, you can connect to your access router. After you have connected to a network device from the terminal server, enter the escape sequence, pressing **Ctrl-Shift-6**, then **x**, to return to the router selection menu. Although this action will bring you back to the router selection menu, your console connection to the access router will still be open and active in the background. You will be able to open additional console connections to other routers. (A terminal server console connection is similar to a standard telephone call in that there can be only one console connection to a router at a time. A second console connection to the same router would be busy. If a console connection is already open and active, then that connection will need to be cleared.)

- Step 8** Enter **3** in the router selection menu to connect to your small-office, home-office (SOHO) router. You should see the following (or something similar) in your Telnet session:

```
Please enter selection:3
Trying h1 (10.10.10.10, 2033)... Open
```

- Step 9** Press **Return** to access the device prompt.
- Step 10** To return to the router selection menu, press **Ctrl-Shift-6**, then **x**. The router selection menu displays.
- Step 11** Enter **3** to reconnect to your SOHO router and regain access to your previous console connection.
- Step 12** Return to the router selection menu by pressing **Ctrl-Shift-6**, then **x**.
- Step 13** Sometimes a connection to a device was not cleared after the previous Telnet user left. To access a device that appears to be in use, use the **clsX** command, where *X* is the number of the device you want to connect to. To clear the console connection to the SOHO router, enter **cls3**. You will be prompted to confirm this action:
- ```
Please enter selection:cls3
[confirm]
```
- Step 14** When you want to log out of the terminal, return to any menu and enter **exit** at the Please Enter Selection prompt:
- ```
Please enter selection:exit
(You have open connections) [confirm]
```
- Step 15** If there are active console connections at that time, you need to confirm by either entering **y** or pressing **Return** to close those connections.
- Step 16** Depending on which operating system is running on your PC, you may need to press **Return** after terminating your Telnet session.
- Step 17** Proceed to Task 2.

Task 2: Preparing the Central Router for the Lab Preconfiguration

This task prepares the central router for the lab preconfiguration.

Exercise Procedure

Complete these steps:

- Step 1** Connect to the console of the central router in your pod.
- Step 2** Configure the LAN interface of the central router with the IP address and subnet mask shown in the setup tables. Enable the interface with the **no shutdown** command.
- Step 3** Using the **copy tftp startup-config** command, load the preconfiguration file for your pod on the central router. The filename is formatted as pXcL, where *p* represents the pod, *X* represents your pod number, *c* represents the central router, and *L* represents the lab number. If, for example, you are on pod 9 and you are preparing for lab 1, copy the file p9c1. Use the TFTP address that is listed in the setup table.

- Step 4** After the central router has copied the preconfiguration file, execute a **show startup-config** command to display the router configuration that will be used on a reload of the central router.
- Step 5** Reload the central router and observe the output.
- Step 6** Proceed to Task 3.

Task 3: Preparing the Branch Router for the Lab Preconfiguration

This task prepares the branch router for the lab preconfiguration.

Exercise Procedure

- Step 1** Connect to the console of the branch router for your pod.
- Step 2** Configure the LAN interface of the branch router with the IP address and subnet mask that is listed in the setup tables. Do not forget to enable the interface with the **no shutdown** command.
- Step 3** Using the **copy tftp startup-config** command, load the startup configuration file on the branch router. The filename is formatted as pXbL, where p represents the pod, X represents your pod number, b represents the branch router, and L represents the lab number. If, for example, you are on pod 9 and you are preparing for lab 1, copy the file p9b1. Use the TFTP address that is listed in the setup table.
- Step 4** After the branch router has copied the preconfiguration file, execute a **show startup-config** command to display the router configuration that will be used on a reload of the branch router.
- Step 5** Reload the branch router and observe the output.
- Step 6** Proceed to Task 4.

Task 4: Preparing the SOHO Router for the Lab Preconfiguration

This task prepares the SOHO Router for the lab preconfiguration.

Exercise Procedure

Complete these steps:

- Step 1** Connect to the console of the SOHO router for your pod.
- Step 2** Configure the LAN interface of the SOHO router with the IP address and subnet mask that is listed in the setup tables. Do not forget to enable the interface with the **no shutdown** command.
- Step 3** Using the **copy tftp startup-config** command, load the preconfiguration file on the SOHO router. The filename is formatted as pXsL, where p represents the pod, X represents your pod number, s represents the SOHO router, and L represents the lab number. If, for example, you are on pod 9 and you are preparing for lab 1, copy the file p9s1. Use the TFTP address that is listed in the setup tables.

Step 4 After the SOHO router has copied the preconfiguration file, execute a **show startup-config** command to display the router configuration that will be used on a reload of the SOHO router.

Step 5 Reload the SOHO router and observe the output.

Exercise Verification

You have completed this exercise when you have attained these results:

- Successfully navigated through the BCRAN remote equipment pods
- Loaded the preconfiguration files onto the central, branch, and SOHO routers from the TFTP server

Lab Exercise 2-1: Configuring Asynchronous Connections with Modems

Complete the lab exercise to practice what you have learned in the related module.

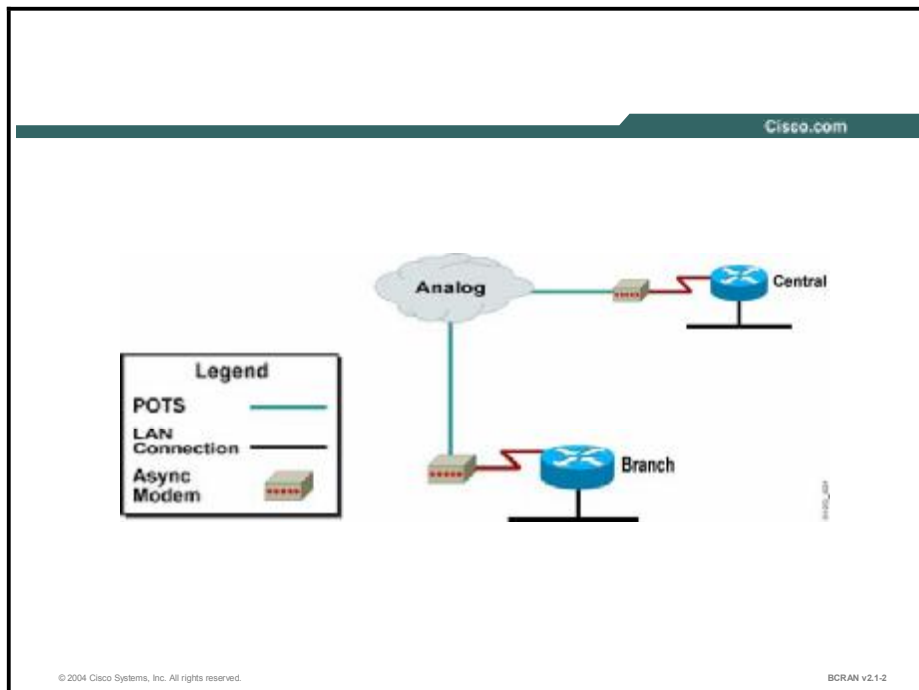
Exercise Objective

On completion of this lab, you will be able to:

- Configure an access server for modem connectivity so telecommuters can access the central site
- Establish a reverse Telnet session to the modem and configure the modem for basic asynchronous operations
- Configure the router auxiliary port to provide remote access to a router for remote configuration and diagnostics
- Set up the branch router to autoconfigure the modem
- Set up a modem connection, initiated by the central site, to the branch site router via the auxiliary port, modeling remote configuration, remote operation, and troubleshooting of network resources

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
Ctrl-Shift-6, then x	Pressing this key combination suspends the current Telnet session and returns you to the system command prompt
debug confmodem	Displays information associated with the discovery and configuration of the modem attached to the router
disconnect	Disconnects an active Telnet session
exec-timeout <i>minutes</i> [<i>seconds</i>]	Sets the interval that the EXEC command interpreter waits until user input is detected
flowcontrol hardware	Use the CTS/RTS signal lines for flow control
ip host <i>name number address</i>	Defines a name and associates it with a port or address for Telnet. (Use a 2xxx number for the line.)
login local	Selects local password checking. Authentication is based on the username specified with the username global configuration command
modem autoconfigure {<i>type modem-type</i> autodiscovery}	Sets the line to use the autoconfigure feature to configure an attached modem either by specifying the modem type or attempting to discover the type automatically
modem inout	Sets the line to allow incoming and outgoing connections
show line	Displays parameters of a terminal line
show session	Displays information about Telnet connections
speed <i>speed</i>	Defines the communications speed between the router and the modem
stopbits {0 1 1.5 2}	Defines the number of stop bits for each byte of asynchronous data
transport input all	Sets a line to allow all protocols
username <i>hostname password password</i>	Sets the username and password for local security reasons

Scenario

The central site and the branch site require occasional dialup connection to each other. On the central site, you will configure the central router auxiliary port for dialup connectivity and manually configure the modem via a reverse Telnet session. On the branch site, you will configure the branch router auxiliary port for dialup connectivity and configure the router to autoconfigure the attached modem.

Setup

Gather the information shown in this table prior to starting this lab.

Pod Number ____	Information Required	Example (X is your pod number; all subnet masks are 255.255.255.0)	Write in the information for your pod ____
Central router	Your (first) LAN interface type	Ethernet 0/0	
Central router	Your (first) LAN interface IP	10.X.0.1	
Central router	Aux line number (use show line command)	65 129	
Central router	Analog phone number	55510nn	
Branch router	Your (first) LAN interface type	FastEthernet0 Ethernet0	
Branch router	Your (first) LAN interface IP	10.X.10.2	
Branch router	Aux line number	5	
Branch router	Analog phone number	55510nn	

Setup Tasks

From your PC, establish a Telnet session on the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet session on the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

Use the TFTP facility to copy the appropriate preconfiguration files to the central and branch routers, and reload the routers.

Determine the terminal line number for the auxiliary port on both the central and branch routers using the **show line** command. Enter the information in the setup table for reference during the lab.

Task 1: Configuring the Auxiliary Port and Line Connectivity on the Central Router

To maximize the availability of the central router interfaces, you will configure the auxiliary port to connect to the modem via a rollover cable and a DCE modem adapter.

Exercise Procedure

Complete the following steps:

- Step 1** Configure the central router with the username **central_X** (where X is the pod number) and the password **cisco**.
- Step 2** Configure the auxiliary interface security settings to challenge users based on the local username.
- Step 3** Configure the auxiliary interface to allow incoming and outgoing modem connections.
- Step 4** Configure the auxiliary interface to allow any input transport protocol.
- Step 5** Configure the auxiliary interface to set the line speed between router and modem to 115200 bps. The default is 9600 bps.
- Step 6** Configure the auxiliary interface to use 1 stop bit and CTS/RTS flow control.
- Step 7** Verify your configuration and the line settings.

If you are using a Cisco 3600 Series router, your output will look similar to this:

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	
0	CTY		-	-	-	-	-	0	0	0/0
65	TTY		-	inout	-	-	-	0	0	0/0
66	TTY		-	inout	-	-	-	0	0	0/0
67	TTY		-	inout	-	-	-	0	0	0/0
68	TTY		-	inout	-	-	-	0	0	0/0
69	TTY		-	inout	-	-	-	0	0	0/0
70	TTY		-	inout	-	-	-	0	0	0/0
129	AUX	115200/115200-	-	inout	-	-	-	0	1	0/0
130	VTY		-	-	-	-	-	0	0	0/0
131	VTY		-	-	-	-	-	0	0	0/0

```

132 VTY          -   -   -   -   -   0   0   0/0
-
133 VTY          -   -   -   -   -   0   0   0/0
-
134 VTY          -   -   -   -   -   0   0   0/0
-

```

Line(s) not in async mode -or- with no hardware support:
1-64, 71-128

If you are using a Cisco 2600 Series router, your output will look similar to this:

```

      Tty Typ      Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise
Overruns  Int
*      0 CTY          -   -      -   -   -     0     0     0/0
-
      65 AUX 115200/115200- inout      -   -     0     1     0/0
-
      66 VTY          -   -      -   -   -     0     0     0/0
-
      67 VTY          -   -      -   -   -     0     0     0/0
-
      68 VTY          -   -      -   -   -     0     0     0/0
-
      69 VTY          -   -      -   -   -     0     0     0/0
-
      70 VTY          -   -      -   -   -     0     0     0/0
-

```

Step 8 To simplify the reverse Telnet connection, create a static host entry called **modem** with the **ip host** command. Use as the port number 2000 + your TTY number, and use the IP address of the central router LAN interface. For example, if you have a Cisco 2600 Series router in your pod and the TTY number of the auxiliary port is 65, the port number will be 2065.

Note The name used here is "modem" but it can be any name you choose. The TCP port number 2129 specifies a port the Telnet protocol will use to establish a connection to line 129 (TCP port 2000 + line number is a Cisco standard). The alias address that the **ip host** command references is the IP address of a valid interface that is up. In this case, the interface is the LAN interface, but it is common to use a loopback interface. Refer to the setup table for this lab for the correct interface IP address.

Step 9 Save your configuration to NVRAM.

Step 10 Proceed to Task 2.

Task 2: Configuring the Central Site Modem

There are several ways to configure a modem. In this example, you will initiate a reverse Telnet connection.

Exercise Procedure

Complete the following steps:

Step 1 From the central router, type **modem**, which is the host alias you just configured. This action connects you to the modem on the TTY line associated with your auxiliary port via reverse Telnet. Troubleshoot if necessary.

Step 2 The **login local** command prompts for a username and password. Enter the username **central_X** and the password **cisco**, then press **Return**.

Step 3 Enter **AT** and press **Return**. Observe that you receive an OK from the modem. AT commands differ by manufacturer. The AT commands used in this exercise are specific to a U.S. Robotics modem.

Step 4 Describe the function of the **AT** commands shown here. Commands are not case sensitive. Notice that typing **\$** provides useful help for the various AT commands.

1. **AT\$** _____

2. **AT&\$** _____

3. **ATD\$** _____

Write the function of each command in the space provided. Remember that you can use the **\$** feature.

4. **AT&F** _____

5. **ATI4** _____

6. **ATI5** _____

7. **ATZ3** _____

8. **ATS0=2** _____

9. **AT&W** _____

10. **ATDT** _____

Step 5 Enter the **AT&F** and **ATZ3** commands to load and reset the original factory defaults for the modem.

Step 6 Enter the **ATI4** command to display the current settings for the modem. The output should be similar to the following:

```
at14
U.S. Robotics 56K FAX EXT Settings...
  B0  E1  F1  M1  Q0  V1  X1  Y0
  BAUD=115200  PARITY=N  WORDLEN=8
  DIAL=TONE    ON HOOK   CID=0
```

```
&A1 &B0 &C1 &D2 &G0 &H0 &I0 &K1
&M4 &N0 &P0 &R1 &S0 &T5 &U0 &Y1
```

```
S00=000 S01=000 S02=043 S03=013 S04=010 S05=008
S06=004
```

```
S07=060 S08=002 S09=006 S10=014 S11=070 S12=050
S13=000
```

```
S15=000 S16=000 S18=000 S19=000 S21=010 S22=017
S23=019
```

```
S25=005 S27=000 S28=008 S29=020 S30=000 S31=128
S32=002
```

```
S33=000 S34=000 S35=000 S36=014 S38=000 S39=000
S40=001
```

```
S41=000 S42=000
```

```
LAST DIALED #:
```

```
OK
```

- Step 7** Enter the following commands in the sequence given to specify the parameters to invoke on the modem.

```
ATS0=2
```

```
AT&C1
```

```
AT&D2
```

```
AT&H1
```

```
AT&R2
```

```
AT&M4
```

```
AT&B1
```

```
AT&K1
```

```
AT&N6
```

Note You could also carefully enter the following commands in the specified sequence:

```
ATS0=2 &C1 &D2 &H1 &R2 &M4 &B1 &K1 &N6
```

- Step 8** Enter the **ATI4** command to display the current settings for the modem. The output should now be similar to the following:

```
ati4
```

```
U.S. Robotics 56K FAX EXT Settings...
```

```
B0 E1 F1 M1 Q0 V1 X4 Y0
BAUD=115200 PARITY=N WORDLEN=8
DIAL=TONE ON HOOK CID=0
&A1 &B1 &C1 &D2 &G0 &H1 &I0 &K1
```


&M4 &N6 &P0 &R2 &S0 &T5 &U0 &Y1

S00=002 S01=000 S02=043 S03=013 S04=010 S05=008
S06=004
S07=060 S08=002 S09=006 S10=014 S11=070 S12=050
S13=000
S15=000 S16=000 S18=000 S19=000 S21=010 S22=017
S23=019
S25=005 S27=000 S28=008 S29=020 S30=000 S31=128
S32=002
S33=000 S34=000 S35=000 S36=014 S38=000 S39=000
S40=001
S41=000 S42=000

LAST DIALED #:

OK

- Step 9** Save the setting to NVRAM with the **AT&W** command.
- Step 10** Press **Ctrl-Shift-6**, and then **x**, to exit the reverse Telnet session.

Note If you are doing the labs remotely, you may not be able to terminate the reverse Telnet session properly. Try pressing the **Ctrl-Shift-6** sequence twice, and then pressing **x** (**Ctrl-Shift-6, Ctrl-Shift-6, x**).

- Step 11** Enter the **show session** command to display the Telnet sessions that are currently active.
- Step 12** Enter the **disconnect** command to clear the reverse Telnet session. (This is a critical command. If you fail to disconnect, you will be unable to reconnect.)
- Step 13** Proceed to Task 3.

Task 3: Configuring the Branch Router Auxiliary Interface

This task will configure the branch router auxiliary interface including security settings.

Exercise Procedure

Complete the following steps:

- Step 1** Configure the branch router with the local username **branch_X** (where X is the pod number) and the password **cisco**.
- Step 2** Configure the auxiliary interface security settings to challenge users based on the local username.
- Step 3** Configure the auxiliary interface to allow incoming and outgoing modem connections.
- Step 4** Configure the auxiliary interface to allow any incoming transport protocol.
- Step 5** 115200 bps. The default is 9600 bps.
- Step 6** Configure the auxiliary interface to use 1 stop bit and CTS/RTS flow control.
- Step 7** Verify your configuration and the line settings. The output should look similar to the following:

```
      Tty Typ      Tx/Rx      A Modem  Roty AccO AccI   Uses   Noise
Overruns  Int
*    0 CTY
0/0      -
      5 AUX 115200/115200- inout    -    -    -     0     1
0/0      -
      6 VTY
0/0      -
      7 VTY
0/0      -
      8 VTY
0/0      -
      9 VTY
0/0      -
     10 VTY
0/0      -
```

```
Line(s) not in async mode -or- with no hardware support:
1-4
```

To simplify the reverse Telnet connection, create a static host entry called **modem** using the **ip host** command. Use the port number 2005 and use the IP address of the branch router LAN interface.

Note The name is “modem,” but it can be any name you choose. The TCP port number 2005 specifies a port that the Telnet protocol will use to establish a connection to line 5 (TCP port 2000 + line number is a Cisco standard). The alias address that the **ip host** command references is the IP address of a valid interface that is up. In this case, the interface is the LAN interface, but it is common to use a loopback interface. Refer to the setup table in this exercise for the correct interface IP address.

Step 8 Save your configuration to NVRAM.

Step 9 Proceed to Task 4.

Task 4: Configuring the Branch Modem

To configure the branch modem, you will enable the router to configure the modem automatically instead of initiating a reverse Telnet session and manually configuring the modem.

Exercise Procedure

Complete the following steps:

Step 1 Enter the **debug confmodem** command to turn on modem configuration debugging. Doing so will display the modem autodetection sequence.

Step 2 Enter the configuration mode and configure the modem line as follows:

```
line aux 0
  modem autoconfigure type usr_sportster
```

Note Instead of autoconfiguring a specific type of modem, you could let the router automatically discover the modem type. To do so, use the **modem autoconfigure discovery** command instead of the **modem autoconfigure type name** command.

Step 3 In a few seconds, you should see messages from the **debug confmodem** command you entered in Step 1. The output should look similar to the following:

```
TTY5: detection speed (115200) response ---OK---
TTY5: Modem command: --AT&F&C1&D2&H1&R2&M4&K1&B1S0=1H0--
TTY5: Modem configuration succeeded
TTY5: detection speed (115200) response ---OK---
TTY5: Done with modem configuration
```

Step 4 Save the configuration to NVRAM.

Step 5 Proceed to Task 5.

Task 5: Testing the Configuration

This task will now test the configuration.

Exercise Procedure

Complete the following steps:

- Step 1** From the central site router, enter **modem** at the command prompt.
- Step 2** When prompted for a username, enter **central_X** and the password **cisco**.
- Step 3** Enter **AT** and press **Return**. Observe that you receive an OK from the modem.
- Step 4** Initiate a call to the branch router. If the telephone number to reach the branch router were 555-1004, then you would enter **ATDT5551004**. Use the number that is listed in the setup table.
- Step 5** Eventually you should see this message:

```
CONNECT 9600/ARQ
```

It will be followed by a prompt for a username. Modems typically require approximately 30 seconds to connect. During this time, they are negotiating parameters such as line speed, data compression, and data encryption.

Note You may have to repeat Steps 4 and 5 more than once to get the desired result.

- Step 6** Enter the valid username **branch_X** and the password **cisco** to connect to the branch router.
- Step 7** You will now be at the branch prompt. Verify that you can access the privileged EXEC mode.
- Step 8** Enter **exit** to finish the session. You should now see the central site modem prompt.
- Step 9** Press **Ctrl-Shift-6**, and then **x**, to exit the reverse Telnet session.

Note If you are doing the lab remotely, you may not be able to terminate the reverse Telnet session properly. Try pressing the **Ctrl-Shift-6** sequence twice, and then **x** (**Ctrl-Shift-6**, **Ctrl-Shift-6**, **x**).

- Step 10** Enter the **disconnect** command to terminate the active Telnet session.

Exercise Verification

You have completed this exercise when you attain these results:

- Established a working modem connection between the branch site and the central site
- Configured an access server for modem connectivity so telecommuters can access the central site
- Connected to a modem via a reverse Telnet session and configured it for basic asynchronous operations
- Configured the branch router auxiliary port to support remote access for configuration and remote diagnostics
- Set up the branch router to autoconfigure the modem

On the central router, verify that your configuration contains lines similar to the following:

```
username central_X password cisco          ! Task 1 Step 1

ip host modem 2XXX 10.X.0.1                ! Task 1 Step

line aux 0
login local                                ! Task 1 Step 2
modem InOut                                ! Task 1 Step 3
transport input all                         ! Task 1 Step 4
speed 115200                                ! Task 1 Step 5
stopbits 1                                  ! Task 1 Step 6
flowcontrol hardware                         ! Task 1 Step 6
```

On the branch router, verify that your configuration contains lines similar to the following:

```
username branch_X password 0 cisco         ! Task 3 Step 1

ip host modem 2XXX 10.X.10.2              ! Task 3 Step 8

line aux 0
login local                                ! Task 3 Step 2
modem InOut                                ! Task 3 Step 3
transport input all                         ! Task 3 Step 4
speed 115200                                ! Task 3 Step 5
stopbits 1                                  ! Task 3 Step 6
flowcontrol hardware                         ! Task 3 Step 6
modem autoconfigure type usr_sportster    ! Task 4 Step 2
```

Lab Exercise Answer Key

Lab Exercise 2-1: Configuring Asynchronous Connections with Modems

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 $1$7AQL$PISjyaTKxaEoZv/r4vfQu.
!
username branch_3 password 0 cisco
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
ip host modem 2005 10.3.10.2
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface BRI0
no ip address
shutdown
no cdp enable
!
interface FastEthernet0
description This is the ethernet network for the branch
router
```

```

ip address 10.3.10.2 255.255.255.0
  speed auto
  no cdp enable
!
interface Serial0
  no ip address
  shutdown
  no cdp enable
!
interface Serial1
  no ip address
  shutdown
  no cdp enable
!
ip classless
no ip http server
ip pim bidir-enable
!
!
no cdp run
!
banner motd ^
Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2
branch branch branch branch branch branch branch branch
-----
-
Notes from the instructor:
All local passwords should be set to "cisco"
-----
-
branch branch branch branch branch branch branch branch
Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2
^
!
line con 0
  exec-timeout 30 0
  logging synchronous level all
  history size 200
line aux 0
  login local
  modem InOut

```

```

modem autoconfigure type usr_sportster
transport input all
stopbits 1
speed 115200
flowcontrol hardware
line vty 0 4
  exec-timeout 30 0
  password cisco
  logging synchronous
  login
  history size 200
!
end

```

Central Router End Configuration

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 $1$ds.D$nr65ungkflUNYSSResgQq/
!
username central_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
ip host modem 2129 10.3.0.1
!
!
call rsvp-sync
!
!
!
!
!
!
controller T1 1/0
  framing sf
  linecode ami

```



```
!  
!  
!  
interface Ethernet0/0  
  description This is the ethernet network for the central  
  router  
  ip address 10.3.0.1 255.255.255.0  
  half-duplex  
  no cdp enable  
!  
interface Ethernet0/1  
  no ip address  
  shutdown  
  half-duplex  
  no cdp enable  
!  
interface Serial3/0  
  no ip address  
  shutdown  
  no cdp enable  
!  
interface Serial3/1  
  no ip address  
  shutdown  
  no cdp enable  
!  
interface Serial3/2  
  no ip address  
  shutdown  
  no cdp enable  
!  
interface Serial3/3  
  no ip address  
  shutdown  
  no cdp enable  
!  
ip classless  
no ip http server  
!  
no cdp run  
!  
!
```

```

dial-peer cor custom
!
!
!
!
banner motd ^
Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2
central central central central central central central
central
-----
-
Notes from the instructor:
All local passwords should be set to "cisco"
-----
-
central central central central central central central
central
Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2 Lab2
^
!
line con 0
  exec-timeout 30 0
  logging synchronous level all
  history size 200
line 65 70
  flush-at-activation
line aux 0
  login local
  modem InOut
  transport input all
  stopbits 1
  speed 115200
  flowcontrol hardware
line vty 0 4
  exec-timeout 30 0
  password cisco
  logging synchronous
  login
  history size 200
!
end

```

Lab Exercise 3-1: Configuring and Verifying PPP Operations

Complete the lab exercise to practice what you learned in the related module.

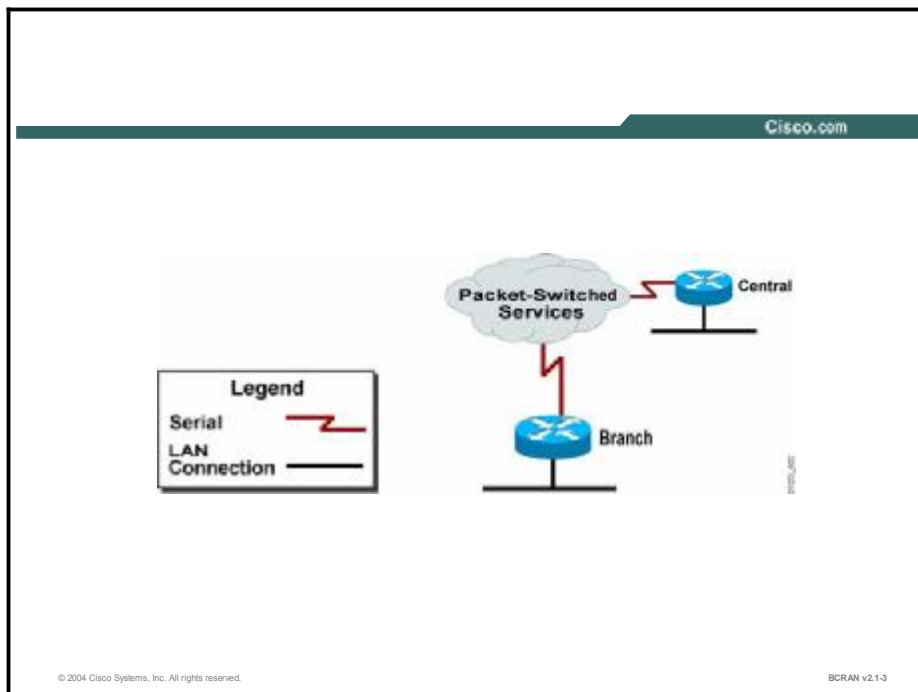
Exercise Objective

On completion of this lab, you will be able to:

- Configure PPP over a dedicated link to allow exchange of data between sites
- Configure PAP or CHAP authentication to allow access to a secure site
- Verify proper configuration and troubleshoot an incorrect configuration so data travels as intended across the PPP link
- Display network operational parameters using the appropriate **show** and **debug** commands so that you can detect anomalies

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
debug ppp authentication	Enables PPP authentication debugging
debug ppp negotiation	Enables PPP negotiation debugging
encapsulation ppp	Encapsulates PPP on the interface
ip address ip-address mask	Assigns an IP address to an interface
ppp authentication chap	Sets Challenge Handshake Authentication protocol (CHAP) as the PPP authentication method
ppp authentication pap	Sets Password Authentication Protocol (PAP) as the PPP authentication method
ppp pap sent-username username password password	Defines the username and password to send to the peer for authentication
ppp reliable-link	Enables Link Access procedure on the data (D) channel (Link Access Procedure, Balanced [LAPB]) on a PPP Link
show interface interface	Displays the configuration of an interface
undebug all	Disables all debugging
username username password password	Sets the username and password on the router for authentication

Scenario

You will configure the serial connection between the central and branch routers to forward IP traffic using PPP encapsulation. The site has selected PPP to take advantage of the security, troubleshooting, and transport protocol-independent features within PPP. Security is implemented first with PAP, then with CHAP. You will examine debugging output to become familiar with the PPP authentication and negotiation processes in the Cisco IOS software.

Note PPP is most commonly seen in dialup scenarios. This module uses a permanent serial connection so that you can focus on the PPP protocol itself, without the added complexity of asynchronous or ISDN dial-on-demand routing (DDR).

Setup

Gather the information shown in this table prior to starting this lab.

Pod Number ____	Information Required	Example (X is your pod number; all subnet masks are 255.255.255.0)	Write in the information for your pod ____
Central router	Your (first) LAN interface type	Ethernet 0/0	
Central router	Your (first) LAN interface IP	10.X.0.1	
Central router	Your (first) WAN interface type	Serial 0/0 Serial 3/0	
Central router	Your (first) WAN interface IP	10.X.160.1	
Branch router	Your (first) LAN interface type	FastEthernet0	
Branch router	Your (first) LAN interface IP	10.X.10.2	
Branch router	Your (first) WAN interface type	Serial 0	
Branch router	Your (first) WAN interface IP	10.X.160.2	

Setup Tasks

From your PC, establish a Telnet session on the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet session on the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

Use the TFTP facility to copy the appropriate preconfiguration files to the central and branch routers and reload the routers.

Task 1: Enabling PPP Debugging and Activating the Link

This task enables PPP debugging and activates the link.

Exercise Procedure

Complete the following steps:

- Step 1** Enable PPP negotiation debugging on the branch router and observe the output while completing the next steps.
- Step 2** Enable the PPP protocol on the serial interface at the branch router.
- Step 3** Enable the serial interface on the branch router, which was administratively shut down from the preconfiguration so that the PPP initialization process could be observed.
- Step 4** Enable PPP negotiation debugging on the central router and observe the output while completing the next steps.
- Step 5** Enable the PPP protocol on the serial interface at the central router.
- Step 6** Enable the serial interface on the central router, which was administratively shut down from the preconfiguration so that the PPP initialization process could be observed.
- Step 7** Enter the **no shutdown** command for the serial interface on the central router. As soon as you have entered the **no shutdown** command and both endpoints of the link are active, the **debug ppp negotiation** command should start displaying PPP negotiation output. Carefully inspect the output.

The central router debug output should be similar to the following:

```
01:30:55: Se0/0 PPP: Using default call direction
01:30:55: Se0/0 PPP: Treating connection as a dedicated line
01:30:55: Se0/0 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0
load]
01:30:55: Se0/0 LCP: O CONFREQ [Closed] id 1 len 10
01:30:55: Se0/0 LCP:   MagicNumber 0x05EEE7D5 (0x050605EEE7D5)
01:30:55: Se0/0 LCP: I CONFREQ [REQsent] id 1 len 10
01:30:55: Se0/0 LCP:   MagicNumber 0x09F99A7A (0x050609F99A7A)
01:30:55: Se0/0 LCP: O CONFACK [REQsent] id 1 len 10
01:30:55: Se0/0 LCP:   MagicNumber 0x09F99A7A (0x050609F99A7A)
01:30:55: Se0/0 LCP: I CONFACK [ACKsent] id 1 len 10
01:30:55: Se0/0 LCP:   MagicNumber 0x05EEE7D5 (0x050605EEE7D5)
01:30:55: Se0/0 LCP: State is Open
01:30:55: Se0/0 PPP: Phase is UP [0 sess, 0 load]
```

The branch router debug output should be similar to the following:

```
00:18:53: Se0 PPP: Treating connection as a dedicated line
00:18:53: Se0 PPP: Phase is ESTABLISHING, Active Open
00:18:53: Se0 LCP: O CONFREQ [Closed] id 1 len 10
00:18:53: Se0 LCP:   MagicNumber 0x09F99A7A (0x050609F99A7A)
00:18:53: Se0 LCP: I CONFREQ [REQsent] id 1 len 10
00:18:53: Se0 LCP:   MagicNumber 0x05EEEE7D5 (0x050605EEEE7D5)
00:18:53: Se0 LCP: O CONFACK [REQsent] id 1 len 10
00:18:53: Se0 LCP:   MagicNumber 0x05EEEE7D5 (0x050605EEEE7D5)
00:18:53: Se0 LCP: I CONFACK [ACKsent] id 1 len 10
00:18:53: Se0 LCP:   MagicNumber 0x09F99A7A (0x050609F99A7A)
00:18:53: Se0 LCP: State is Open
00:18:53: Se0 PPP: Phase is FORWARDING, Attempting Forward
00:18:53: Se0 PPP: Phase is ESTABLISHING, Finish LCP
00:18:53: Se0 PPP: Phase is UP
```

Note The **debug ppp negotiation** command displays a great deal of valuable information. Notice specifically that the LCP phase completes before PPP goes up and the interface moves to the up and up state.

Step 8 Proceed to Task 2.

Task 2: Configuring PPP for the IP Protocol and Verifying the Connection

This task configures PPP for IP and will verify the connection.

Exercise Procedure

Complete the following steps:

- Step 1** Disable the serial link at the central router and observe the debug output. Note that only the PPP and LCP protocols were running and are now terminating.
- Step 2** Configure the branch router serial interface with the appropriate IP address.
- Step 3** Configure the central router serial interface with the appropriate IP address.
- Step 4** Enable the central router serial interface. Notice that because you have now configured an IP address and the IP protocol has been enabled on the interface, there are now additional negotiations for IPCP after PPP is up.
- Step 5** Verify IP connectivity by pinging the central router from the branch router.

Step 6 Inspect the configuration for the serial interface by entering the **show interface** command. The output should be similar to the following:

```
<Output omitted>
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP
<Output omitted>
```

Note the states of the LCP and the configured NCPs.

Step 7 Which command will turn off all debugging?

Step 8 Disable debugging on both routers.

Step 9 Proceed to Task 3.

Task 3: Adding PAP Authentication to the Link

The following steps will configure the link to use PAP authentication and improve security.

Exercise Procedure

Complete these steps:

Note Be sure that all debugging has been disabled prior to starting this exercise.

Step 1 Shut down the serial interface at the central router, which will allow you to examine the PAP authentication.

Step 2 Configure PAP authentication, using the command list, on the central router serial interface.

Step 3 Configure the central router to send its hostname and the password **cisco** using the command list.

Step 4 On the central router, create a username and password for the branch router. Use the username of the branch router in your pod and the password **cisco**.

Note Because PAP sends passwords unencrypted, it is good security practice to use different PAP passwords in each direction. Also, keep in mind that both the username and password are case sensitive.

Step 5 On the branch router, configure PPP PAP authentication on the router serial interface.

Note Disregard warning messages similar to the following:
AAA: Warning, authentication list "default" is not defined for PPP.

- Step 6** Configure the branch router, using the command list, to send the PAP username of the branch router hostname and the password **cisco**.
- Step 7** Create a username and password for the central router. Use the username of the central router in your pod and the password **cisco**.
- Step 8** Which command will enable PPP authentication debugging on the router?

- Step 9** Enable debugging of PPP authentication on the central router.
- Step 10** Re-enable the central router serial interface.
- Step 11** Observe the output of the **debug ppp authentication** command on the router. The output should be similar to the following:
- ```
04:04:03: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
04:04:03: Serial interface PPP: Treating connection as a dedicated line
04:04:03: Serial interface PAP: O AUTH-REQ id 3 len 19 from "Central"
04:04:03: Serial interface PAP: I AUTH-REQ id 3 len 17 from "Branch"
04:04:03: Serial interface PAP: Authenticating peer Branch
04:04:03: Serial interface PAP: O AUTH-ACK id 3 len 5
04:04:03: Serial interface PAP: I AUTH-ACK id 3 len 5
04:04:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface SerialX/X, changed state to up
```
- Step 12** Proceed to Task 4.

## Task 4: Changing the Authentication from PAP to CHAP

The following steps will convert the serial link from PAP to CHAP authentication.

### Exercise Procedure

Complete these steps:

- Step 1** Disable the central router serial interface.
- Step 2** Remove PPP PAP authentication.
- Step 3** Activate CHAP authentication at the central router.
- Step 4** Which command will enable CHAP authentication on the PPP link?  
\_\_\_\_\_
- Step 5** On the branch router, remove PPP authentication PAP and then activate CHAP authentication.
- Step 6** On the central router, enable the central router serial interface.

**Step 7** Observe the output of the **debug ppp authentication** command on the router. The output should be similar to the following:

```
01:04:48: Se3/0 PPP: Using default call direction
01:04:48: Se3/0 PPP: Treating connection as a dedicated line
01:04:48: Se3/0 CHAP: O CHALLENGE id 1 len 30 from "central_X"
01:04:48: Se3/0 CHAP: I CHALLENGE id 1 len 29 from "branch_X"
01:04:48: Se3/0 CHAP: O RESPONSE id 1 len 30 from "central_X"
01:04:48: Se3/0 CHAP: I RESPONSE id 1 len 29 from "branch_X"
01:04:48: Se3/0 CHAP: O SUCCESS id 1 len 4
01:04:48: Se3/0 CHAP: I SUCCESS id 1 len
```

---

**Note** You do not need to alter the **ppp pap sent-username** configuration command because it applies only to PAP and not CHAP.

---

**Step 8** On the central router, use the **show interface** command to verify that the link comes up correctly.

**Step 9** Disable all debugging at the central router.

**Step 10** Proceed to Task 5.

## Optional Task 5: Changing LCP Parameters and Observing Renegotiation

In tasks 1 through 4, you administratively shut down one end of the link before making any changes. This shutdown was done solely to simplify the debugging output. PPP does not require that an interface be shut down to reconfigure it. In this task, you will make a change to a running link and watch LCP renegotiate, along with any NCPs.

### Exercise Procedure

Complete these steps:

**Step 1** Enable the **debug ppp negotiation** command on both routers.

**Step 2** At the central router, configure the PPP serial interface for LAPB using the **ppp reliable-link** command.

---

**Note** The LCP reliable transmission option is shown in this exercise as an example of an optional LCP parameter. It is rarely used in practice because the extra overhead that it imposes is not justified on modern high-quality transmission media.

---

**Step 3** Notice that LCP immediately restarts its negotiation phase. Keep in mind that you have reconfigured only one side for reliable mode. Do you expect it to work? Your output should be similar to the following:

```
*Mar 1 03:56:18.055: Se0/0 IPCP: State is Closed
*Mar 1 03:56:18.055: Se0/0 CDPCP: State is Closed
```

```

*Mar 1 03:56:18.055: Se0/0 PPP: Phase is ESTABLISHING,
renegotiate LCP
*Mar 1 03:56:18.055: Se0/0 LCP: O CONFREQ [Closed] id 20 len
19
*Mar 1 03:56:18.055: Se0/0 LCP: AuthProto CHAP
(0x0305C22305)
*Mar 1 03:56:18.055: Se0/0 LCP: MagicNumber 0x11018D3B
(0x050611018D3B)
*Mar 1 03:56:18.055: Se0/0 LCP: ReliableLink window 7 addr
0 (0x0B040700)
*Mar 1 03:56:18.055: Se0/0 IPCP: Remove route to 192.168.1.2
*Mar 1 03:56:18.063: Se0/0 LCP: I CONFREQ [REQsent] id 96 len
15
*Mar 1 03:56:18.063: Se0/0 LCP: AuthProto CHAP
(0x0305C22305)
*Mar 1 03:56:18.063: Se0/0 LCP: MagicNumber 0x50E77B84
(0x050650E77B84)
*Mar 1 03:56:18.063: Se0/0 LCP: O CONFACK [REQsent] id 96 len
15
*Mar 1 03:56:18.063: Se0/0 LCP: AuthProto CHAP
(0x0305C22305)
*Mar 1 03:56:18.063: Se0/0 LCP: MagicNumber 0x50E77B84
(0x050650E77B84)
*Mar 1 03:56:18.063: Se0/0 LCP: I CONFREQ [ACKsent] id 20 len
8
*Mar 1 03:56:18.063: Se0/0 LCP: ReliableLink window 7 addr
0 (0x0B040700)
*Mar 1 03:56:18.063: Se0/0 LCP: O CONFREQ [ACKsent] id 21 len
15
*Mar 1 03:56:18.063: Se0/0 LCP: AuthProto CHAP
(0x0305C22305)
*Mar 1 03:56:18.063: Se0/0 LCP: MagicNumber 0x11018D3B
(0x050611018D3B)
*Mar 1 03:56:18.071: Se0/0 LCP: I CONFACK [ACKsent] id 21 len
15
*Mar 1 03:56:18.071: Se0/0 LCP: AuthProto CHAP
(0x0305C22305)
*Mar 1 03:56:18.071: Se0/0 LCP: MagicNumber 0x11018D3B
(0x050611018D3B)
*Mar 1 03:56:18.071: Se0/0 LCP: State is Open

```

(PPP negotiation continues with the authentication and NCP phases.)

In this example, the branch router is not configured for reliable mode and therefore rejects the configuration request. The central router then resends its configuration request without the rejected option, and the link comes up normally.

## Exercise Verification

You have completed this exercise when you have attained these results:

- Configured PPP over a dedicated link
- Configured PAP or CHAP authentication to allow access to a secure site
- Verified proper configuration so that IP data travels as intended across the PPP link
- Used various **show** and **debug** commands to display network operational parameters

On the central router, verify that your configuration contains lines similar to the following:

```
username branch_X password 0 cisco ! Task 3 Step 4

interface SerialX/0
encapsulation ppp ! Task 1 Step 5
 ip address 10.X.160.1 255.255.255.0 ! Task 2 Step 3
 ppp authentication chap ! Task 4 Step 3
 ppp pap sent-username central_X password Cisco ! Task 3 Step 3
 ppp reliable-link ! Task 5 Step 2
no shutdown ! Task 4 Step 5
```

On the branch router, verify that your configuration contains lines similar to the following:

```
username central_X password 0 cisco ! Task 3 Step 7

interface Serial0
ip address 10.X.160.2 255.255.255.0 ! Task 2 Step 2
encapsulation ppp ! Task 1 Step 2
 ppp authentication chap ! Task 4 Step 4
 ppp pap sent-username branch_X password cisco ! Task 3 Step 6
no shutdown ! Task 1 Step 3
```

# Lab Exercise Answer Key

## Lab Exercise 3-1: Configuring and Verifying PPP Operations

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1EyIE$59RGcc2IGAA9TZbPt59/u/
!
username central_3 password 0 cisco
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface BRI0
no ip address
shutdown
no cdp enable
!
interface FastEthernet0
description This is the ethernet network for the branch
router
ip address 10.3.10.2 255.255.255.0
```

```

speed auto
 no cdp enable
!
interface Serial0
 description This interface connects directly to central via a
serial line
 bandwidth 128
 ip address 10.3.160.2 255.255.255.0
 encapsulation ppp
 no cdp enable
 ppp authentication chap
 ppp pap sent-username branch_3 password 0 cisco
!
interface Serial1
 no ip address
 shutdown
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.160.1
no ip http server
ip pim bidir-enable
!
!
no cdp run
!
banner motd ^
Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3
branch branch branch branch branch branch branch branch

-
Notes from the instructor:
All local passwords should be set to "cisco"

-
branch branch branch branch branch branch branch branch
Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3
^
!
!
line con 0

```

```
exec-timeout 30 0
logging synchronous level all
history size 200
line aux 0
line vty 0 4
exec-timeout 30 0
password cisco
logging synchronous
login
history size 200
!
no scheduler allocate
end
```

### Central Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1K6/G$YzrM00UiBCxa8UzqGp/XH0
!
username branch_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
!
call rsvp-sync
!
!
!
!
!
!
controller T1 1/0
framing sf
linecode ami
!
```

```

!
!
interface Ethernet0/0
 description This is the ethernet network for the central
 router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Serial3/0
 description This interface connects directly to branch via a
 serial line
 bandwidth 128
 ip address 10.3.160.1 255.255.255.0
 encapsulation ppp
 clockrate 128000
 no cdp enable
 ppp reliable-link
 ppp authentication chap
 ppp pap sent-username central_3 password 0 cisco
!
interface Serial3/1
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/2
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/3
 no ip address
 shutdown
 no cdp enable
!

```



```

ip classless
ip route 10.3.10.0 255.255.255.0 10.3.160.2
no ip http server
!
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3
central central central central central central central
central

-
Notes from the instructor:
All local passwords should be set to "cisco"

-
central central central central central central central
central
Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab3 Lab4 Lab3
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end

```

# Lab Exercise 4-1: E-Lab: Simulation for Configuring a Cisco 827 Router for NAT with PPPoA

Complete this lab exercise to practice what you learned in the related module.

## Exercise Objective

Upon completing this exercise, you will be able to:

- Perform a simulated install procedure
- Configure a Cisco 827 router for NAT with PPPoA

## Visual Objective

Use the E-Lab Show Topology button to see your visual objective.

## Scenario

Refer to the E-Lab for your scenario.

# Lab Exercise 5-1: Configuring a Site-to-Site IPSec VPN Using Preshared Keys

Complete this lab exercise to practice what you learned in the related module.

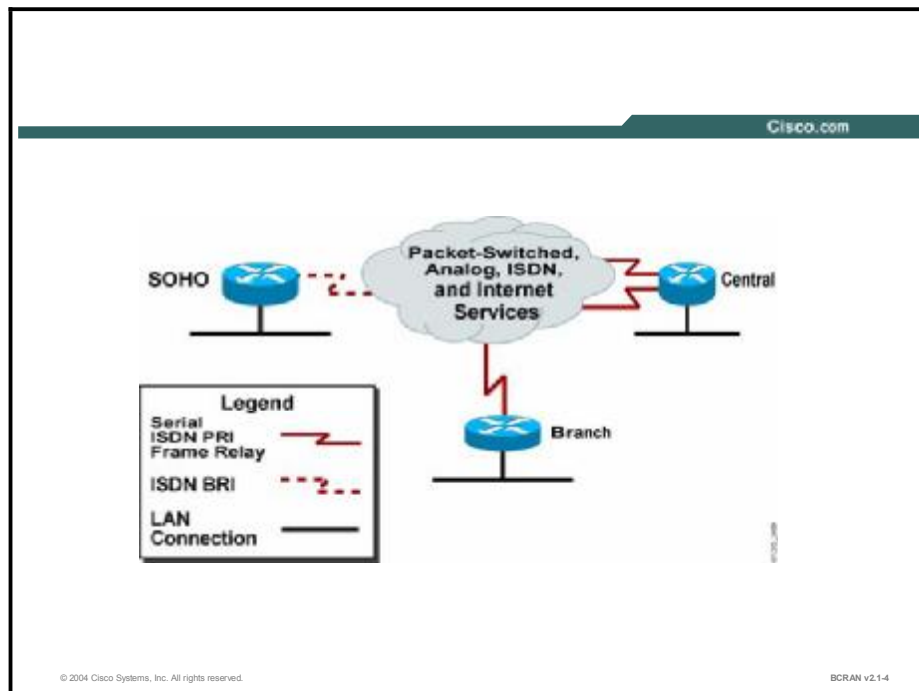
## Exercise Objective

Upon completion of this lab exercise, you will be able to:

- Plan and configure IKE between two sites
- Configure IPSec between two sites
- Verify and test an IPSec VPN

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



## Command List

The commands used in this exercise are described in the table here.

### Configuration Commands

| Command                                                                                                                                                                                                           | Description                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>authentication</b> [ <i>pre-shared</i>   <i>rsa-sig</i>   <i>rsa-encr</i> ]                                                                                                                                    | Configures the authentication method. Configure Internet Key Exchange (IKE) to use preshared keys for this lab.                                                                                                            |
| <b>clear crypto sa</b><br><b>clear crypto isakmp</b>                                                                                                                                                              | Deletes the IPsec and Internet Security Association and Key Management Protocol (ISAKMP) SAs                                                                                                                               |
| <b>crypto isakmp enable</b>                                                                                                                                                                                       | Enables the IKE process                                                                                                                                                                                                    |
| <b>crypto isakmp policy</b><br><i>priority-number</i>                                                                                                                                                             | Creates IKE policy. Uniquely identifies the IKE policy and assigns a priority to the policy.                                                                                                                               |
| <b>crypto isakmp key</b><br><i>keystring address peer address</i>                                                                                                                                                 | Configures a preshared authentication key                                                                                                                                                                                  |
| <b>crypto ipsec transform-set</b><br><i>WORD</i> [ <i>ah-md5-hmac</i>   <i>ah-sha-hmac</i>   <i>md5-hmac</i>   <i>sha-hmac</i> ]   <i>esp-des</i>   <i>esp-md5-hmac</i>   <i>esp-null</i>   <i>esp-sha-hmac</i> ] | Configures transform set suites. Transform sets equal a combination of an AH transform, an ESP transform, and the IPsec mode (either tunnel or transport mode).                                                            |
| <b>crypto map</b> <i>map-name</i>                                                                                                                                                                                 | Applies the crypto map to the IPsec router interface connected to the Internet with the crypto map command in interface configuration mode                                                                                 |
| <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i>                                                                                                                                                            | Configures IPsec crypto map                                                                                                                                                                                                |
| <b>debug crypto ipsec</b><br><b>debug crypto isakmp</b>                                                                                                                                                           | Debugs the ISAKMP and IPsec negotiation and events                                                                                                                                                                         |
| <b>match address</b> <i>ACL-number</i>                                                                                                                                                                            | Identifies the extended ACL by its name or number. The value should match the access-list number or name argument of a previously defined IP-extended access control list (ACL) being matched.                             |
| <b>set peer</b> [ <i>hostname</i>   <i>ip-address</i> ]                                                                                                                                                           | Specifies the allowed IPsec peer by IP address or hostname                                                                                                                                                                 |
| <b>set transform-set</b><br>[ <i>set_name(s)</i> ]                                                                                                                                                                | Specifies the list of transform sets in priority order. For an IPsec manual crypto map, you can specify only one transform set. For an IPsec-ISAKMP or dynamic crypto map entry, you can specify up to six transform sets. |
| <b>show crypto isakmp policy</b>                                                                                                                                                                                  | Displays configured IKE protection policy                                                                                                                                                                                  |
| <b>show crypto map</b><br><b>show crypto ipsec transform set</b><br><b>show crypto ipsec sa</b><br><b>show crypto isakmp sa</b>                                                                                   | Displays configured crypto maps, transform sets, and security associations                                                                                                                                                 |
| <b>show crypto engine connections active</b>                                                                                                                                                                      | Displays a status summary for any active IPsec connections                                                                                                                                                                 |

## Scenario

Management has decided that communications between the SOHO and branch office requires a method of insuring that sensitive corporate data is not being intercepted on the Frame Relay link. As the network administrator, you have decided to implement a site-to-site VPN solution. The solution that you will be implementing will enable a site-to-site IPSec based VPN to ensure confidentiality, integrity, and authentication. In this scenario, the central Site will act as the Internet service provider.

## Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number ____ | Information Required          | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod ____ |
|-----------------|-------------------------------|--------------------------------------------------------------------|--------------------------------------------|
| Central router  | Your (first) WAN interface IP | 10.X.160.1                                                         |                                            |
| Central router  | ISDN number                   | 555X100                                                            |                                            |
| Central router  | Dialer 2 IP to SOHO           | 10.X.210.1                                                         |                                            |
| Branch router   | Your (first) LAN interface IP | 10.X.10.2                                                          |                                            |
| Branch router   | Your (first) WAN interface IP | 10.X.160.2                                                         |                                            |
| SOHO router     | Your (first) LAN interface IP | 10.X.100.3                                                         |                                            |
| SOHO router     | ISDN number                   | 555X300                                                            |                                            |
| SOHO router     | Dialer 2 IP to central        | ip unnumbered Loopback0                                            |                                            |
| SOHO router     | Loopback 0 IP                 | 10.X.210.3                                                         |                                            |

### Setup Tasks

From your PC, establish a Telnet connection to the terminal server and open a console connection to the central router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a second console connection to the branch router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a third console connection to the SOHO router of your pod.

You will now be able to configure and observe output on all routers simultaneously.

TFTP the appropriate preconfiguration files on the central, branch, and SOHO routers and reload the routers.

Verify that your branch and central routers each have a serial link connection to each other.

Verify that your central and SOHO routers each have an ISDN connection to the ISDN service provider.

Verify that the branch router can successfully execute a ping to the LAN interface of the SOHO router.

Verify that the SOHO router can successfully execute a ping to the LAN interface of the branch router.

## Task 1: Configure IKE on the Central Router

Use the following steps to configure IKE on the central router.

### Exercise Procedure

Complete these steps:

**Step 1** On the branch router, plan the parameters for IKE. (The default values are in bold.)

| Parameter                                       | Branch Site | SOHO Office |
|-------------------------------------------------|-------------|-------------|
| Key distribution method—manual or <b>isakmp</b> | isakmp      | isakmp      |
| Encryption algorithm— <b>DES</b> or 3DES        | DES         | DES         |
| Hash algorithm—MD5 or <b>SHA-1</b>              | SHA-1       | SHA-1       |
| Authentication method—Pre-share or <b>RSA</b>   | pre-share   | pre-share   |
| Key exchange—D-H <b>Group 1</b> or 2            | Group 1     | Group 1     |
| IKE SA Lifetime— <b>86400</b> seconds or less   | 86400       | 86400       |
| Peer IP Address                                 | 10.X.210.3  | 10.X.160.2  |

**Step 2** Using the command list, enable IKE on the branch router.

**Step 3** Using the command list, create an IKE policy with a priority of 100 using preshared keys as the method of authentication.

**Step 4** Configure the preshared key to be *cisco1234*, using the Loopback 0 IP of the SOHO router as the address of your peer.

---

**Note** A given preshared key is a private key shared between two peers. At a given peer you could specify the same key to share with multiple remote peers; however, a more secure approach is to specify different keys to share between different pairs of peers.

---

**Step 5** Save the branch router configuration.

**Step 6** To verify the branch router IKE policy, which command would you use?

---

**Step 7** Your configuration output should look similar to the following:

```
Protection suite of priority 100
 encryption algorithm: DES - Data Encryption Standard
 (56 bit keys) .
 hash algorithm: Secure Hash Standard
```

```

 authentication method: Pre-Shared Key
 Diffie-Hellman group: #1 (768 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite
 encryption algorithm: DES - Data Encryption Standard
(56 bit keys).
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman
Signature
 Diffie-Hellman group: #1 (768 bit)
 lifetime: 86400 seconds, no volume limit

```

**Step 8** Proceed to Task 2.

## Task 2: Configure IKE on the SOHO Router

Use the following steps to configure IKE on the SOHO router.

### Exercise Procedure

Complete these steps:

- Step 1** Using the command list, enable IKE on the SOHO router.
- Step 2** Using the command list, create an IKE policy with a priority of 100 using preshared keys as the method of authentication.
- Step 3** Using the command list, configure a preshared key of *cisco1234*, using the first WAN Interface IP of the branch router as your peer address.
- Step 4** Save the SOHO router configuration.
- Step 5** Verify the SOHO router IKE policy. Your configuration output should look similar to the following:

```

Protection suite of priority 100
 encryption algorithm: DES - Data Encryption Standard
(56 bit keys).
 hash algorithm: Secure Hash Standard
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #1 (768 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite
 encryption algorithm: DES - Data Encryption Standard
(56 bit keys).
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman
Signature
 Diffie-Hellman group: #1 (768 bit)

```

lifetime:

86400 seconds, no volume limit

**Step 6** Proceed to Task 3.

## Task 3: Plan and Configure IPsec on the Branch Router

Use the following steps to involve planning and configuring IPsec on the branch router.

### Exercise Procedure

Complete these steps:

**Step 1** Plan the IPsec policies.

| Policy                       | Branch       | SOHO         |
|------------------------------|--------------|--------------|
| Transform set                | esp-des      | esp-des      |
| Traffic type to be encrypted | IP           | IP           |
| SA establishment             | ipsec-isakmp | ipsec-isakmp |

**Step 2** You must configure an access list that will serve as the rule that specifies which traffic will be encrypted. For this lab, you must protect all traffic originating from the branch router LAN network going to the SOHO router LAN network. Configure an extended access list 120 that will define this traffic going between the branch router and SOHO router.

**Step 3** Using the command list, configure an IPsec transform set call MYSET and specify that you will be using Encapsulating Security Payload (ESP) with Data Encryption Standard (DES).

---

**Note** Up to three transform sets can be in a set. Sets are limited to one AH and up to two ESP transforms.

---

**Step 4** Using the command list, configure an IPsec crypto map using a map name of MYMAP and a sequence number 110. Configure this crypto map using the **ipsec-isakmp** command.

**Step 5** Configure the crypto map MYMAP to match the access list 120.

**Step 6** Configure the crypto map MYMAP to set the peer address to the SOHO router loopback 0 interface IP.

**Step 7** Configure the crypto map MYMAP to also set the transform set MYSET upon the match condition.

**Step 8** Apply crypto map **MYMAP** to the branch router serial interface.

**Step 9** Exit the configuration.

**Step 10** Use the **show crypto ipsec sa** command and verify your configuration settings.

**Step 11** Proceed to Task 4.



## Task 4: Plan and Configure IPSec on the SOHO Router

Use the following steps to plan and configure IPSec on the SOHO router.

### Exercise Procedure

Complete these steps:

- Step 1** On the SOHO router you must configure an access list that will serve as the rule that specifies which traffic will be encrypted. For this lab, you must protect all traffic originating from the SOHO router LAN network going to the branch router LAN network. Configure an extended access list 120 that will define this traffic going between the SOHO and branch router.
- Step 2** Using the command list, configure an IPSec transform set called MYSET and specify that you will be using ESP with DES.
- Step 3** Using the command list, configure an IPSec crypto map using a map name of MYMAP and a sequence number 110. Configure this crypto map using the **ipsec-isakmp** command.
- Step 4** Configure the crypto map MYMAP to match the access list 120.
- Step 5** Configure the crypto map MYMAP to set the peer address as the branch serial interface IP.
- Step 6** Configure the crypto map MYMAP to also set the transform set MYSET upon the match condition.
- Step 7** Apply crypto map **MYMAP** to the SOHO router loopback0 interface.
- Step 8** Exit the configuration and verify using the **show run** command.
- Step 9** Use the **show crypto ipsec sa** command and verify your configuration settings.
- Step 10** Proceed to Task 5.

## Task 5: Test and Verify the VPN operation

Use the following steps to tests and verify for proper VPN operation.

### Exercise Procedure

Complete these steps:

- Step 1** Go to the branch router and disable synchronous logging on the console.

---

**Note** Synchronous logging was configured from the preconfiguration file. Although this command adds to the ease of configuration by keeping unsolicited console messages from being interspersed with solicited EXEC output, it also buffers debug output until the completion of an EXEC process, such as a ping. You will be disabling this functionality so that you can observe the debug output in real time.

---

- Step 2** Enable debugging to observe the ISAKMP and IPSec negotiation and security association creation.

- Step 3** Use the **show crypto ipsec sa** command and write the amount of packets that have been encrypted and decrypted.  
Packets encrypted \_\_\_\_\_ Packets decrypted \_\_\_\_\_
- Step 4** Use the command list to determine if there are any active IPsec connections. How many? \_\_\_\_\_
- Step 5** From the branch router, ping the SOHO router Loopback 0 Interface IP and LAN interface IP address.
- Step 6** Did you observe any debug information? \_\_\_\_\_
- Step 7** From the branch router, do an extended ping using the branch router LAN interface IP address as the source, and use as the destination IP the SOHO router LAN interface IP address.
- Step 8** Now verify the security associations using the **show crypto ipsec sa** and **show crypto isakmp sa** commands.
- Step 9** Complete the following information from the show commands:  
Packets encrypted \_\_\_\_\_ Packets decrypted \_\_\_\_\_
- Step 10** Use the command list to determine if there are any active IPsec connections. How many? \_\_\_\_\_  
How many connections comprise an IPsec tunnel and why?  
\_\_\_\_\_
- 
- Step 11** Optional. If you want to observe the process again, clear the SAs using the **clear crypto sa** and the **clear crypto isakmp** commands. Then generate interesting traffic by doing additional extended pings between routers.

## Exercise Verification

You completed this exercise when you attain these results:

- If you successfully pinged the SOHO LAN IP address from the branch office router and vice versa. Also, you must verify that the security associations have been created and are protecting the traffic.

On the branch router, verify that your configuration contains lines similar to the following:

```
crypto isakmp enable ! Task 1 step 2
crypto isakmp policy 100 ! Task 1 step 4
 authentication pre-share ! Task 1 step 4
crypto isakmp key cisco1234 address 10.X.210.3 ! Task 1 step 5

crypto ipsec transform-set MYSET esp-des ! Task 3 step 3
crypto map MYMAP 110 ipsec-isakmp ! Task 3 step 4
 set peer 10.X.210.3 ! Task 3 step 6
 set transform-set MYSET ! Task 3 step 7
 match address 120 ! Task 3 step 5
```

```

interface Serial 0
crypto map MYMAP ! Task 3 step 8
! Task 3 step 2
access-list 120 permit ip 10.X.10.0 0.0.0.255 10.X.100.0 0.0.0.255

line console 0
 no logging synchronous ! Task 5 step 1

```

On the SOHO router, verify that your configuration contains lines similar to the following:

```

crypto isakmp enable ! Task 2 step 1
crypto isakmp policy 100 ! Task 2 step 3
 authentication pre-share ! Task 2 step 3
crypto isakmp key cisco1234 address 10.X.160.2 ! Task 2 step 4

```

```

crypto ipsec transform-set MYSET esp-des ! Task 4 step 2
crypto map MYMAP 110 ipsec-isakmp ! Task 4 step 3
 set peer 10.X.160.2 ! Task 4 step 5
 set transform-set MYSET ! Task 4 step 6
 match address 120 ! Task 4 step 4

```

```

interface Loopback0
 ip address 10.X.210.3 255.255.255.0 ! From preconfig

```

```

interface Dialer 2 ! From preconfig
ip unnumbered Loopback0 ! From preconfig
crypto map MYMAP ! Task 4 step 8

```

```

! Task 4 step 1
access-list 120 permit ip 10.X.100.0 0.0.0.255 10.X.10.0 0.0.0.255

```

# Lab Exercise Answer Key

## Lab Exercise 5-1: Configuring a Site-to-Site IPSec VPN Using Preshared Keys

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1t0HV$quka4kAjmrkyAkXpxbrOp/
!
memory-size iomem 25
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 100
 authentication pre-share
crypto isakmp key cisco1234 address 10.3.210.3
!
!
crypto ipsec transform-set MYSET esp-des
!
crypto map MYMAP 110 ipsec-isakmp
 set peer 10.3.210.3
 set transform-set MYSET
 match address 120
!
```

```

!
!
!
interface BRI0
 no ip address
 shutdown
 no cdp enable
!
interface FastEthernet0
 description This is the Ethernet network for the Branch router
 ip address 10.3.10.2 255.255.255.0
 speed auto
 no cdp enable
!
interface Serial0
 description This interface connects directly to Central via a
serial line
 bandwidth 128
 ip address 10.3.160.2 255.255.255.0
 encapsulation ppp
 no cdp enable
 crypto map MYMAP
!
interface Serial1
 no ip address
 shutdown
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.160.1
no ip http server
ip pim bidir-enable
!
!
access-list 120 permit ip 10.3.10.0 0.0.0.255 10.3.100.0
0.0.0.255
no cdp run
!
banner motd ^
Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5
branch branch branch branch branch branch branch branch

```

-----  
Notes from the instructor:

All local passwords should be set to "cisco"  
-----

branch branch branch branch branch branch branch branch

Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5

^

```
!
line con 0
 exec-timeout 30 0
 history size 200
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end
```

### Central Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1N.O.$iD2A0G19WY51P5xk8cO.U1
!
username soho_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
!
isdn switch-type primary-5ess
call rsvp-sync
```

```

!
!
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
!
interface Ethernet0/0
 description This is the Ethernet network for the Central router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Serial1/0:23
 no ip address
 encapsulation ppp
 dialer pool-member 2
 isdn switch-type primary-5ess
 no cdp enable
 ppp authentication chap
!
interface Serial3/0
 description This interface connects directly to Branch via a
 serial line
 bandwidth 128
 ip address 10.3.160.1 255.255.255.0
 encapsulation ppp
 clockrate 128000
 no cdp enable

```

```

!
interface Serial3/1
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/2
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/3
 no ip address
 shutdown
 no cdp enable
!
interface Dialer2
 description This dialer goes from Central to soho
 ip address 10.3.210.1 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer remote-name soho_3
 dialer string 5553300
 dialer-group 1
 no cdp enable
 ppp authentication chap
!
ip classless
ip route 10.3.10.0 255.255.255.0 10.3.160.2
ip route 10.3.100.0 255.255.255.0 10.3.210.3
no ip http server
!
dialer-list 1 protocol ip permit
no cdp run
!
!
dial-peer cor custom
!
!
!

```



```

!
banner motd ^
Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5
central central central central central central central

Notes from the instructor:
All local passwords should be set to "cisco"

central central central central central central central
Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end

```

### SOHO Router End Configuration

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname soho_3
!
enable secret 5 1aNN7$a0cNnou/3pPLS5d5ZRy8b1
!
username central_3 password 0 cisco
ip subnet-zero

```

```

no ip domain-lookup
!
isdn switch-type basic-5ess
!
crypto isakmp policy 100
 authentication pre-share
crypto isakmp key cisco1234 address 10.3.160.2
!
!
crypto ipsec transform-set MYSET esp-des
!
crypto map MYMAP 110 ipsec-isakmp
 set peer 10.3.160.2
 set transform-set MYSET
 match address 120
!
!
!
!
interface Loopback0
 ip address 10.3.210.3 255.255.255.0
 crypto map MYMAP
!
interface Ethernet0
 description This is the Ethernet network for the soho router
 ip address 10.3.10.3 255.255.255.0 secondary
 ip address 10.3.100.3 255.255.255.0
 no cdp enable
!
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 2
 isdn switch-type basic-5ess
 no cdp enable
 ppp authentication chap
!
interface Dialer2
 description This dialer goes from soho to Central
 ip unnumbered Loopback0

```

```

encapsulation ppp
dialer pool 2
dialer remote-name central_3
dialer string 5553100
dialer-group 1
no cdp enable
ppp authentication chap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.210.1
no ip http server
!
access-list 120 permit ip 10.3.100.0 0.0.0.255 10.3.10.0
0.0.0.255
dialer-list 1 protocol ip permit
no cdp run
banner motd ^
Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab12
soho soho soho soho soho soho soho soho soho soho soho soho

-
Notes from the instructor:
All local passwords should be set to "cisco"

-
soho soho soho soho soho soho soho soho soho soho soho soho
Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5 Lab5
^
!
line con 0
exec-timeout 30 0
logging synchronous level all
history size 200
line vty 0 4
exec-timeout 30 0
password cisco
logging synchronous
login
history size 200
!
end

```

# Lab Exercise 6-1: Using ISDN and DDR to Enhance Remote Connectivity

Complete the lab exercise to practice what you learned in the related module.

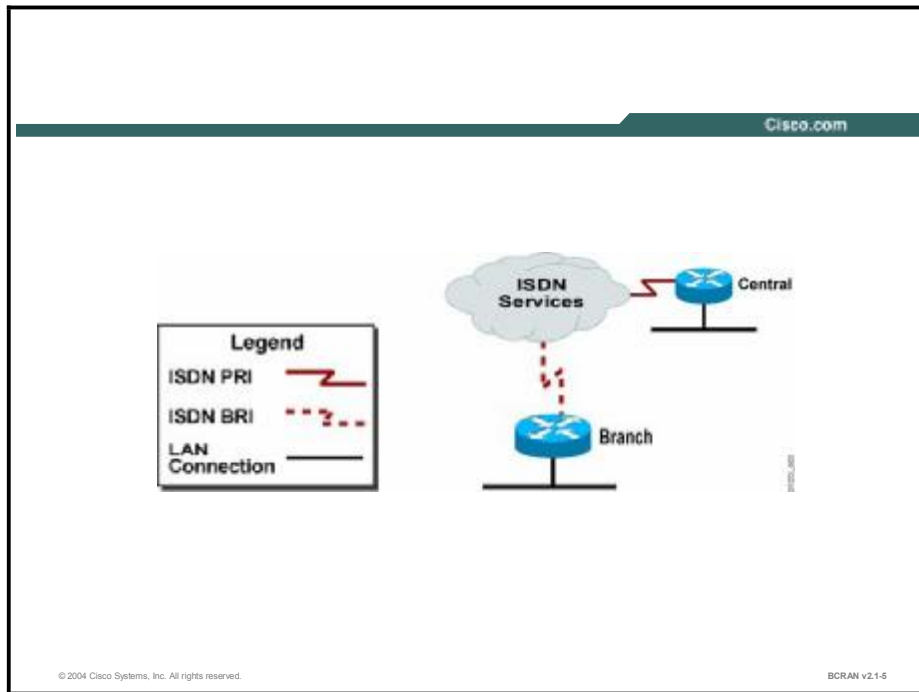
## Exercise Objective

Upon completing this lab, you will be able to:

- Configure ISDN BRI, including the switch type
- Configure ISDN PRI, including the switch type, controller type, framing type, line coding, PRI group timeslots, and speed
- Configure PPP encapsulation, including authentication, bandwidth aggregation, and callback
- Configure PPP authentication using CHAP for security between sites
- Configure MLP to aggregate bandwidth
- Configure PPP callback to model situations where it is more economical for the site receiving the call to pay for it
- Identify the Q.921 and Q.931 signaling and call setup sequences, given an ISDN call connection

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



# Command List

The commands used in this exercise are described in the table here.

## Configuration Commands

| Command                                                                                                                                                                         | Description                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>clocksource</b> <i>source</i>                                                                                                                                                | Specifies the PRI controller clock source                                                                                          |
| <b>debug dialer</b>                                                                                                                                                             | Monitors dialer events                                                                                                             |
| <b>debug isdn q921</b>                                                                                                                                                          | Monitors Q921 negotiations                                                                                                         |
| <b>debug isdn q931</b>                                                                                                                                                          | Monitors Q931 negotiations                                                                                                         |
| <b>dialer callback-secure</b>                                                                                                                                                   | Enables callback security                                                                                                          |
| <b>dialer callback-server</b><br><i>username</i>                                                                                                                                | Specifies that the callback server use the username when calling back to the client                                                |
| <b>dialer-group</b> <i>group-number</i>                                                                                                                                         | Assigns a dialer group to an interface                                                                                             |
| <b>dialer hold-queue</b><br><i>packets</i>                                                                                                                                      | Specifies the amount of packets that will be held in queue                                                                         |
| <b>dialer idle-timeout</b><br><i>sec</i>                                                                                                                                        | Specifies how long the line will remain active with no additional interesting traffic                                              |
| <b>dialer-list</b> <i>dialer-group</i> <b>protocol</b><br><i>protocol-name</i> { <b>permit</b><br>  <b>deny</b>   <b>list</b> <i>access-list-number</i>   <i>access-group</i> } | Specifies interesting traffic and associates it to a dialer group                                                                  |
| <b>dialer load-threshold</b><br><i>load</i>                                                                                                                                     | Specifies the load threshold to activate additional lines                                                                          |
| <b>dialer map ip</b> <i>next-hop-address</i> <b>name</b><br><i>destination-router-name</i> <i>phone-number</i>                                                                  | Specifies how to call a destination                                                                                                |
| <b>encapsulation</b> <b>ppp</b>                                                                                                                                                 | Enables the PPP protocol on the interface                                                                                          |
| <b>framing</b> <i>framing-type</i>                                                                                                                                              | Specifies the PRI controller framing type on a line                                                                                |
| <b>isdn switch-type</b><br><b>basic-switch-type</b>                                                                                                                             | Specifies a BRI switch type                                                                                                        |
| <b>isdn switch-type</b><br><b>primary-switch-type</b>                                                                                                                           | Specifies a PRI switch type                                                                                                        |
| <b>linecode</b> <i>type</i>                                                                                                                                                     | Specifies the PRI controller line code                                                                                             |
| <b>map-class</b> <b>dialer</b><br><i>class-name</i>                                                                                                                             | Specifies the dialer map class                                                                                                     |
| <b>ppp authentication</b><br><b>chap</b>                                                                                                                                        | Sets CHAP as the PPP authentication method                                                                                         |
| <b>ppp authentication</b><br><b>chap callin</b>                                                                                                                                 | Sets CHAP as the PPP authentication method but specifies that the authentication only occur once and by the remote initiating peer |
| <b>ppp callback</b> <b>accept</b>                                                                                                                                               | Enables callback capability on the server interface                                                                                |

| Command                         | Description                                                               |
|---------------------------------|---------------------------------------------------------------------------|
| <b>ppp callback request</b>     | Enables callback capability on the client                                 |
| <b>ppp multilink</b>            | Enables multilink capability                                              |
| <b>pri-group timeslots 1-24</b> | Enables PRI on the interface and assigns the timeslots                    |
| <b>show dialer</b>              | Displays general diagnostic information for interfaces configured for DDR |
| <b>show isdn status</b>         | Displays the ISDN line status information                                 |

## Scenario

Your company requires an ISDN connection between the central site and many branch sites. Therefore, the central router has an ISDN PRI interface installed. For branch sites, the router has an ISDN BRI interface installed.

Configure both routers to place ISDN calls between the central site and a branch site. Configure Multilink PPP (MLP) to maximize the bandwidth. Finally, the central site has negotiated a better service agreement with the telco provider. It is more economical for the central site to incur the toll charge rather than the branch site. For this reason, configure PPP callback.

## Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number _____ | Information Required             | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod |
|------------------|----------------------------------|--------------------------------------------------------------------|---------------------------------------|
| Central router   | Your (first) LAN interface type  | Ethernet 0/0                                                       |                                       |
| Central router   | Your (first) LAN interface IP    | 10.X.0.1                                                           |                                       |
| Central router   | Your (first) ISDN controller     | T1 1/0                                                             |                                       |
| Central router   | ISDN interface IP to branch      | 10.X.200.1                                                         |                                       |
| Central router   | ISDN switch type                 | primary-5ess                                                       |                                       |
| Central router   | ISDN number                      | 555X100                                                            |                                       |
| Branch router    | Your (first) LAN interface type  | FastEthernet0                                                      |                                       |
| Branch router    | Your (first) LAN interface IP    | 10.X.10.2                                                          |                                       |
| Branch router    | Your (first) ISDN interface type | Bri0                                                               |                                       |
| Branch router    | ISDN interface IP to central     | 10.X.200.2                                                         |                                       |
| Branch router    | ISDN switch type                 | basic-5ess                                                         |                                       |

| Pod Number _____ | Information Required | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod |
|------------------|----------------------|--------------------------------------------------------------------|---------------------------------------|
| Branch router    | ISDN number          | 555X200                                                            |                                       |

## Setup Tasks

From your PC, establish a Telnet connection to the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

TFTP the appropriate preconfiguration files to the central and branch routers and reload the routers.

## Task 1: Configuring the ISDN BRI on the Branch Office Router

Use the following steps to configure the ISDN BRI on the branch office router.

### Exercise Procedure

Complete these steps:

- Step 1** Using the command list, configure the branch router to use the ISDN switch type that is listed in the setup table.
- Step 2** Using the command list, configure a username **central\_X** (where **X** is the number of your pod) and a password **cisco** for the connection to the central router.
- Step 3** Configure the BRI 0 interface for PPP encapsulation and CHAP authentication.

---

**Note** Ignore the following message: AAA: Warning, authentication list "default" is not defined for PPP, because in this exercise you will be using local authentication only.

---

- Step 4** Assign the dialer list 1 to the BRI 0 interface.
- Step 5** Configure the BRI 0 for an idle timeout of 60 seconds.
- Step 6** Configure the BRI 0 for a hold queue of 5 packets.
- Step 7** Configure the BRI 0 with a dialer map, which configures the central router IP address with the central router hostname and ISDN number.
- Step 8** Configure the BRI 0 with an IP address that is listed in the setup table.

---

**Note** Do not enter the **no shut** command, because you must identify the Q.921 signaling and call setup sequences.

---

- Step 9** Configure a dialer list 1 to allow all IP packets to trigger a call.

- Step 10** Configure a static default route with a next-hop IP address set to the central router.
- Step 11** Verify and save your configuration.
- Step 12** Examine ISDN status and enable Q.921 debugging. Use these commands to view the current status of your router ISDN interface and connections:

```
show isdn status
show interface bri 0
debug isdn q921
```

The output from these commands should be similar to these examples:

```
Branch#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
 dsl 0, interface ISDN Switchtype = basic-5ess
Layer 1 Status:
 DEACTIVATED
Layer 2 Status:
 Layer 2 NOT Activated
Layer 3 Status:
 0 Active Layer 3 Call(s)
Active dsl 0 CCBs = 0
The Free Channel Mask: 0x80000003
Number of L2 Discards = 0, L2 Session ID = 0
Total Allocated ISDN CCBs = 0
```

```
Branch#show interface bri0
BRI0 is administratively down, line protocol is down
Hardware is PQUICC BRI
Internet address is 10.2.200.2/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
< Output Omitted >
```

```
Branch#debug isdn q921
ISDN Q921 packets debugging is on
```



**Step 13** Activate the BRI 0 interface and observe the output generated by the **debug** command. The output should be similar to the following:

```
00:43:25: %LINK-3-UPDOWN: Interface BRI0:1, changed state to
down
00:43:25: %LINK-3-UPDOWN: Interface BRI0:2, changed state to
down
00:43:25: ISDN BR0: RX <- IDREM ri=0 ai=127
00:43:25: %LINK-3-UPDOWN: Interface BRI0, changed state to up
00:43:25: ISDN BR0: TX -> IDREQ ri=86 ai=127
00:43:25: ISDN BR0: RX <- IDASSN ri=86 ai=64
00:43:25: ISDN BR0: TX -> SABMEp c/r=0 sapi=0 tei=64
00:43:25: ISDN BR0: RX <- UAf c/r=0 sapi=0 tei=64
00:43:25: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 64
changed to up
```

---

**Note** Q.921 debugging displays activity between the telco switch and the router every ten seconds.

---

**Step 14** Return to privileged EXEC mode and turn off the debugging.

**Step 15** Now that the BRI 0 interface has been activated, examine the output of the **show isdn status** and the **show interface bri 0** commands.

```
show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
 dsl 0, interface ISDN Switchtype = basic-5ess
Layer 1 Status:
 ACTIVE
Layer 2 Status:
 TEI = 64, Ces = 1, SAPI = 0, State =
MULTIPLE FRAME ESTABLISHED
Layer 3 Status:
 0 Active Layer 3 Call(s)
Active dsl 0 CCBS = 0
The Free Channel Mask: 0x80000003
Number of L2 Discards = 0, L2 Session ID = 3
Total Allocated ISDN CCBS = 0

show interface bri 0
BRI0 is up, line protocol is up (spoofing)
Hardware is PQUICC BRI
Internet address is 10.2.200.1/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
```

< Output Omitted >

Notice that the terminal endpoint identifier (TEI) reported by the **show isdn status** command corresponds to the number seen in the Q.921 debugging. Also note the up-up (spoofing) state of the BRI interface.

**Step 16** Proceed to Task 2.

## Task 2: Configuring ISDN PRI on Your Central Site Router

Use the following steps to configure the ISDN PRI on your central site router.

### Exercise Procedure

Complete these steps:

- Step 1** Using the command list, configure the central router to use the ISDN switch type that is listed in the setup table.
- Step 2** Using the command list, configure a username **branch\_X** (where **X** is the number of your pod) and a password **cisco** for the connection to the branch router.
- Step 3** Configure the ISDN PRI controller with “Primary Rate ISDN controller.”
- Step 4** Configure the T1 1/0 controller to use a linecode **b8zs** and framing type **esf**.
- Step 5** Configure the T1 1/0 controller to extract the clock from the line.

---

**Note** The T1 controller must also have a clock source identified as part of the basic link parameters. By default, the controller is configured to extract the clock from the line that is the default and will not appear in your final configuration.

---

- Step 6** Enable PRI and assign timeslots on the T1 controller. When you complete the configuration, you will see the newly created subinterfaces that represent the enabled channels change states. The last line should show that the D channel, Serial 1/0:23, is up. The output should look similar to:

```
00:19:56: %ISDN-6-LAYER2UP: Layer 2 for Interface Se1/0:23,
TEI 0 changed to up
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:0, changed state to down
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:1, changed state to down
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:2, changed state to down
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:3, changed state to down
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:4, changed state to down
```

```
00:19:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0:5, changed state to down
<Output omitted>
00:20:00: %LINK-3-UPDOWN: Interface Serial1/0:23, changed
state to up
```

- Step 7** Configure the Serial1/0:23 interface for PPP encapsulation and CHAP authentication.
- Step 8** Assign the dialer list 1 to the Serial1/0:23 interface.
- Step 9** Configure Serial1/0:23 for an idle timeout of 60 seconds.
- Step 10** Configure the Serial1/0:23 interface for a hold queue of 5 packets.
- Step 11** Configure the Serial1/0:23 interface with a dialer map, which configures the branch router IP address with the branch router hostname and ISDN number.
- Step 12** Configure the Serial1/0:23 interface with an IP address that is listed in the setup table.
- Step 13** Configure a dialer list 1 to allow all IP packets to trigger a call.
- Step 14** Configure a static route to the branch router stub network with a next-hop IP address set to the branch router.
- Step 15** Verify and save your configuration.
- Step 16** Examine ISDN status of your PRI interface with the **show isdn status** and **show interface serial 1/0:23** commands.

**show isdn status**

```
Global ISDN Switchtype = primary-5ess
```

```
ISDN Serial1/0:23 interface
```

```
 dsl 0, interface ISDN Switchtype = primary-ni
```

```
 Layer 1 Status:
```

```
 ACTIVE
```

```
 Layer 2 Status:
```

```
 TEI = 0, Ces = 1, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
```

```
 Layer 3 Status:
```

```
 0 Active Layer 3 Call(s)
```

```
 Activated dsl 0 CCBS = 0
```

```
 Total Allocated ISDN CCBS = 0
```

**show interface serial 1/0:23**

```
Serial/0:23 is up, line protocol is up (spoofing)
```

```
 Hardware is DSX1
```

```
 Internet address is 10.1.200.1/24
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255,
load 1/255
```

```
Encapsulation PPP, loopback not set
```

```
< Output Omitted >
```

**Step 17** Proceed to Task 3.

## Task 3: Verifying the ISDN Connection

In this task you will be using various **show** and **debug** commands to become familiar with ISDN operations.

### Exercise Procedure

Complete these steps:

**Step 1** Enter the branch router and disable synchronous logging for the console port.

---

**Note** Synchronous logging was configured from the preconfiguration file. Although this command adds to the ease of configuration by keeping unsolicited console messages from being interspersed with solicited EXEC output, it also buffers debug output until the completion of an EXEC process, such as a ping. You will be disabling this functionality so that you can observe the debug output in real time.

---

**Step 2** From the branch router, ping the central site router LAN interface. The output should be similar to:

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.X.0.1, timeout is 2
seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/78/264 ms
```

```
00:13:24: %LINK-3-UPDOWN: Interface BRI0:1, changed state to
up
```

```
00:13:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
```

```
00:13:30: %ISDN-6-CONNECT: Interface BRI0:1 is now connected
to 5552100 central_2_
```

---

**Note** Your ISDN connection is now active and will remain active as long as interesting IP traffic travels over the link. Remember that if the link sits idle for longer than 60 seconds, the BRI 0 interface will disconnect if set with the **dialer idle-timeout 60** command. If you repeatedly issue the **show dialer** command, you can accurately estimate when the line will disconnect by noting the "Time until disconnect XX secs."

---

**Step 3** Enter **show dialer**. The output should be similar to:

```
show dialer
```

```
BRI0 - dialer type = ISDN
```

| Dial String<br>status | Successes | Failures | Last DNIS | Last     |
|-----------------------|-----------|----------|-----------|----------|
| 555X100<br>successful |           | 1        | 0         | 00:00:21 |

# Lab Exercise 7-1: Using Dialer Profiles to Enhance DDR

Complete the lab exercise to practice what you learned in the related module.

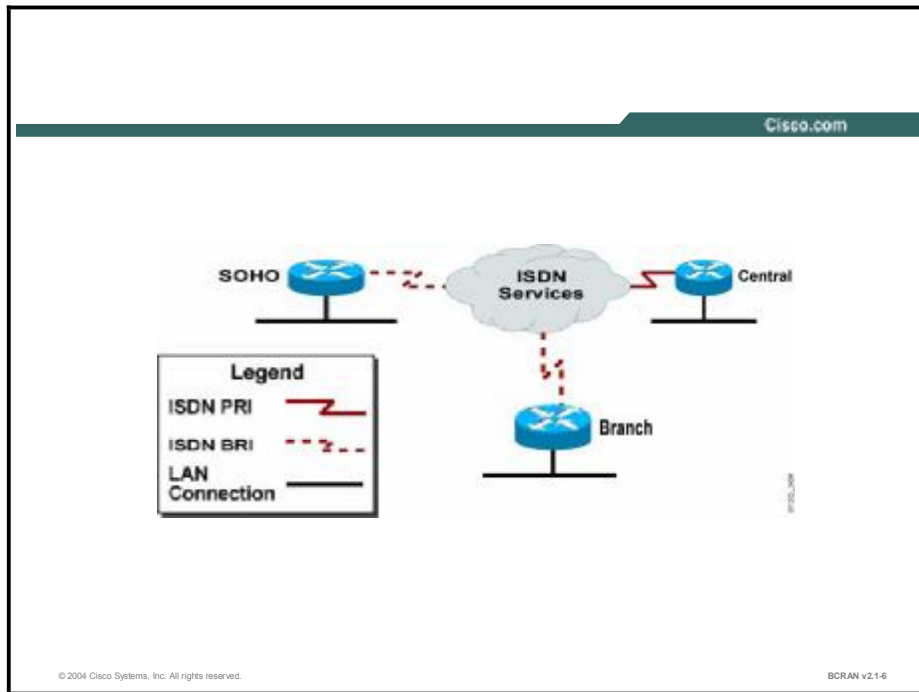
## Exercise Objective

Upon completing this lab, you will be able to:

- Configure a dialer interface on the central site and remote routers
- Demonstrate that using dialer interfaces allows BRI interfaces to use both B channels independently

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



## Command List

The commands used in this exercise are described in the table here.

### Configuration Commands

| Command                                                                                                                                            | Description                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>dialer-group</b> <i>group-number</i>                                                                                                            | Assigns a dialer group to an interface                                      |
| <b>dialer-list</b> <i>dialer-group protocol-name</i> { <b>permit</b>   <b>deny</b>   <b>list</b> <i>access-list-number</i>   <i>access-group</i> } | Specifies interesting traffic and associates it to a dialer group           |
| <b>dialer pool</b> <i>number</i>                                                                                                                   | Specifies that you use the interfaces in this pool to reach the destination |
| <b>dialer pool-member</b> <i>number</i>                                                                                                            | Assigns an interface to a dialer pool                                       |
| <b>dialer remote-name</b> <i>remote router name</i>                                                                                                | Specifies the name of the remote router                                     |
| <b>dialer string</b> <i>phone-number</i>                                                                                                           | Specifies the phone number used to reach the remote router                  |
| <b>encapsulation</b> <b>ppp</b>                                                                                                                    | Enables PPP protocol on the interface                                       |
| <b>interface dialer</b> <i>number</i>                                                                                                              | Creates a dialer interface                                                  |
| <b>ip route</b> <i>network network-mask next-hop</i>                                                                                               | Configures a static or default route                                        |
| <b>ppp authentication chap</b>                                                                                                                     | Sets CHAP as the PPP authentication method                                  |
| <b>username</b> <i>hostname password password</i>                                                                                                  | Specifies a username and password for authentication                        |

## Scenario

Given a central site with an ISDN PRI interface, configure it to receive BRI calls over dialer interfaces. Test and verify operation of the BRI calls.

# Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number ____ | Information Required             | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod ____ |
|-----------------|----------------------------------|--------------------------------------------------------------------|--------------------------------------------|
| Central router  | Your (first) LAN interface type  | Ethernet 0/0                                                       |                                            |
| Central router  | Your (first) LAN interface IP    | 10.X.0.1                                                           |                                            |
| Central router  | Your (first) ISDN controller     | T1 1/0                                                             |                                            |
| Central router  | ISDN switch type                 | primary-5ess                                                       |                                            |
| Central router  | ISDN number                      | 555X100                                                            |                                            |
| Central router  | Dialer 1 IP to branch            | 10.X.200.1                                                         |                                            |
| Central router  | Dialer 2 IP to SOHO              | 10.X.210.1                                                         |                                            |
| Branch router   | Your (first) LAN interface type  | FastEthernet0<br>Ethernet0                                         |                                            |
| Branch router   | Your (first) LAN interface IP    | 10.X.10.2                                                          |                                            |
| Branch router   | Your (first) ISDN interface type | Bri0                                                               |                                            |
| Branch router   | ISDN switch type                 | basic-5ess                                                         |                                            |
| Branch router   | ISDN number                      | 555X200                                                            |                                            |
| Branch router   | Dialer 1 IP to central           | 10.X.200.2                                                         |                                            |
| Branch router   | Dialer 3 IP to SOHO              | 10.X.220.2                                                         |                                            |
| SOHO router     | Your (first) LAN interface type  | Ethernet 0                                                         |                                            |
| SOHO router     | Your (first) LAN interface IP    | 10.X.0.3                                                           |                                            |
| SOHO router     | Your (first) ISDN interface type | Bri0                                                               |                                            |
| SOHO router     | ISDN number                      | 555X300                                                            |                                            |
| SOHO router     | Dialer 2 IP to central           | 10.X.210.3                                                         |                                            |
| SOHO router     | Dialer 3 IP to branch            | 10.X.220.3                                                         |                                            |



## Setup Tasks

From your PC, establish a Telnet session to the terminal server and open a console connection to the central router of your pod.

From your PC, establish a Telnet session to the terminal server again and open a second console connection to the branch router of your pod.

From your PC, establish a Telnet session to the terminal server again and open a third console connection to the SOHO router of your pod.

You will now be able to configure and observe output on all routers simultaneously.

TFTP the appropriate preconfiguration files to the central, branch, and SOHO routers and reload them.

## Task 1: Configuring the Central Site PRI to Use Dialer Profiles

Use the following steps to configure the central site PRI to use dialer profiles.

### Exercise Procedure

Complete these steps:

- Step 1** On the central router, configure the ISDN switch type that is listed in the setup table.
- Step 2** On the central router, create a dialer 1 interface. This dialer profile will connect the central router to the branch router.
- Step 3** For the dialer 1 interface, create a description to assist in identifying the destination router for the interface.
- Step 4** For the dialer 1 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 5** For the dialer 1 interface, assign dialer-list 1 to the dialer interface.
- Step 6** For the dialer 1 interface, configure PPP encapsulation and CHAP authentication.
- Step 7** For the dialer 1 interface, configure the remote router name.
- Step 8** For the dialer 1 interface, configure it to belong to dialer pool 1.
- Step 9** For the dialer 1 interface, configure the dial string for the branch router. Use the dial string that is listed in the setup table.
- Step 10** On the central router, create a dialer 2 interface. This dialer profile will connect the central router to the SOHO router.
- Step 11** For the dialer 2 interface, create a description to assist in identifying the destination router for the interface.
- Step 12** For the dialer 2 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 13** For the dialer 2 interface, assign dialer-list 1 to the dialer interface.
- Step 14** For the dialer 2 interface, configure PPP encapsulation and CHAP authentication.

- Step 15** For the dialer 2 interface, configure the remote router name.
- Step 16** For the dialer 2 interface, configure it to belong to dialer pool 2.
- Step 17** For the dialer 2 interface, configure the dial string for the SOHO router. Use the dial string that is listed in the setup table.
- Step 18** Link the serial 1/0:23 interface of the central router to dialer pool 1 and 2.
- Step 19** You will also need to configure PPP encapsulation and CHAP authentication on the ISDN interface.
- Step 20** Create usernames and passwords for the CHAP authentication on your dialer profiles.
- Step 21** Create the dialer list for your dialer profiles that will forward all IP traffic.
- Step 22** Configure static routes to the stub networks at the branch and SOHO sites.
- Step 23** Verify and save the router configuration.
- Step 24** Proceed to Task 2.

## Task 2: Configuring the Branch BRI Interface to Use Dialer Profiles

Use the following steps to configure the branch BRI interface to use dialer profiles.

### Exercise Procedure

Complete these steps:

- Step 1** On the branch router, configure the ISDN switch type that is listed in the setup table.
- Step 2** On the branch, create a dialer 1 interface. This dialer profile will connect the branch to the central router.
- Step 3** For the dialer 1 interface, create a description to assist in identifying the destination router for the interface.
- Step 4** For the dialer 1 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 5** For the dialer 1 interface, assign dialer-list 1 to the dialer interface.
- Step 6** For the dialer 1 interface, configure PPP encapsulation and CHAP authentication. As before, you are authenticating locally only, so disregard the AAA default list warning message.
- Step 7** For the dialer 1 interface, configure the remote router name.
- Step 8** For the dialer 1 interface, configure it to belong to dialer pool 1.
- Step 9** For the dialer 1 interface, configure the dial string for the central router. Use the dial string that is listed in the setup table.
- Step 10** On the branch router, create a dialer 3 interface. This dialer profile will connect to branch router to the SOHO router.

- Step 11** For the dialer 3 interface, create a description to assist in identifying the destination router for the interface.
- Step 12** For the dialer 3 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 13** For the dialer 3 interface, assign dialer-list 1 to the dialer interface.
- Step 14** For the dialer 3 interface, configure PPP encapsulation and CHAP authentication. As before, you are authenticating locally only, so disregard the AAA default list warning message.
- Step 15** For the dialer 3 interface, configure the remote router name.
- Step 16** For the dialer 3 interface, configure it to belong to dialer pool 3.
- Step 17** For the dialer 3 interface, configure the dial string for the SOHO router. Use the dial string that is listed in the setup table.
- Step 18** Link the branch router BRI 0 interface to Dialer pool 1 and 3.
- Step 19** You will also need to configure PPP encapsulation and CHAP authentication on the ISDN interface.
- Step 20** Create usernames and passwords for the CHAP authentication on your dialer profiles.
- Step 21** Create the dialer list for your dialer profiles that will forward all IP traffic.
- Step 22** Configure the static default route to the central site and a static route for the stub SOHO network.
- Step 23** Verify and save the router configuration.
- Step 24** Proceed to Task 3.

## Task 3: Configuring the SOHO BRI Interface to Use Dialer Profiles

Use the following steps to configure the SOHO BRI interface to use dialer profiles.

### Exercise Procedure

Complete these steps:

- Step 1** On the SOHO router, configure the ISDN switch type that is listed in the setup table.
- Step 2** On the SOHO router, create a dialer 2 interface. This dialer profile will connect the SOHO to the central router.
- Step 3** For the dialer 2 interface, create a description to assist in identifying the destination router for the interface.
- Step 4** For the dialer 2 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 5** For the dialer 2 interface, assign dialer-list 1 to the dialer interface.

- Step 6** For the dialer 2 interface, configure PPP encapsulation and CHAP authentication. As before, you are authenticating locally only, so disregard the AAA default list warning message.
- Step 7** For the dialer 2 interface, configure the remote router name.
- Step 8** For the dialer 2 interface, configure it to belong to dialer pool 2.
- Step 9** For the dialer 2 interface, configure the dial string for the central router. Use the dial string that is listed in the setup table.
- Step 10** On the SOHO router, create a dialer 3 interface. This dialer profile will connect the SOHO router to the branch router.
- Step 11** For the dialer 3 interface, create a description to assist in identifying the destination router for the interface.
- Step 12** For the dialer 3 interface, assign an IP address and subnet mask. Use the IP address and subnet mask identified in the setup table.
- Step 13** For the dialer 3 interface, assign dialer-list 1 to the dialer interface.
- Step 14** For the dialer 3 interface, configure PPP encapsulation and CHAP authentication.
- Step 15** For the dialer 3 interface, configure the remote router name.
- Step 16** For the dialer 3 interface, configure it to belong to dialer pool 3.
- Step 17** For the dialer 3 interface, configure the dial string for the branch router. Use the dial string that is listed in the setup table.
- Step 18** Link the Bri0 interface of the branch router to dialer pool 2 and 3.
- Step 19** You will also need to configure PPP encapsulation and CHAP authentication on the ISDN interface.
- Step 20** Create usernames and passwords for the CHAP authentication on your dialer profiles.
- Step 21** Create the dialer list for your dialer profiles that will forward all IP traffic.
- Step 22** Configure the static default route to the central site and a static route for the branch stub network.
- Step 23** Verify and save the router configuration.
- Step 24** Proceed to Task 4.

## Task 4: Testing the Dialer Profiles

Use the following steps to test the dialer profiles you have configured.

### Exercise Procedure

Complete these steps:

- Step 1** From the branch router, use the **ping** command to verify connectivity between the LAN interfaces of the branch router and the central router.
- Step 2** From the branch router, use the **ping** command to verify connectivity between the LAN interfaces of the branch router and the SOHO router.
- Step 3** From the SOHO router, use the **ping** command to verify connectivity between the LAN interfaces of the SOHO router and the central router.
- Step 4** From the central router, enter the **show dialer** command and examine the output. If the previous steps were executed less than two minutes before, the output should be similar to the following:

< Output Omitted >

```
Serial1/0:18 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
```

#### Dialer state is data link layer up

```
Interface bound to profile Di2
Time until disconnect 93 secs
Connected to 555X300 (SOHO)
```

```
Serial1/0:19 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
```

#### Dialer state is data link layer up

```
Interface bound to profile Di1
Time until disconnect 104 secs
Connected to 555X200 (Branch)
```

< Output Omitted >

```
Serial1/0:23 - dialer type = ISDN
```

| Dial String | Successes | Failures | Last DNIS | Last |
|-------------|-----------|----------|-----------|------|
| status      |           |          |           |      |

```
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.
```

### Di1 - dialer type = DIALER PROFILE

```
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Number of active calls = 1
```

| Dial String<br>status | Successes    | Failures | Last DNIS | Last |
|-----------------------|--------------|----------|-----------|------|
| 555X200<br>successful | 2<br>Default | 0        | 00:14:55  |      |

### Di2 - dialer type = DIALER PROFILE

```
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Number of active calls = 1
```

| Dial String<br>status | Successes    | Failures | Last DNIS | Last |
|-----------------------|--------------|----------|-----------|------|
| 555X300<br>successful | 2<br>Default | 0        | 00:14:49  |      |

## Exercise Verification

You have completed this exercise when you attain these results:

- You are able to successfully ping between the branch, central, and SOHO sites.

On the central router, verify that your configuration contains lines similar to the following:

```
username soho_X password 0 cisco ! Task 1 Step 20
username branch_X password 0 cisco ! Task 1 Step 20

isdn switch-type primary-ni ! Task 1 Step 1

interface Serial1/0:23
 encapsulation ppp ! Task 1 Step 19
 dialer pool-member 1 ! Task 1 Step 18
 dialer pool-member 2 ! Task 1 Step 18
 ppp authentication chap ! Task 1 Step 19
```

```

interface dialer 1 ! Task 1 Step 2
 description This dialer goes from Central to Branch ! Task 1 Step
3
 ip address 10.X.200.1 255.255.255.0 ! Task 1 Step 4
 dialer-group 1 ! Task 1 Step 5
 encapsulation ppp ! Task 1 Step 6
 ppp authentication chap ! Task 1 Step 6
 dialer remote-name branch_X ! Task 1 Step 7
 dialer string 555X200 ! Task 1 Step 9
 dialer pool 1 ! Task 1 Step 8

interface dialer 2 ! Task 1 Step 10
 description This dialer goes from Central to SOHO ! Task 1 Step
11
 ip address 10.X.210.1 255.255.255.0 ! Task 1 Step 12
 dialer-group 1 ! Task 1 Step 13
 encapsulation ppp ! Task 1 Step 14
 ppp authentication chap ! Task 1 Step 14
 dialer remote-name soho_X ! Task 1 Step 15
 dialer string 555X300 ! Task 1 Step 17
 dialer pool 2 ! Task 1 Step 16

ip route 10.X.10.0 255.255.255.0 10.X.200.2 ! Task 1 Step 22
ip route 10.X.100.0 255.255.255.0 10.X.210.3 ! Task 1 Step 22

dialer-list 1 protocol ip permit ! Task 1 Step 21

```

On the branch router, verify that your configuration contains lines similar to the following:

```

username soho_X password 0 cisco ! Task 2 Step 20
username central_X password 0 cisco ! Task 2 Step 20

isdn switch-type basic-net3 ! Task 2 Step 1

interface BRI0
 encapsulation ppp ! Task 2 Step 19
 dialer pool-member 1 ! Task 2 Step 18
 dialer pool-member 3 ! Task 2 Step 18

```

```

ppp authentication chap ! Task 2 Step 19

interface dialer 1 ! Task 2 Step 2
 description This dialer goes from Branch to Central ! Task 2 Step
 3
 ip address 10.X.200.2 255.255.255.0 ! Task 2 Step 4
 dialer-group 1 ! Task 2 Step 5
 encapsulation ppp ! Task 2 Step 6
 ppp authentication chap ! Task 2 Step 6
 dialer remote-name central_X ! Task 2 Step 7
 dialer string 555X100 ! Task 2 Step 9
 dialer pool 1 ! Task 2 Step 8

interface dialer 3 ! Task 2 Step 10
 description This dialer goes from Branch to SOHO! Task 2 Step 11
 ip address 10.X.220.2 255.255.255.0 ! Task 2 Step 12
 dialer-group 1 ! Task 2 Step 13
 encapsulation ppp ! Task 2 Step 14
 ppp authentication chap ! Task 2 Step 14
 dialer remote-name soho_X ! Task 2 Step 15
 dialer string 555X300 ! Task 2 Step 17
 dialer pool 3 ! Task 2 Step 16

ip route 0.0.0.0 0.0.0.0 10.X.200.1 ! Task 2 Step 22
ip route 10.X.100.0 255.255.255.0 10.X.220.3 ! Task 2 Step 22

dialer-list 1 protocol ip permit ! Task 2 Step 21

```

On the SOHO router, verify that your configuration contains lines similar to the following:

```

username branch_X password 0 cisco ! Task 3 Step 20
username central_X password 0 cisco ! Task 3 Step 20

isdn switch-type basic-ni ! Task 3 Step 1

interface BRI0
 encapsulation ppp ! Task 3 Step 19
 dialer pool-member 2 ! Task 3 Step 18
 dialer pool-member 3 ! Task 3 Step 18
 ppp authentication chap ! Task 3 Step 19

```



```

interface dialer 2 ! Task 3 Step 2
 description This dialer goes from SOHO to Central ! Task 3 Step
3
 ip address 10.X.210.3 255.255.255.0 ! Task 3 Step 4
 dialer-group 1 ! Task 3 Step 5
 encapsulation ppp ! Task 3 Step 6
 ppp authentication chap ! Task 3 Step 6
 dialer remote-name central_X ! Task 3 Step 7
 dialer string 555X100 ! Task 3 Step 9
 dialer pool 2 ! Task 3 Step 8

interface dialer 3 ! Task 3 Step 10
 description This dialer goes from SOHO to Branch! Task 3 Step 11
 ip address 10.X.220.3 255.255.255.0 ! Task 3 Step 12
 dialer-group 1 ! Task 3 Step 13
 encapsulation ppp ! Task 3 Step 14
 ppp authentication chap ! Task 3 Step 14
 dialer remote-name branch_X ! Task 3 Step 15
 dialer string 555X200 ! Task 3 Step 17
 dialer pool 3 ! Task 3 Step 16

dialer-list 1 protocol ip permit ! Task 3 Step 21

ip route 0.0.0.0 0.0.0.0 10.X.210.1 ! Task 3 Step 22
ip route 10.X.10.0 255.255.255.0 10.X.220.2 ! Task 3 Step 22

```

# Lab Exercise Answer Key

## Lab Exercise 7-1: Using Dialer Profiles to Enhance DDR

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 $1$1g/L$1InA9RZbNpwk1BPWuPl/K1
!
username central_3 password 0 cisco
username soho_3 password 0 cisco
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
isdn switch-type basic-5ess
!
!
!
!
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
dialer pool-member 3
isdn switch-type basic-5ess
no cdp enable
```

```

 ppp authentication chap
 !
interface FastEthernet0
 description This is the Ethernet network for the Branch router
 ip address 10.3.10.2 255.255.255.0
 speed auto
 no cdp enable
 !
interface Serial0
 no ip address
 shutdown
 no cdp enable
 !
interface Serial1
 no ip address
 shutdown
 no cdp enable
 !
interface Dialer1
 description This dialer goes from Branch to Central
 ip address 10.3.200.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer remote-name central_3
 dialer string 5553100
 dialer-group 1
 no cdp enable
 ppp authentication chap
 !
interface Dialer3
 description This dialer goes from Branch to SOHO
 ip address 10.3.220.2 255.255.255.0
 encapsulation ppp
 dialer pool 3
 dialer remote-name soho_3
 dialer string 5553300
 dialer-group 1
 no cdp enable
 ppp authentication chap
 !

```

```

ip classless
ip route 0.0.0.0 0.0.0.0 10.3.200.1
ip route 10.3.100.0 255.255.255.0 10.3.220.3
no ip http server
 ip pim bidir-enable
 !
 !
 dialer-list 1 protocol ip permit
no cdp run
 !
 banner motd ^
 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
 branch branch branch branch branch branch branch branch

 -
 Notes from the instructor:
 All local passwords should be set to "cisco"

 -
 branch branch branch branch branch branch branch branch
 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
 ^
 !
 line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
 line aux 0
 line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
 !
end

```

## Central Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1vPs9$vbj73XnJ1OmaqdvIyCTri/
!
username soho_3 password 0 cisco
username branch_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
!
isdn switch-type primary-5ess
call rsvp-sync
!
!
!
!
!
!
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
!
!
!
interface Ethernet0/0
description This is the Ethernet network for the Central router
ip address 10.3.0.1 255.255.255.0
half-duplex
no cdp enable
!
interface Ethernet0/1
```

```

no ip address
shutdown
half-duplex
no cdp enable
!
interface Serial1/0:23
no ip address
encapsulation ppp
dialer pool-member 1
dialer pool-member 2
isdn switch-type primary-5ess
no cdp enable
ppp authentication chap
!
interface Serial3/0
no ip address
shutdown
no cdp enable
!
interface Serial3/1
no ip address
shutdown
no cdp enable
!
interface Serial3/2
no ip address
shutdown
no cdp enable
!
interface Serial3/3
no ip address
shutdown
no cdp enable
!
interface Dialer1
description This dialer goes from Central to Branch
ip address 10.3.200.1 255.255.255.0
encapsulation ppp
dialer pool 1
dialer remote-name branch_3

```

```

dialer string 5553200
dialer-group 1
no cdp enable
ppp authentication chap
!
interface Dialer2
description This dialer goes from Central to SOHO
ip address 10.3.210.1 255.255.255.0
encapsulation ppp
dialer pool 2
dialer remote-name soho_3
dialer string 5553300
dialer-group 1
no cdp enable
ppp authentication chap
!
ip classless
ip route 10.3.10.0 255.255.255.0 10.3.200.2
ip route 10.3.100.0 255.255.255.0 10.3.210.3
no ip http server
!
dialer-list 1 protocol ip permit
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
central central central central central central central central

Notes from the instructor:
All local passwords should be set to "cisco"

central central central central central central central central
Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
^

```

```

!
line con 0
 exec-timeout 30 0
 logging synchronous level all
history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end

```

### SOHO Router End Configuration

```

version 12.2

 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
!
hostname soho_3
!
enable secret 5 1aNN7$a0cNnou/3pPLS5d5ZRy8b1
!
username central_3 password 0 cisco
username branch_3 password 0 cisco
ip subnet-zero
no ip domain-lookup
!
isdn switch-type basic-5ess
!
!
!
!
interface Ethernet0
 description This is the Ethernet network for the soho router

```



```

 ip address 10.3.100.3 255.255.255.0
 no cdp enable
!
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 2
 dialer pool-member 3
 isdn switch-type basic-5ess
 no cdp enable
 ppp authentication chap
!
interface Dialer2
 description This dialer goes from SOHO to Central
 ip address 10.3.210.3 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer remote-name central_3
 dialer string 5553100
 dialer-group 1
 no cdp enable
 ppp authentication chap
!
interface Dialer3
 description This dialer goes from SOHO to Branch
 ip address 10.3.220.3 255.255.255.0
 encapsulation ppp
 dialer pool 3
 dialer remote-name branch_3
 dialer string 5553200
 dialer-group 1
 no cdp enable
 ppp authentication chap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.210.1
ip route 10.3.10.0 255.255.255.0 10.3.220.2
no ip http server
!
dialer-list 1 protocol ip permit

```

```
no cdp run
banner motd ^
Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
soho soho soho soho soho soho soho soho soho soho soho soho

Notes from the instructor:
All local passwords should be set to "cisco"

soho soho soho soho soho soho soho soho soho soho soho soho
Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7 Lab7
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end
```

# Lab Exercise 8-1: Establishing a Dedicated Frame Relay Connection and Controlling Traffic Flow

Complete this lab exercise to practice what you learned in the related module.

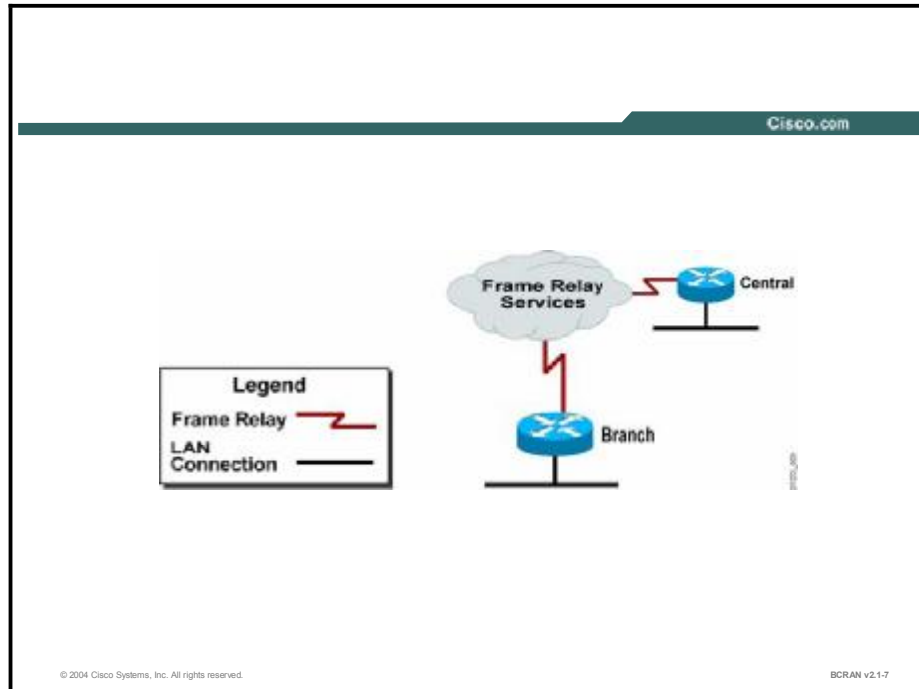
## Exercise Objective

Upon completing this lab, you will be able to:

- Configure a Frame Relay interface and subinterface
- Configure FRTS
- Verify Frame Relay operation

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



## Command List

The commands used in this exercise are described in the table here.

### Configuration Commands

| Command                                                                          | Description                                                                                                                   |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>encapsulation frame-relay</b>                                                 | Enables Frame Relay encapsulation                                                                                             |
| <b>frame-relay adaptive-shaping becn</b>                                         | The <b>map class</b> subcommand used to specify that traffic should be throttled based on BECN messages                       |
| <b>frame-relay class map-class-name</b>                                          | Associates a map class with an interface or subinterface                                                                      |
| <b>frame-relay cir traffic-rate</b>                                              | Changes the default Frame Relay traffic rate of 56 kbps                                                                       |
| <b>frame-relay interface-dlci dlci-number</b>                                    | Assigns a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server       |
| <b>frame-relay traffic-rate cir eir (peak rate)</b>                              | Specifies the traffic rates to be enforced by Frame Relay traffic shaping (FRTS)                                              |
| <b>frame-relay traffic-shaping</b>                                               | Enables Frame Relay traffic shaping on virtual circuits (VCs) on an interface                                                 |
| <b>interface serial number.subinterface-number {multipoint   point-to-point}</b> | Enters subinterface configuration mode. Multipoint or point-to-point must be specified                                        |
| <b>load-interval</b>                                                             | Changes the default time period for load calculations on an interface                                                         |
| <b>map-class frame-relay map-class-name</b>                                      | Specifies a map class to define a quality of service such as Frame Relay traffic shaping for a switched virtual circuit (SVC) |
| <b>show frame-relay map</b>                                                      | Displays the current Frame Relay map entries and information about the connections                                            |
| <b>show frame-relay pvc</b>                                                      | Displays the status and statistics for a Frame Relay permanent virtual circuit (PVC) on a per-interface and DLCI basis        |
| <b>show traffic-shape statistics</b>                                             | Displays which subinterfaces are active for traffic shaping and how much traffic has been shaped                              |

## Scenario

Given a central site with a Frame Relay network connection to its branch office, configure Frame Relay on the central site and branch office routers. Also, configure subinterfaces on the central site router to accommodate one VC connection to the branch using the Frame Relay network. Often, the physical lines at the central site are larger and may accommodate more bandwidth than at the branch office. For this reason, enable FRTS to control traffic flow from the central site.

## Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number ____         | Information Required                   | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod ____ |
|-------------------------|----------------------------------------|--------------------------------------------------------------------|--------------------------------------------|
| Central router          | Your (first) LAN interface type        | Ethernet 0/0                                                       |                                            |
| Central router          | Your (first) LAN interface IP          | 10.X.0.1                                                           |                                            |
| Central router          | Your (second) WAN interface type       | Serial 0/1<br>Serial 3/1                                           |                                            |
| Central router          | Your (second) WAN interface IP address | 10.X.150.1                                                         |                                            |
| Central router          | Frame Relay DLCI                       | X12                                                                |                                            |
| Cisco Secure AAA server | IP address                             | 10.X.0.200                                                         |                                            |
| Branch router           | Your (first) LAN interface type        | FastEthernet0<br>Ethernet0                                         |                                            |
| Branch router           | Your (first) LAN interface IP          | 10.X.10.2                                                          |                                            |
| Branch router           | Your (second) WAN interface type       | Serial 1                                                           |                                            |
| Branch router           | Your (second) WAN interface IP address | 10.X.150.2                                                         |                                            |
| Branch router           | Frame Relay DLCI                       | X21                                                                |                                            |

### Setup Tasks

From your PC, establish a Telnet session to the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet session to the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

TFTP the appropriate preconfiguration files to the central and branch routers and reload the routers.

# Task 1: Configuring Frame Relay Subinterfaces on the Central Site Router

Assume that the central site needs to connect to multiple branch offices, but the central site has only a single link to your ISP. You have determined that Frame Relay is the option that best suits the organizational needs, but that it is not cost-effective to have a separate link into the ISP cloud for each branch office. You must configure your single link to support multiple VC connections to the other branch offices. In this section, you will configure a point-to-point subinterface to connect to one of the branch office routers.

## Exercise Procedure

Complete these steps:

**Step 1** On the central site router, using the command list, enable the second WAN interface of your central site router for Frame Relay.

**Step 2** Change the default load calculation interval from five minutes to 30 seconds.

---

**Note** IP addresses are configured on the subinterfaces; no IP address is specified on the physical interface.

---

**Step 3** Using the command list, on the central site router, create a subinterface with a “0.1” for point-to-point operation and with a description “This interface goes to the branch office.”

**Step 4** Configure the subinterface with the Frame Relay IP address that is listed in the setup table.

**Step 5** Using the command list, configure the Frame Relay subinterface with a bandwidth of 9 kbps.

---

**Note** This setting is only used for the routing protocol to correctly calculate the metric to the branch site. The default metric for serial interfaces on Cisco routers is 1.544 Mbps.

---

**Step 6** Using the command list, assign the Frame Relay subinterface with the Frame Relay DLCI going to the branch router.

**Step 7** Save your configuration on the central site router.

**Step 8** Verify that the status of the main Frame Relay serial interface and the line protocol, Frame Relay, are both up. Output should be similar to the following:

```
Serial3/1 is up, line protocol is up
 Hardware is CD2430 in sync mode
 MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation FRAME-RELAY, loopback not set
 Keepalive set (10 sec)
 LMI enq sent 22, LMI stat recvd 23, LMI upd recvd 0, DTE
```

```

LMI up
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
<output omitted>

```

**Step 9** What is the current status of the Frame Relay PVC and why? \_\_\_\_\_

The output on your central site router should be similar to the following:

**PVC Statistics for interface SerialX/1 (Frame Relay DTE)**

|          | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local    | 0      | 1        | 0       | 0      |
| Switched | 0      | 0        | 0       | 0      |
| Unused   | 0      | 0        | 0       | 0      |

```

DLCI = XXX, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE,
INTERFACE = SerialX/1.1

```

```

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN
pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN
pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
 pvc create time 00:04:27,
last time pvc status changed

```

---

**Caution** If the PVC status is deleted, do not proceed with this lab. This means the Frame Relay switch does not know about the DLCI number that you entered on the router.

---

**Step 10** Proceed to Task 2.

## Task 2: Configuring a Frame Relay Subinterface on the Branch Office Router

In this section you will configure a point-to-point subinterface on the branch router to connect to the central office router.

### Exercise Procedure

Complete these steps:

- Step 1** On the branch office router, using the command list, enable the second WAN interface of your branch site router for Frame Relay.
- Step 2** Change the default load calculation interval from five minutes to 30 seconds.
- Step 3** Using the command list, on the branch router, create a subinterface “0.1” for point-to-point operation and with a description “This interface goes to central office.”
- Step 4** Configure the serial “0.1” subinterface with the Frame Relay IP address that is listed in the setup table.
- Step 5** Using the command list, configure the serial 1.1 subinterface with a bandwidth of 9 kbps.
- Step 6** Using the command list, assign the serial “0.1” subinterface with the Frame Relay DLCI going to the central router.
- Step 7** Save your configuration at the branch router.
- Step 8** Verify that the status of the main Frame Relay serial interface and the line protocol, Frame Relay, are both up. Output should be similar to the following:

```
Serial1 is up, line protocol is up
 Hardware is PowerQUICC Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation FRAME-RELAY, loopback not set
 Keepalive set (10 sec)
 LMI enq sent 25, LMI stat recvd 26, LMI upd recvd 0, DTE
LMI up
 LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
 LMI DLCI 1023 LMI type is CISCO frame relay DTE
show frame-relay pvc
```



**Step 9** What is the current status of the Frame Relay PVC and why? \_\_\_\_\_

The output on your branch site router should be similar to the following:

**PVC Statistics for interface Serial0 (Frame Relay DTE)**

|          | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local    | 1      | 0        | 0       | 0      |
| Switched | 0      | 0        | 0       | 0      |
| Unused   | 0      | 0        | 0       | 0      |

DLCI = X21, DLCI USAGE = LOCAL, PVC STATUS = **ACTIVE**, INTERFACE = Serial1.1

```
input pkts 69 output pkts 57 in bytes
6065
out bytes 4203 dropped pkts 0 in FECN
pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN
pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 53 out bcast bytes 3971
pvc create time 00:04:43, last time pvc status changed
00:04:33
```

**Step 10** Proceed to Task 3.

## Task 3: Verifying Frame Relay Operation

Use the following steps to verify for proper Frame Relay operation.

### Exercise Procedure

Complete these steps:

- Step 1** At both router, use the **show ip route** command to verify an EIGRP route to the LAN network of the remote site.
- Step 2** View the dynamically generated route maps that your router can use to route traffic with the **show frame-relay map** command. Verify that the map to the branch office routers LAN interface network is in the map table.
- Step 3** To verify connectivity with your peer, ping to the LAN interface of the remote router.
- Step 4** Proceed to Task 4.

## Task 4: Enabling Adaptive Traffic Shaping Using BECN

Use the following steps to enable adaptive traffic shaping by using BECN.

### Exercise Procedure

Complete these steps:

- Step 1** On the central site router, using the command list, create a Frame Relay map named TSLAB.
- Step 2** Using the command list, define backward explicit congestion notification (BECN) support as the traffic-shaping method for the TSLAB map class.
- Step 3** Using the command list, enable traffic shaping on the main Frame Relay serial interface of the central router.
- Step 4** Using the command list, configure the main Frame Relay serial interface of the central router to use the Frame Relay map TSLAB.
- Step 5** Verify that traffic shaping is enabled and adapts to BECN by showing the PVC status information. Your output should be similar to the following:

PVC Statistics for interface SerialX/1 (Frame Relay DTE)

|          | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local    | 1      | 0        | 0       | 0      |
| Switched | 0      | 0        | 0       | 0      |
| Unused   | 0      | 0        | 0       | 0      |

DLCI = XXX, DLCI USAGE = LOCAL, PVC STATUS = **ACTIVE**, INTERFACE = SerialX/1.1

```
input pkts 352 output pkts 365 in bytes
28008
out bytes 30060 dropped pkts 0 in FECN
pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN
pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 356 out bcast bytes 29252
```

**Shaping adapts to BECN**

```
pvc create time 00:30:54, last time pvc status changed
00:25:14
```

**Step 6** Use the **show frame-relay pvc *DLCI*** command to again verify that traffic shaping is enabled, and that it adapts to BECN. Notice that the Frame Relay interface defaults to a committed information rate (CIR) of 56 kbps. Your output should look similar to the following:

```
PVC Statistics for interface SerialX/1 (Frame Relay DTE)
```

```
DLCI = XXX, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE
= SerialX/1.1
```

```
input pkts 172 output pkts 185 in bytes
13563
out bytes 15537 dropped pkts 0 in FECN
pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN
pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 176 out bcast bytes 14729
```

```
Shaping adapts to BECN
```

```
pvc create time 00:18:04, last time pvc status changed
00:12:24
```

```
cir 56000 bc 7000 be 0 limit 875
interval 125
```

```
mincir 28000 byte increment 875 Adaptive Shaping BECN
pkts 57 bytes 4572 pkts delayed 0 bytes
delayed 0
```

```
shaping inactive
```

```
traffic shaping drops 0
```

```
SerialX/1.1 dlci XXX is first come first serve default
queuing
```

```
Output queue 0/40, 0 drop, 0 dequeued
```

---

**Note** The **frame-relay class** command has been applied to the main interface. This causes each subinterface to inherit the properties of the main interface. The default CIR for traffic shaping is 56 kbps. This can cause serious disruption of services to a high-speed serial interface because each subinterface will be limited to 56 kbps of outbound traffic.

---

**Step 7** Proceed to Task 5.

## Task 5: Modifying Frame Relay Traffic Shaping

In the previous task, you enabled adaptive traffic shaping for all flows from the central site. You will now enable per-DLCI traffic shaping which can be applied to individual sub-interfaces. You will first have to demonstrate that traffic peaks at speeds higher than 9600 bps between the central site and the branch site. To implement FRTS, you will lower the CIR at the central-site router, forcing the router to shape the traffic to avoid bursting beyond the Internet service provider (ISP) guaranteed rates and dropping frames.

### Exercise Procedure

Complete these steps:

- Step 1** Verify that the load at the Frame Relay interface of the branch site router is calculated every 30 seconds with the **show interface** command. Output should be similar to the following:

```
Serial0 is up, line protocol is up
```

```
< Output omitted >
```

```
30 second input rate 0 bits/sec, 0 packets/sec
```

```
30 second output rate 0 bits/sec, 0 packets/sec
```

```
< Output omitted >
```

As the interface forwards or receives data, the traffic rate will be displayed.

- Step 2** To test the traffic rate between sites, use the extended **ping** command from the central router. Ping the Ethernet interface of the branch router 100 times with 1500-byte datagrams.

---

**Note** This will cause the central router to send large amounts of Internet Control Message Protocol (ICMP) traffic to the branch site.

---

- Step 3** While traffic is being generated from the central router, switch back to the branch router and verify that the serial interface is receiving traffic above 9600 bps with the **show interface** command. You may need to repeat this command several times. Output should be similar to the following:

```
< Output omitted >
```

```
30 second input rate 13000 bits/sec, 2 packets/sec
```

```
30 second output rate 13000 bits/sec, 2 packets/sec
```

```
< Output omitted >
```

Now that you have verified that the traffic rate is not limited to 9600 bps, you are now ready to enable traffic shaping on the central site.

**Step 4** At the central site router, modify the map class TSLAB by changing the committed information rate from the default of 56,000 bps to 9600 bps.

**Step 5** Now define the FRTS CIR and peak rates that will be used to enforce traffic shaping. For the purposes of this lab, the CIR and the peak rate will be the same. You will shape the traffic flows from the central site to 9600 bps.

---

**Note** The throttling back of traffic is now based on the Frame Relay traffic-rate command.

---

**Step 6** Execute an extended ping to the LAN interface of the branch router 100 times with 1500-byte datagrams.

**Step 7** While traffic is still being sent from the central router, switch back to the branch router. Use the **show interface** command repeatedly and verify that traffic is flowing at a rate no higher than 9600 bps. Output should be similar to the following:

```
< Output omitted >
```

```
30 second input rate 9000 bits/sec, 2 packets/sec
30 second output rate 9000 bits/sec, 2 packets/sec
```

```
< Output omitted >
```

The input traffic rate should also not exceed 9000 bps.

**Step 8** On the central router, use the **show traffic-shape statistics** command to see if shaping is active and how many packets have been delayed per subinterface.

```
Access Queue Packets Bytes Packets Bytes
Shaping
I/F List Depth Delayed
Se X/1.1 0 4608 2101252 1331 1592164 no
```

**Step 9** Use the **show frame-relay pvc DLCI#** command to verify that traffic shaping is enabled but not active. Your output should look like similar to the following:

```
PVC Statistics for interface SerialX/1 (Frame Relay DTE)
```

```
DLCI = XXX, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE
= SerialX/1.1
```

```

 input pkts 355 output pkts 375 in bytes
 170746
 out bytes 173114 dropped pkts 0 in FECN
 pkts 0
 in BECN pkts 0 out FECN pkts 0 out BECN
 pkts 0
 in DE pkts 0 out DE pkts 0
 out bcast pkts 271 out bcast bytes 22426
 Shaping adapts to BECN
 pvc create time 00:24:08, last time pvc status changed
 00:19:18
 cir 9600 bc 9600 be 0 limit 150
 interval 125
 mincir 4800 byte increment 150 Adaptive Shaping BECN
 pkts 312 bytes 167433 pkts delayed 130 bytes
 delayed 151342
 shaping inactive
 traffic shaping drops 0
 SerialX/1.1 dlci XXX is first come first serve default
 queuing

Output queue 0/40, 0 drop, 130 dequeued

```

## Exercise Verification

You have completed this exercise when you attain these results:

- You successfully pinged the LAN interfaces of the central site router from the branch office router and vice versa, and enabled traffic shaping on the central site router to the lower speed branch office router.

On the central router, verify that your configuration contains added lines similar to the following:

```

interface SerialX/1
 encapsulation frame-relay ! Task 1 step 1
 load-interval 30 ! Task 1 step 2
 frame-relay class TSLAB ! Task 4 step 4
 frame-relay traffic-shaping ! Task 4 step 3

interface SerialX/1.1 point-to-point ! Task 1 step 3
 description This interface goes to branch office ! Task 1 step 3
 bandwidth 9 ! Task 1 step 5
 ip address 10.X.150.1 255.255.255.0 ! Task 1 step 4
 frame-relay interface-dlci X12 ! Task 1 step 6

```

```
map-class frame-relay TSLAB ! Task 4 step 1
frame-relay adaptive-shaping becn ! Task 4 step 2
frame-relay cir 9600 ! Task 5 step 4
frame-relay traffic-rate 9600 9600 ! Task 5 step 5
```

On the Branch router verify that your configuration contains lines similar to the following:

```
interface Serial1
 encapsulation frame-relay ! Task 2 step 1
 load-interval 30 ! Task 2 step 2

interface Serial1.1 point-to-point ! Task 2 step 3
 description This interface goes to central office! Task 2 step 3
 bandwidth 9 ! Task 2 step 5
 ip address 10.X.150.2 255.255.255.0 ! Task 2 step 4
 frame-relay interface-dlci X21 ! Task 2 step 6
```

# Lab Exercise Answer Key

## Lab Exercise 8-1: Establishing a Dedicated Frame Relay Connection and Controlling Traffic Flow

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1VNoh$D/VR81iICXdHBV1fzCxX..
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface BRI0
no ip address
shutdown
no cdp enable
!
interface FastEthernet0
description This is the Ethernet network for the Branch
router
ip address 10.3.10.2 255.255.255.0
```



```

 speed auto
 no cdp enable
 !
interface Serial0
 no ip address
 shutdown
 no cdp enable
 !
interface Serial1
 no ip address
 encapsulation frame-relay
 load-interval 30
 !
interface Serial1.1 point-to-point
 description This interface goes to central office
 bandwidth 9
 ip address 10.3.150.2 255.255.255.0
 no cdp enable
 frame-relay interface-dlci 321
 !
router eigrp 100
 passive-interface FastEthernet0
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-changes
 !
ip classless
no ip http server
ip pim bidir-enable
 !
 !
no cdp run
 !
banner motd ^
Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8
branch branch branch branch branch branch branch branch

```

-----

Notes from the instructor:

All local passwords should be set to "cisco"

-----



```

controller T1 1/0
 framing sf
 linecode ami
 !
 !
 !
 interface Ethernet0/0
 description This is the Ethernet network for the Central router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
 !
 interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
 !
 interface Serial3/0
 no ip address
 shutdown
 no cdp enable
 !
 interface Serial3/1
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 frame-relay class TSLAB
 frame-relay traffic-shaping
 !
 interface Serial3/1.1 point-to-point
 description This interface goes to branch office
 bandwidth 9
 ip address 10.3.150.1 255.255.255.0
 no cdp enable
 frame-relay interface-dlci 312
 !
 interface Serial3/2
 no ip address

```

```

shutdown
no cdp enable
!
interface Serial3/3
no ip address
shutdown
no cdp enable
!
router eigrp 100
passive-interface Ethernet0/0
network 10.0.0.0
no auto-summary
!
ip classless
no ip http server
!
!
map-class frame-relay TSLAB
frame-relay cir 9600
frame-relay traffic-rate 9600 9600
frame-relay adaptive-shaping becn
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8
central central central central central central central central central

Notes from the instructor:
All local passwords should be set to "cisco"

central central central central central central central central central
Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8 Lab8
^
!

```

```
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end
```

# Lab Exercise 9-1: Enabling a Backup to a Primary Connection

Complete this lab exercise to practice what you learned in the related module.

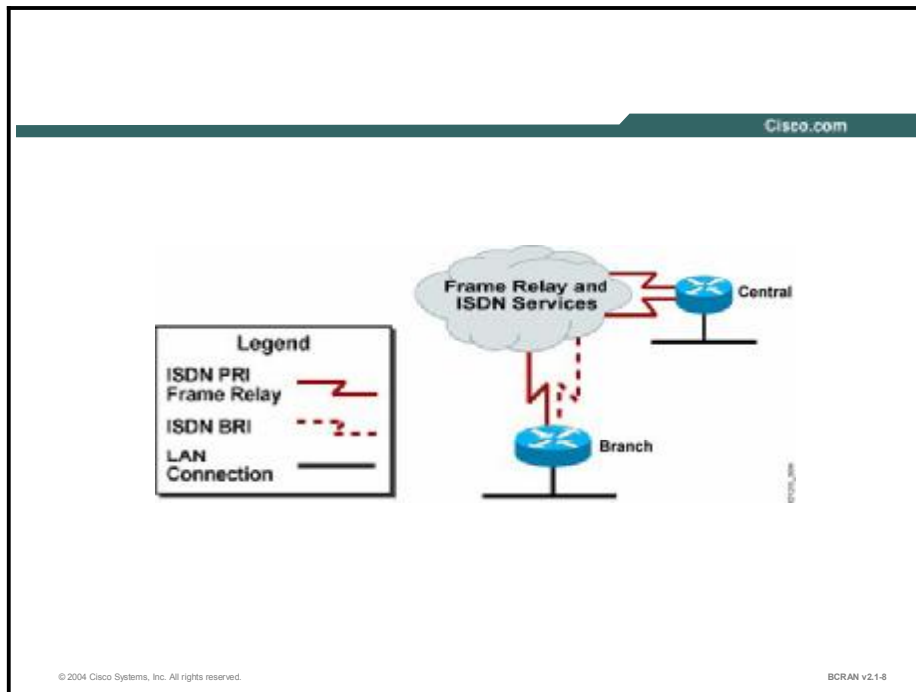
## Exercise Objective

Upon completing this lab, you will be able to:

- Configure a dial backup connection for your primary connection
- Enable the backup connection when the primary connection fails

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



## Command List

The commands used in this exercise are described in the table here.

### Configuration Commands

| Command                                                                                                                                                                         | Description                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>backup delay</b> { <b>enable-delay</b>   <b>never</b> }<br>{ <b>disable-delay</b>   <b>never</b> }                                                                           | Defines how much time should elapse before a secondary line status changes and after a primary line status changes |
| <b>backup interface</b><br><i>interface-type number</i>                                                                                                                         | Sets an interface as a secondary or dial backup interface                                                          |
| <b>debug backup</b>                                                                                                                                                             | Shows the backup process in real-time                                                                              |
| <b>dialer-list</b> <i>dialer-group</i> <b>protocol</b><br><i>protocol-name</i> { <b>permit</b><br>  <b>deny</b>   <b>list</b> <i>access-list-number</i>   <i>access-group</i> } | Specifies interesting traffic and associates it to a dialer group                                                  |
| <b>(no) logging console</b>                                                                                                                                                     | Enables and disables the logging of messages to the console                                                        |
| <b>show backup</b>                                                                                                                                                              | Shows the backup status                                                                                            |

## Scenario

Critical information is required to travel across the Frame Relay connection between the central site and remote branch office. Currently, you have connectivity from the branch router to the central office via an ISDN provider and a Frame Relay provider. You would like to use the ISDN provider only when the Frame Relay link is down. For this reason, you must configure the ISDN connection to back up the primary Frame Relay connection in the event the primary connection fails. The EIGRP routing protocol has been enabled on all links between the central and branch routers.

## Setup

Gather the information in this table prior to starting this lab.

| Pod Number ____ | Information Required                   | Example (where X is your pod number). All subnet masks are 255.255.255.0 | Write in the information for your pod ____ |
|-----------------|----------------------------------------|--------------------------------------------------------------------------|--------------------------------------------|
| Central router  | Your (first) LAN interface type        | Ethernet 0/0                                                             |                                            |
| Central router  | Your (first) LAN interface IP          | 10.X.0.1                                                                 |                                            |
| Central router  | ISDN switch type                       | primary-5ess                                                             |                                            |
| Central router  | ISDN number                            | 555X100                                                                  |                                            |
| Central router  | Dialer 1 IP to branch                  | 10.X.200.1                                                               |                                            |
| Central router  | Your (second) WAN interface type       | Serial 0/1<br>Serial 3/1                                                 |                                            |
| Central router  | Your (second) WAN interface IP address | 10.X.150.1                                                               |                                            |
| Central router  | Frame Relay DLCI                       | X12                                                                      |                                            |
| Central router  | Initial config file name               | PXc8                                                                     |                                            |
| Central router  | TFTP server address                    | 10.X.0.200                                                               |                                            |
| Branch router   | Your (first) LAN interface type        | FastEthernet0<br>Ethernet0                                               |                                            |
| Branch router   | Your (first) LAN interface IP          | 10.X.10.2                                                                |                                            |
| Branch router   | ISDN interface IP to central           | 10.X.200.2                                                               |                                            |
| Branch router   | ISDN switch type                       | basic-5ess                                                               |                                            |
| Branch router   | ISDN number                            | 555X200                                                                  |                                            |
| Branch router   | Dialer 1 IP to central                 | 10.X.200.2                                                               |                                            |
| Branch router   | Your (second) WAN interface type       | Serial 1                                                                 |                                            |
| Branch router   | Your (second) WAN interface IP address | 10.X.150.2                                                               |                                            |
| Branch router   | Frame Relay DLCI                       | X21                                                                      |                                            |
| Branch router   | Initial config file name               | PXb8                                                                     |                                            |
| Branch router   | TFTP server address                    | 10.X.10.200                                                              |                                            |



## Setup Tasks

From your PC, establish a Telnet connection to the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

TFTP the appropriate preconfiguration files to the central and branch routers and reload the routers.

Verify that your central site router and branch office routers each have a Frame Relay connection to the service provider cloud.

Verify that your central site router and branch office routers each have an ISDN connection to the service provider cloud.

As a part of the preconfiguration, a map-class named BACKUP has been enabled on the Frame Relay interface. Frame Relay end-to-end keepalives (EEKs) have been enabled in the map class so that the routers will be notified when the link is down.

Verify that you have connectivity between the central and branch routers by executing a ping between the ISDN link and the Frame Relay link.

Verify on the branch router that you have the central LAN interface network in the routing table.

Verify on the central router that you have the branch router LAN interface in the routing table.

---

**Note** As a part of the preconfiguration, it should be noted that the ISDN link is being activated by EIGRP. When you have completely configured both routers for backup operation, the ISDN line will no longer be brought up unless the Frame Relay interface is disabled.

---

## Task 1: Establishing a Backup Connection on the Central Router

On the central router, you have a Frame Relay primary connection and an ISDN backup connection to the branch router.

### Exercise Procedure

Complete these steps:

- Step 1** On the central site router, verify that the dialer interface is spoofing with the **show interface dialer 1** command. Output should be similar to the following:

```
CENTRAL_X# show interfaces dialer 1
Dialer1 is up, line protocol is up (spoofing)
<Output omitted>
```

- Step 2** Using the command list, configure the dialer 1 interface to back up the serial Frame Relay subinterface.
- Step 3** The dialer 1 interface should dial the branch router 20 seconds after the central router detects a Frame Relay connection failure. The ISDN line should also disconnect 40 seconds after Frame Relay connection is restored. Using the command list, configure this feature on the central router.
- Step 4** Save your configuration.
- Step 5** Proceed to Task 2.

## Task 2: Configuring Backup Operation on the Branch Router

On the branch router, you have a Frame Relay connection and an ISDN backup connection to the central router. You must now configure the branch router to compliment the backup operation configuration at the central site router.

### Exercise Procedure

Complete these steps:

- Step 1** The ISDN connection is already operational from the preconfiguration. This was done so that you could verify its operation prior to configuring the backup. You will now need to remove the dialer list to prevent the branch router from also bringing up the ISDN connection for EIGRP.

What is it about EIGRP that is bringing the ISDN connection up and down? \_\_\_\_\_

---

**Note** It is always best practice to verify basic connectivity and operation before implementing more advanced configurations and technologies.

---

- Step 2** Create an extended access-list 101 that denies EIGRP but allows all other IP traffic.
- Step 3** Now you must configure the branch router with a new dialer list that matches interesting traffic based on the access-list 101, and which will bring up the ISDN backup connection for interesting traffic other than EIGRP.

## Task 3: Verifying and Enabling the Dial Backup

Use the following steps to verify and enable the dial backup.

### Exercise Procedure

Complete these steps:

- Step 1** On the central site router, enter the **show interface dialer 1** command to verify that dialer 1 is in **standby mode**.
- Step 2** Use the **show backup** command and record the following information:
- Primary interface \_\_\_\_\_
- Backup interface \_\_\_\_\_
- Status \_\_\_\_\_
- Step 3** Use the **show ip route** command to determine which interface is the preferred route to the branch router LAN interface network. Record the results.
- \_\_\_\_\_
- Step 4** On the central office router, issue the command **debug backup**.
- Step 5** Console into the branch office router.
- Step 6** Shutdown the serial Frame Relay interface of the branch router and go back to the central router to examine the backup debugging events.
- Step 7** After the backup dialer interface has made connection to the branch router, verify the status of the backup interface and record your results.
- Primary interface \_\_\_\_\_
- Backup interface \_\_\_\_\_
- Status \_\_\_\_\_
- Step 6** Determine which interface is the preferred route to the branch router LAN interface network. Record the results:
- \_\_\_\_\_
- Notice that the access list at the branch router that denied EIGRP only kept EIGRP from bringing up the ISDN connection but not from distributing routes after the connection was made.
- Step 7** From the branch office router, restore the Frame Relay interface and console back to the central router to observe the backup debugging output.
- Step 8** After the debugging output has stated that the dialer 1 interface is in standby mode, verify that the central router is using the Frame Relay interface to the FastEthernet network of the branch router.

## Exercise Verification

You have completed this exercise when you attain these results:

- If the secondary line came up upon failure of the primary line and the backup line went down shortly after the primary line reengaged.

On the central router, verify that your configuration contains added lines similar to the following:

```
int serial X/1.1
backup interface dialer 1 ! Task 1 Step 2
backup delay 20 40 ! Task 1 Step 3
```

On the branch router, verify that your configuration contains added lines similar to the following:

```
access-list 101 deny eigrp any any ! Task 2 Step 2
access-list 101 permit ip any any ! Task 2 Step
2
dialer-list 1 protocol ip list 101 ! Task 2 Step 3
```

# Lab Exercise Answer Key

## Lab Exercise 9-1: Enabling a Backup to a Primary Connection

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1JrCH$wkvEFxkiU0SftE6H.YEDE.
!
username central_3 password 0 cisco
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
isdn switch-type basic-5ess
!
!
!
!
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-5ess
no cdp enable
ppp authentication chap
!
```

```

interface FastEthernet0
 description This is the Ethernet network for the Branch router
 ip address 10.3.10.2 255.255.255.0
 speed auto
 no cdp enable
!
interface Serial0
 no ip address
 encapsulation frame-relay
 shutdown
!
interface Serial1
 bandwidth 32
 no ip address
 encapsulation frame-relay
 frame-relay class BACKUPLAB
!
interface Serial1.1 point-to-point
 description This interface goes to Central
 ip address 10.3.150.2 255.255.255.0
 no cdp enable
 frame-relay interface-dlci 321
!
interface Dialer1
 description This dialer goes from Branch to Central
 ip address 10.3.200.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer remote-name central_3
 dialer string 5553100
 dialer-group 1
 no cdp enable
 ppp authentication chap
!
router eigrp 100
 passive-interface FastEthernet0
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!

```

```

ip classless
no ip http server
ip pim bidir-enable
!
!
!
map-class frame-relay BACKUPLAB
 frame-relay end-to-end keepalive mode bidirectional
 frame-relay adaptive-shaping becn
access-list 101 deny eigrp any any
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
no cdp run
!
banner motd ^
Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9
branch branch branch branch branch branch branch branch

Notes from the instructor:
All local passwords should be set to "cisco"

branch branch branch branch branch branch branch branch
Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab8 Lab9
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
no scheduler allocate
end

```

## Central Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1sFQN$FqoBYgbb6bbkpC6ERDrKg1
!
username branch_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
!
isdn switch-type primary-5ess
call rsvp-sync
!
!
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
!
interface Ethernet0/0
 description This is the Ethernet network for the Central router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
```



```

shutdown
half-duplex
no cdp enable
!
interface Serial1/0:23
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type primary-5ess
no cdp enable
ppp authentication chap
!
interface Serial3/0
no ip address
shutdown
no cdp enable
!
interface Serial3/1
bandwidth 128
no ip address
encapsulation frame-relay
frame-relay class BACKUPLAB
!
interface Serial3/1.1 point-to-point
description This interface goes to branch office
backup delay 20 40
backup interface Dialer1
ip address 10.3.150.1 255.255.255.0
no cdp enable
frame-relay interface-dlci 312
!
interface Serial3/2
no ip address
shutdown
no cdp enable
!
interface Serial3/3
no ip address
shutdown
no cdp enable

```

```

!
interface Dialer1
 description This dialer goes from Central to Branch
 ip address 10.3.200.1 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer remote-name branch_3
 dialer string 5553200
 dialer-group 1
 no cdp enable
 ppp authentication chap
!
router eigrp 100
 passive-interface Ethernet0/0
 network 10.0.0.0
 no auto-summary
!
ip classless
no ip http server
!
!
map-class frame-relay BACKUPLAB
 frame-relay end-to-end keepalive mode bidirectional
 frame-relay adaptive-shaping becn
dialer-list 1 protocol ip permit
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9
central central central central central central central central

Notes from the instructor:
All local passwords should be set to "cisco"

```

```
central central central central central central central central
Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9 Lab9
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end
```

# Lab Exercise 10-1: Managing Network Performance Using CBWFQ and LLQ

Complete this lab exercise to practice what you learned in the related module.

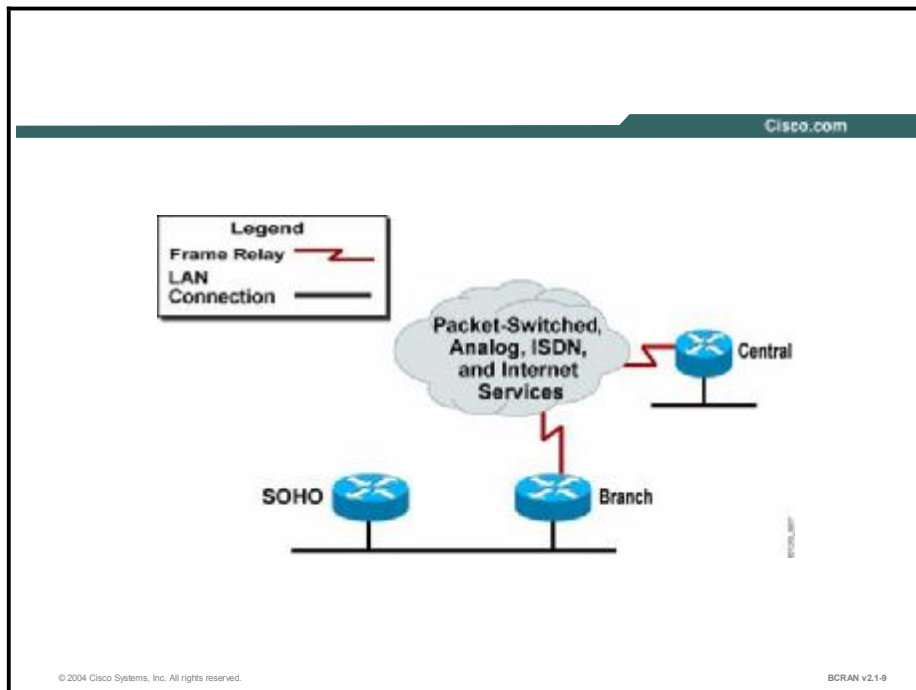
## Exercise Objective

Upon completing this lab, you will be able to:

- Use an access list to define the traffic of interest that you want to classify
- Configure a class map that associates an access list with a traffic class
- Configure a policy map that associates a traffic class to a queue and guarantees bandwidth
- Configure CBWFQ on an interface
- Verify CBWFQ operation

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



# Command List

The commands used in this exercise are described in the table here.

## Configuration Commands

| Command                                                 | Description                                                                               |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>bandwidth percent</b><br><i>bandwidth-allocation</i> | Used to configure the percentage of bandwidth to be allocated for a class                 |
| <b>class class-map-name</b>                             | Used to define a class within a policy map                                                |
| <b>class-map {match-all   match-any} name</b>           | Used to configure quality of service (QoS) class maps.                                    |
| <b>match access-group</b><br><i>access-list</i>         | Used to define a match from an access list to a class-map                                 |
| <b>policy-map name</b>                                  | Used to create a traffic policy                                                           |
| <b>service-policy output</b><br><i>policy-map-name</i>  | Used to attach the traffic policy to the interface                                        |
| <b>show frame-relay pvc</b><br>[ <i>dlci</i> ]          | Used to display detailed information about the state of a PVC on a router                 |
| <b>show policy-map</b><br>[ <i>interface</i> ]          | Used to display the configuration of all classes forming the specified service policy map |
| <b>priority bandwidth-kbps</b>                          | Used within a policy map to define the priority bandwidth                                 |

## Scenario

Users at the branch office are reporting problems with traffic coming from the central site. HTTP packets are being dropped due to other network traffic that is on the Frame Relay link. Users at the central office have also been complaining that Telnet traffic going to the branch office is also being degraded.

After studying traffic patterns, management has decided to allocate 50 percent of the available Frame Relay bandwidth for HTTP network traffic going to the branch office from the central office LAN connection. Another 25 percent of all network traffic traversing the Frame Relay link will be allocated to Telnet traffic coming from the central office LAN connection. All other traffic will contend for the remaining available Frame Relay bandwidth.

As the lead network engineer, you have decided to implement class-based weighted fair queuing (CBWFQ) to support the management-defined QoS requirements.

## Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number ____ | Information Required                         | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod ____ |
|-----------------|----------------------------------------------|--------------------------------------------------------------------|--------------------------------------------|
| Central router  | Your (first) LAN interface type              | Ethernet 0/0                                                       |                                            |
| Central router  | Your (first) LAN interface IP                | 10.X.0.1                                                           |                                            |
| Central router  | Your (second/Frame Relay) WAN interface type | Serial 0/1<br>Serial 3/1                                           |                                            |
| Central router  | Your (second/Frame Relay) WAN interface IP   | 10.X.150.1                                                         |                                            |
| Central router  | Frame Relay DLCI                             | X12                                                                |                                            |
| Central router  | Initial config file name                     | pXc9                                                               |                                            |
| Central router  | TFTP server address                          | 10.x.0.200                                                         |                                            |
| Branch router   | Your (first) LAN interface type              | FastEthernet0<br>Ethernet0                                         |                                            |
| Branch router   | Your (first) LAN interface IP                | 10.X.10.2                                                          |                                            |
| Branch router   | Your (second/Frame Relay) WAN interface type | Serial 1                                                           |                                            |
| Branch router   | Your (second/Frame Relay) WAN interface IP   | 10.X.150.2                                                         |                                            |
| Branch router   | Frame Relay DLCI                             | X21                                                                |                                            |
| Branch router   | Initial config file name                     | PXb9                                                               | Branch Router                              |
| Branch router   | TFTP server address                          | 10.X.10.200                                                        | Branch Router                              |
| SOHO router     | Your (first) LAN interface type              | Ethernet 0                                                         |                                            |
| SOHO router     | Your (first) LAN interface IP                | 10.X.10.3                                                          |                                            |
| SOHO router     | Loopback 42 IP                               | 10.X.42.3                                                          |                                            |
| SOHO router     | Loopback 43 IP                               | 10.X.43.3                                                          |                                            |
| SOHO router     | Loopback 44 IP                               | 10.X.44.3                                                          |                                            |
| SOHO router     | initial config file name                     | PXc9                                                               |                                            |
| SOHO router     | TFTP server address                          | 10.X.100.200                                                       |                                            |

## Setup Tasks

From your PC, establish a Telnet connection to the terminal server and open a console connection to the central router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a second console connection to the branch router of your pod.

From your PC, establish a Telnet connection to the terminal server again and open a third console connection to the SOHO router of your pod.

You will now be able to configure and observe output on all routers simultaneously.

TFTP the appropriate preconfiguration files to the central, branch, and SOHO routers, then reload the routers.

Verify that your central site and branch office routers each have a Frame Relay connection to the service provider cloud.

The SOHO site is located near the branch site and connects to it via a LAN network connection. The SOHO router will be used to generate IP traffic to test QoS configurations on the Frame Relay connection. Three loopback interfaces have been configured on the SOHO router for the extended ping tests, which will simulate user traffic.

Verify that you have connectivity between the central and branch routers by executing a ping between Frame Relay links.

Verify that you can execute an extended ping from the three loopback interfaces of the SOHO router to the LAN IP address of the central router.

## Task 1: Configuring a Class Map and Policy Map for CBWFQ

Use the following steps to configure a class map and policy map for CBWFQ.

### Exercise Procedure

Complete these steps:

- Step 1** On a central site router, create an extended IP access list 100 to permit HTTP traffic requests coming from the LAN network of the central site to go to the LAN network of the branch site.
- Step 2** Create an extended IP access list 101 to permit Telnet traffic requests originating from the LAN network of the central site to go to the LAN network of the branch site.
- Step 3** Using the command list, create a class map named HTTP-CLASS and configure a match condition with access list 100.
- Step 4** Using the command list, create a class map named TELNET-CLASS and configure a match condition with access list 101.
- Step 5** Create a policy map named CBWFQ-CENTRAL.

- Step 6** In the policy map, create a traffic policy for class HTTP-CLASS, allocating a minimum of 50 percent of the available bandwidth. Under the same policy map, create a traffic policy for class TELNET-CLASS allocating a minimum of 25 percent of the available bandwidth.
- Step 7** Apply the policy-map CBWFQ-CENTRAL to the Frame Relay traffic shaping map class TSLAB.
- Step 8** You have now configured QoS for the users at the central site accessing the LAN network of the branch office. Save the central router configuration.
- Step 9** Proceed to Task 2.

## Task 2: Verifying the CBWFQ Configuration on the Central Router

Use the following steps to verify the CBWFQ configuration on the central router.

### Exercise Procedure

Complete these steps:

- Step 1** On the central site router, use the **show** commands that are listed in the command list to complete the following information:

Bandwidth allocated to the HTTP-CLASS: \_\_\_\_\_

Bandwidth offered rate for the HTTP-CLASS: \_\_\_\_\_

Bandwidth allocated to the TELNET-CLASS: \_\_\_\_\_

Bandwidth offered rate for the TELNET-CLASS: \_\_\_\_\_

- Step 2** What command would you use to verify that the CBWFQ is applied correctly to your Frame Relay interface to display the following information:

<Output Omitted>

```

Shaping adapts to BECN
pvc create time 01:05:49, last time pvc status changed
00:52:48
 cir 9600 bc 9600 be 0 byte limit 150
interval 125
 mincir 4800 byte increment 150 Adaptive Shaping BECN
 pkts 800 bytes 52000 pkts delayed 8 bytes
delayed 832
 shaping inactive
 traffic shaping drops 0
 service policy CBWFQ-CENTRAL
<Output Omitted >

```



What command did you enter? \_\_\_\_\_

**Step 3** Proceed to Task 3.

## Task 3: Implementing LLQ and CBWFQ on the Branch Router

Use the following steps to configure LLQ and CBWFQ on the branch router.

### Exercise Procedure

Complete these steps:

- Step 1** On the branch router, create an extended IP access list 102 to permit traffic from the loopback 42 interface of the SOHO site to the LAN network of the central site. This is to simulate all low-latency dependent traffic flow such as voice over IP and will be your low latency queuing (LLQ).
- Step 2** Create an extended IP access list 103 to permit traffic from the loopback 43 interface of the SOHO site to the LAN network of the central site.
- Step 3** Create an extended IP access list 104 to permit traffic from the loopback 44 interface of the SOHO site to the LAN network of the central site. This will simulate another data-only traffic flow that is vital, but again there are no low-latency requirements and it will use CBWFQ.
- Step 4** Using the command list, create a class map named LLQ-102-CLASS and configure a match condition with access list 102.
- Step 5** Using the command list, create a class map named CBWFQ-103-CLASS and configure a match condition with access list 103.
- Step 6** Using the command list, create a class map named CBWFQ-104-CLASS and configure a match condition with access list 104.
- Step 7** Create a policy map named CBWFQ-BRANCH.
- Step 8** Create a traffic policy for the class of traffic named LLQ-102-CLASS, specifying a priority of 8 kbps. This will be your priority queue used to implement LLQ and will service traffic coming from loopback 42 at the SOHO router. Loopback 42 can be considered a voice-enabled resource that is sensitive to delay and jitter. For users at the central site, you want to ensure the quality of the voice being transmitted across the Frame Relay link.
- Step 9** Why will LLQ support voice traffic? \_\_\_\_\_
- Step 10** Create a traffic policy for the class of traffic named CBWFQ-103-CLASS, specifying a bandwidth of 25 percent. This will be your CBWFQ queue that will service traffic coming from loopback 43 at the SOHO router. As such, you want to guarantee a minimum percentage of the available bandwidth after the LLQ uses its 8 kbps.

- Step 11** Create a traffic policy for the class of traffic named CBWFQ-104-CLASS, specifying a bandwidth of 25 percent. This will be your CBWFQ queue that will service traffic coming from loopback 44 at the SOHO router. As such, you want to guarantee a minimum percentage of the available bandwidth after the LLQ uses its 8 kbps. The queues servicing loopbacks 43 and 44 will be in contention for the remaining bandwidth across the Frame Relay link.
- Step 12** Apply the policy map CBWFQ-BRANCH to the Frame Relay traffic shaping map class TSLAB.
- Step 13** You have now configured QoS for the users at the LAN network of the branch office accessing the central site. Save the configuration of the branch office router.
- Step 14** Proceed to Task 4.

## Task 4: Verifying the CBWFQ/LLQ Configuration on the Branch Router

You will now verify the CBWFQ/LLQ configuration on the branch router using the following procedure.

### Exercise Procedure

Complete these steps:

- Step 1** On the branch site router, use the **show** commands listed in the command list to complete the following information:
- Bandwidth allocated to the LLQ-102-CLASS: \_\_\_\_\_
- The amount of burst that LLQ-102-CLASS is allowed: \_\_\_\_\_
- Bandwidth allocated to the CBWFQ-103-CLASS: \_\_\_\_\_
- Bandwidth allocated to the CBWFQ-104-CLASS: \_\_\_\_\_
- Step 2** Proceed to Task 5

## Task 5: Generating Traffic from the SOHO Router to Congest the Branch-to-Central Frame Relay Link

You will establish three connections to the SOHO router to generate significant network traffic. You must accomplish all three extended ping sessions in a timely manner to congest the Frame Relay link between the branch and central site. Read these steps before attempting to complete this task.

### Exercise Procedure

Complete these steps:

- Step 1** Enter the console session to the SOHO router.
- Step 2** Execute an extended ping to the LAN interface of the central router, using the loopback 42 address as the source address. In addition, use 2000 as the ping repeat count with a datagram size of 60 bytes. This will simulate a voice-over-IP data flow for which you configured LLQ.
- Step 3** While the extended ping is ongoing, enter the console to the central router.
- Step 4** Establish a Telnet session to the SOHO router from the central router.
- Step 5** Execute another extended ping to the LAN interface of the central router using the loopback 43 address as the source address. In addition, use 1500 as the ping count with a datagram size of 1500 bytes. This will simulate the IP data flow that will use CBWFQ.
- Step 6** While that extended ping is ongoing, suspend the Telnet session by pressing **Ctrl-shift-6** twice, and then pressing **Ctrl-x**. You should now be at the prompt of the central router.
- Step 7** Establish a second Telnet session into the SOHO router from the central router.
- Step 8** Execute another extended ping to the LAN interface of the central router, using the loopback 44 address as the source address. In addition, use 1500 as the ping count with a datagram size of 1500 bytes. This will simulate the other IP data flow that will use CBWFQ.
- Step 9** Enter the console session of the branch router.
- Step 10** On the branch site router, use the **show** commands that are listed in the command list repeatedly to complete the following information:

---

**Note** It will take a few minutes before the CBWFQs reach their maximum threshold of 64 packets and begin to start dropping packets.

---

**Bandwidth allocated to the LLQ-102-CLASS:** \_\_\_\_\_

**Bandwidth allocated to the CBWFQ-103-CLASS:** \_\_\_\_\_

**Bandwidth allocated to the CBWFQ-104-CLASS:** \_\_\_\_\_

**Drop rate for the CBWFQ-103-CLASS:** \_\_\_\_\_

Drop rate for the CBWFQ-104-CLASS: \_\_\_\_\_

## Exercise Verification

You have completed this exercise when you attain these results:

- If you were able to configure and verify that CBWFQ and LLQ were configured properly.

On the central router, verify that your configuration contains added lines similar to the following:

```
class-map match-all TELNET-CLASS ! Task 1 Step 4
 match access-group 101 ! Task 1 Step 4
class-map match-all HTTP-CLASS ! Task 1 Step 3
 match access-group 100 ! Task 1 Step 3

policy-map CBWFQ-CENTRAL ! Task 1 Step 6
 class HTTP-CLASS ! Task 1 Step 7
 bandwidth percent 50 ! Task 1 Step 7
 class TELNET-CLASS ! Task 1 Step 7
 bandwidth percent 25 ! Task 1 Step 7

map-class frame-relay TSLAB ! from preconfig
 frame-relay cir 128000 ! from preconfig
 frame-relay be 32000 ! from preconfig
 frame-relay traffic-rate 96000 128000 ! from preconfig
 no frame-relay adaptive-shaping ! from preconfig
 service-policy output CBWFQ-CENTRAL ! Task 1 step 8

access-list 100 permit tcp 10.X.0.0 0.0.0.255 eq www 10.X.10.0
0.0.0.255 ! Task 1 step 1
access-list 101 permit tcp 10.X.0.0 0.0.0.255 eq telnet 10.X.10.0
0.0.0.255 ! Task 1 step 2
```

On the branch router, verify that your configuration contains lines similar to the following:

```
class-map match-all LLQ-102-CLASS ! Task 3 Step 4
 match access-group 102 ! Task 3 Step 4
class-map match-all CBWFQ-103-CLASS ! Task 3 Step 5
 match access-group 103 ! Task 3 Step 5
class-map match-all CBWFQ-104-CLASS ! Task 3 Step 6
 match access-group 104 ! Task 3 Step 6

policy-map CBWFQ-BRANCH ! Task 3 Step 7
 class LLQ-102-CLASS ! Task 3 Step 8
```

```

 priority 8 ! Task 3 Step 8
class CBWFQ-103-CLASS ! Task 3 Step 9
 bandwidth percent 25 ! Task 3 Step 9
class CBWFQ-104-CLASS ! Task 3 Step 10
 bandwidth percent 25 ! Task 3 Step 10

map-class frame-relay TSLAB ! from preconfig
frame-relay cir 28000 ! from preconfig
frame-relay mincir 16000 ! from preconfig
frame-relay be 4000 ! from preconfig
frame-relay traffic-rate 8000 8000 ! from preconfig
no frame-relay adaptive-shaping ! from preconfig
service-policy output CBWFQ-BRANCH ! Task 3 step 11

access-list 102 permit ip host 10.X.42.3 10.X.0.0 0.0.0.255! Task 3
step 2
access-list 103 permit ip host 10.X.43.3 10.X.0.0 0.0.0.255! Task 3
step 3
access-list 104 permit ip host 10.X.44.3 10.X.0.0 0.0.0.255! Task 3
step 4

```

# Lab Exercise Answer Key

## Lab Exercise 10-1: Managing Network Performance Using CBWFQ and LLQ

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1tq5Y$vyypkD8k41/haNVuHZwd0./
!
memory-size iomem 25
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
class-map match-all LLQ-102-CLASS
 match access-group 102
class-map match-all CBWFQ-104-CLASS
 match access-group 104
class-map match-all CBWFQ-103-CLASS
 match access-group 103
!
!
policy-map CBWFQ-BRANCH
 class LLQ-102-CLASS
 priority 8
 class CBWFQ-103-CLASS
```

```

 bandwidth percent 25
 class CBWFQ-104-CLASS
 bandwidth percent 25
!
!
!
!
!
interface BRI0
 no ip address
 shutdown
 no cdp enable
!
interface FastEthernet0
 description This is the Ethernet network for the Branch router
 ip address 10.3.10.2 255.255.255.0
 speed auto
 no cdp enable
!
interface Serial0
 no ip address
 shutdown
 no cdp enable
!
interface Serial1
 bandwidth 32
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
!
interface Serial1.1 point-to-point
 description This interface goes to Central
 ip address 10.3.150.2 255.255.255.0
 no cdp enable
 frame-relay class TSLAB
 frame-relay interface-dlci 321
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.150.1

```

```

ip route 10.3.40.0 255.255.248.0 10.3.10.3
no ip http server
ip pim bidir-enable
!
!
!
map-class frame-relay TSLAB
 frame-relay cir 28000
 frame-relay be 4000
 frame-relay mincir 16000
 frame-relay traffic-rate 8000 8000
 no frame-relay adaptive-shaping
 service-policy output CBWFQ-BRANCH
access-list 102 permit ip host 10.3.42.3 10.3.0.0 0.0.0.255
access-list 103 permit ip host 10.3.43.3 10.3.0.0 0.0.0.255
access-list 104 permit ip host 10.3.44.3 10.3.0.0 0.0.0.255
no cdp run
!
banner motd ^
Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
Lab10

branch branch branch branch branch branch branch branch

Notes from the instructor:
All local passwords should be set to "cisco"

branch branch branch branch branch branch branch branch
Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
Lab10
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login

```



```
 history size 200
!
end
```

### Central Router End Configuration

```
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1FDyO$nf5uluCduC8FKzMNZCfde/
!
ip subnet-zero
!
!
no ip domain-lookup
!
!
class-map match-all TELNET-CLASS
 match access-group 101
class-map match-all HTTP-CLASS
 match access-group 100
!
!
policy-map CBWFQ-CENTRAL
 class HTTP-CLASS
 bandwidth percent 50
 class TELNET-CLASS
 bandwidth percent 25
!
!
call rsvp-sync
!
!
!
!
!
!
!
controller T1 1/0
```

```

framing sf
linecode ami
!
!
!
interface Ethernet0/0
 description This is the Ethernet network for the Central router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Serial3/0
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/1
 bandwidth 128
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
!
interface Serial3/1.1 point-to-point
 description This interface goes to branch office
 ip address 10.3.150.1 255.255.255.0
 no cdp enable
 frame-relay class TSLAB
 frame-relay interface-dlci 312
!
interface Serial3/2
 no ip address
 shutdown
 no cdp enable

```

```

!
interface Serial3/3
 no ip address
 shutdown
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.150.2
no ip http server
!
!
map-class frame-relay TSLAB
 frame-relay cir 128000
 frame-relay be 32000
 frame-relay traffic-rate 96000 128000
 no frame-relay adaptive-shaping
 service-policy output CBWFQ-CENTRAL
access-list 100 permit tcp 10.3.0.0 0.0.0.255 eq www 10.3.10.0
 0.0.0.255
access-list 101 permit tcp 10.3.0.0 0.0.0.255 eq telnet 10.3.10.0
 0.0.0.255
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab10 Lab9 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
 Lab10
central central central central central central central central

Notes from the instructor:
All local passwords should be set to "cisco"

central central central central central central central central
Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
 Lab10
^
!

```

```

line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end

```

### SOHO Router End Configuration

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname soho_3
!
enable secret 5 1aNN7$a0cNnou/3pPLS5d5ZRy8b1
!
ip subnet-zero
no ip domain-lookup
!
!
!
!
!
interface Loopback42
 description loopback used to generate 60 byte voice traffic
 ip address 10.3.42.3 255.255.255.0
!
interface Loopback43
 description loopback used to generate 1500 byte traffic
 ip address 10.3.43.3 255.255.255.0
!

```

```

interface Loopback44
 description loopback used to generate 1500 byte traffic
 ip address 10.3.44.3 255.255.255.0
!
interface Ethernet0
 description This is the Ethernet network for the SOHO router
 ip address 10.3.100.3 255.255.255.0 secondary
 ip address 10.3.10.3 255.255.255.0
 no cdp enable
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.10.2
no ip http server
!
no cdp run
banner motd ^
Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
 Lab10
soho soho soho soho soho soho soho soho soho soho soho soho

Notes from the instructor:
All local passwords should be set to "cisco"

soho soho soho soho soho soho soho soho soho soho soho soho
Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10 Lab10
 Lab10
^
!
line con 0
 exec-timeout 30 0
 logging synchronous level all
 history size 200
line vty 0 4
 exec-timeout 30 0
 password cisco

```

```
logging synchronous
login
history size 200
!
end
```

# Lab Exercise 11-1: Using AAA to Scale Access Control

Complete the lab exercise to practice what you learned in the related module.

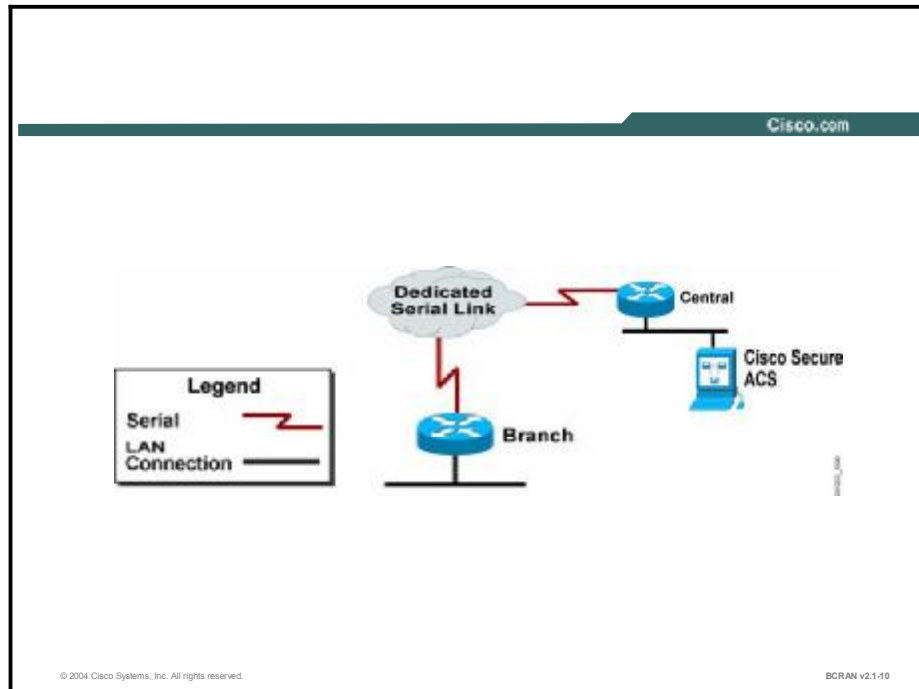
## Exercise Objective

In this exercise you will complete the following tasks:

- Configure the central router for AAA authentication to a Cisco Secure ACS server for user Telnet sessions
- Configure the central router for AAA authorization to a Cisco Secure ACS server to authorize users for different EXEC privilege levels
- Configure the central router for AAA accounting to a Cisco Secure ACS server to record accounting information for EXEC privileges committed and network access
- Configure the central router console port and virtual terminal lines for “back door” access in the event of a Cisco Secure ACS server failure

## Visual Objective

The figure illustrates what you will accomplish in this exercise.



## Command List

The commands used in this exercise are described in the table here.

### Helpful Commands

| Command                                                          | Description                                                                                                  |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>aaa accounting exec default start-stop group TACACS+</b>      | Specifies that start-stop accounting will be used on all EXEC processes                                      |
| <b>aaa accounting network default start-stop group TACACS+</b>   | Specifies that start-stop accounting will be used on all network processes                                   |
| <b>aaa authentication login no_tacacs enable</b>                 | Specifies that the login authentication list that no_tacacs is to use the enable password for authentication |
| <b>aaa authentication login telnet-order group TACACS+ local</b> | Specifies the order of authentication methods for login attempts                                             |
| <b>aaa authorization exec default group tacacs</b>               | Specifies that authorization for EXEC processes will be from TACACS+                                         |
| <b>aaa new-model</b>                                             | Enables authentication, authorization, and accounting (AAA) access control                                   |
| <b>debug aaa accounting</b>                                      | Displays the output of the AAA accounting process                                                            |
| <b>debug aaa authentication</b>                                  | Displays the output of the AAA authentication process                                                        |
| <b>debug aaa authorization</b>                                   | Displays the output of the AAA authorization process                                                         |
| <b>debug radius</b>                                              | Displays the output of the AAA RADIUS process                                                                |
| <b>debug tacacs</b>                                              | Displays the output of the AAA TACACS+ process                                                               |
| <b>debug tacacs events</b>                                       | Displays the output of the AAA TACACS+ process                                                               |
| <b>login authentication no_tacacs</b>                            | Applies the list no_tacacs as the login authentication method                                                |
| <b>radius-server host address</b>                                | Specifies the IP address of the RADIUS server                                                                |
| <b>radius-server key cisco</b>                                   | Specifies a key of "cisco" for authentication between the access server and the RADIUS server                |
| <b>reload cancel</b>                                             | Stops a scheduled reload                                                                                     |
| <b>reload in hhh:mm</b>                                          | Reloads the router in the event you lock yourself out                                                        |
| <b>tacacs-server host address single-connection</b>              | Specifies the IP address of the TACACS+ server                                                               |
| <b>tacacs-server key cisco</b>                                   | Specifies a key of "cisco" for authentication between the access server and the TACACS+ server               |
| <b>username username password password</b>                       | Sets the username and password on the router for local authentication                                        |
| <b>undebug all</b>                                               | Disables all or specific debugging                                                                           |



## Scenario

You will configure the central router to use a preconfigured Cisco Secure TACACS+ Server that shares the Ethernet backbone with all the central routers. This process will allow you to centralize your authentication usernames and passwords, your authorization control processes, and all of your accounting records throughout your enterprise.

## Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number _____        | Information Required            | Example (X is your pod number; all subnet masks are 255.255.255.0) | Write in the information for your pod |
|-------------------------|---------------------------------|--------------------------------------------------------------------|---------------------------------------|
| Central router          | Your (first) LAN interface type | Ethernet 0/0                                                       |                                       |
| Central router          | Your (first) LAN interface IP   | 10.X.0.1                                                           |                                       |
| Central router          | Your (first) WAN interface type | Serial 0/0<br>Serial 3/0                                           |                                       |
| Central router          | Your (first) WAN interface IP   | 10.X.160.1                                                         |                                       |
| Cisco Secure AAA Server | IP address                      | 10.X.0.200                                                         |                                       |
| Branch router           | Your (first) LAN interface IP   | 10.X.10.2                                                          |                                       |
| Branch router           | Your (first) LAN interface type | FastEthernet 0                                                     |                                       |
| Branch router           | Your (first) WAN interface type | Serial 0                                                           |                                       |
| Branch router           | Your (first) WAN interface IP   | 10.X.160.2                                                         |                                       |

### Setup Tasks

From your PC, establish a Telnet session on the terminal server and open a console connection to the branch router of your pod.

From your PC, establish a Telnet session on the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

Using the TFTP facility, copy the appropriate preconfiguration files to the central and branch routers, then reload.

Verify the network connectivity by executing a ping from the branch router to the Cisco Secure TACACS+ Server.

## Task 1: Preparing the Central Router for AAA Operation

This task prepares the central router for AAA operation.

### Exercise Procedure

Complete these steps:

- Step 1** Log in to the EXEC privilege mode on your central router. Enter the command **reload in 60**.

---

**Note** If you make a mistake when you are configuring the router to use the AAA server for authentication, you may accidentally lock yourself out of the router. Executing a **reload in 60** (minutes) command will cause your router to reload automatically in 60 minutes. This action will insure that you will be able to recover from the mistake when the router reloads. Refer to your lab command reference list to cancel the reload operation.

---

- Step 2** Enable the AAA access control service.

- Step 3** Enter the command that will create an authentication list named **no\_tacacs** using the enable secret password as the password for login authentications.

- Step 4** Configure your central router console to use the **no\_tacacs** authentication list. This action will create a back door at the console to allow you to access the router without using the Cisco Secure ACS server by authenticating users with the enable secret password, which is stored locally.

- Step 5** Log out of the central router without closing the console session completely.

---

**Caution** Do not save your configuration until you have completed Task 2 and tested it.

---

- Step 6** Proceed to Task 2.

## Task 2: Testing the Central Router Console Back Door

This task will test how to gain access through the central router console back door.

### Exercise Procedure

Complete these steps:

- Step 1** On the console session of your central router, press **Return**. You will be prompted for a password.

- Step 2** Enter the enable secret password. If your back door is configured properly, you will be granted access.

If you were able to gain access to the console of your central router, save your configuration.

- Step 3** Proceed to Task 3.

## Task 3: Configuring and Testing the Central Router for AAA Local User Authentication

This task configures and tests the central router for AAA local user authentication.

### Exercise Procedure

Complete these steps:

- Step 1** At your central router, enable TACACS+ and AAA authentication debugging. Observe the debug output of the central router while completing the steps in this task. Look for any AAA authentication activity pertaining to the branch router.
- Step 2** Open the branch router console session.
- Step 3** From the branch router, attempt to establish a Telnet session on the central router using the username **user** and the password **letmein**. This attempt will be unsuccessful because this username and password are on the Cisco Secure ACS server. Your central router is configured to check only locally for usernames and passwords.
- Step 4** From the branch router, attempt to establish a Telnet session on the central router using the username **localuser** and the password **cisco**. This attempt will be successful only after you have configured a local username and password on the central router.
- Step 5** On the central router, configure the local username **localuser** and the password **cisco**.
- Step 6** Repeat Step 4. You should now be able to access the central router.
- Step 7** Disable all debugging on the central router and log out.
- Step 8** Proceed to Task 4.

## Task 4: Configuring and Testing the Central Router for AAA TACACS+ User Authentication

This task configures and tests the central router for AAA TACACS+ user authentication.

### Exercise Procedure

Complete these steps:

- Step 1** Configure your central router with the address of the Cisco Secure ACS server and the key **cisco** for the AAA service using the TACACS+ protocol.
- Step 2** Configure your central router with the same key for the AAA service, but use the RADIUS protocol.
- Step 3** Configure a login authentication list named **telnet-order**. The list should be configured in such a way that Telnet sessions would be authenticated by the Cisco Secure ACS server using the TACACS+ protocol first and then by the local username and password if the Cisco Secure ACS server were unreachable.

- Step 4** Configure the central router virtual terminal lines to use the **telnet-order** authentication list when authenticating Telnet sessions.
- Step 5** Enable both TACACS+ and TACACS+ events debugging. Observe the debug output on the central router while performing the next steps.
- Step 6** From the branch router,, establish a Telnet session on the central router with the username **localuser** and the password **cisco**. You will not be successful because you are now using the Cisco Secure ACS server as your ACS server, where the username **localuser** is not configured.
- Step 7** Again, attempt to establish a Telnet session from the branch router to the central router, but use the username **user** and the password **letmein**. You will succeed because the Cisco Secure ACS server has been preconfigured with that username and password.
- Step 8** Exit to the branch router.

While you were executing the unsuccessful login in Steps 6 and 7, the central router should have generated TACACS+ debug output similar to this:

```
00:47:15: TAC+: Using default tacacs server-group "tacacs+"
list.
00:47:15: TAC+: Opening TCP/IP to 10.1.0.200/49 timeout=5
00:47:15: TAC+: Opened TCP/IP handle 0x62A17ADC to
10.1.0.200/49
```

<Output omitted>

```
00:47:15: TAC+: ver=192 id=1628988694 received AUTHEN status =
GETUSER
```

<Output omitted>

```
00:47:21: TAC+: ver=192 id=1628988694 received AUTHEN status =
GETPASS
```

<Output omitted>

```
00:47:24: TAC+: ver=192 id=1628988694 received AUTHEN status =
FAIL
```

A successful login would look similar to this:

```
00:47:44: TAC+: Using default tacacs server-group "tacacs+"
list.
```

<Output omitted>

```
00:47:45: TAC+: ver=192 id=3696549381 received AUTHEN status =
GETUSER
```

<Output omitted>

```
00:47:49: TAC+: ver=192 id=3696549381 received AUTHEN status =
GETPASS
```

<Output omitted>

```
00:47:51: TAC+: ver=192 id=3696549381 received AUTHEN status =
PASS
```

**Step 9** Disable all debugging.

**Step 10** Proceed to Task 5.

## Task 5: Configuring and Testing the Central Router AAA EXEC Authorization

This task configures and tests the central router AAA EXEC authorization.

### Exercise Procedure

Complete these steps:

- Step 1** Enable AAA authorization, TACACS+, and TACACS+ events debugging at the central router and observe the debug output while completing the next steps.
- Step 2** Establish a Telnet session from the branch router to the central router using the username **superuser** and the password **root**. This username and password have also been preconfigured on the Cisco Secure ACS server.

---

**Note** As indicated by the prompt you see on completing Step 2, the username superuser is in user EXEC mode. To be authorized to use the higher-level commands available in privileged EXEC mode, you would have to supply the local enable secret password.

---

**Step 3** Exit to the branch router.

**Step 4** On the central router, configure AAA authorization for the privileged EXEC mode using the Cisco Secure ACS server and the default authorization list.

---

**Note** Ignore the following console message:  
02:23:33: AAA/AUTHOR: config command authorization not enabled

---

- Step 5** Establish a Telnet session from the branch router to the central router using the username **superuser** and the password **root**. You should automatically be placed in privileged EXEC mode because the Cisco Secure ACS server has authorized the user superuser. There is no need to supply the local enable secret password to use privileged EXEC commands. This output indicates that authorization for the EXEC process is functioning.
- Step 6** Exit to the branch router.
- Step 7** Again establish a Telnet session from the branch router to the central router using the username **user** with the password **letmein**.

---

**Note** Because the user **user** has been preconfigured on the Cisco Secure ACS server, you are able to authenticate and access user EXEC mode. However, you would have to supply the local enable secret password to access privileged EXEC mode.

---

- Step 8** While logged into the central router as the user **user**, enter the privileged EXEC mode.

---

**Note** Notice the difference between authentication and authorization. The user **user** is still able gain access to the privileged user EXEC mode by providing the local enable secret password, which is still the configured enable authentication method. The lack of authorization does not prohibit that access.

---

- Step 9** Exit to the branch router.

While you completed Task 5, the central router should have generated AAA TACACS+ and authorization debug output similar to the following user debug output:

<Output omitted>

```
01:36:57: TAC+: periodic timer stopped (queue empty)
01:36:57: TAC+: (793171495): received author response status =
PASS_ADD
01:36:57: TAC+: Closing TCP/IP 0x62A2FB88 connection to
10.1.0.200/49
```

The following is an example of how the superuser debug output should look:

```
01:00:31: TAC+: 10.1.0.200 req=62A30D58 Qd id=88587168 ver=192
handle=0x62A19238 (ESTAB) expire=5 AUTHOR/START queued
```

<Output omitted>

```
01:00:31: TAC+: (88587168) AUTHOR/START processed
```

<Output omitted>

```
01:00:31: TAC+: (88587168): received author response status =
PASS_ADD
01:00:31: TAC+: Closing TCP/IP 0x62A19238 connection to
10.1.0.200/49
01:00:31: TAC+: Received Attribute "priv-lvl=15"
```

The following is an example of how the user AAA authorization debug output should look:

<Output omitted>

```
16:26:47: tty66 AAA/AUTHOR/EXEC (2667327940): Port='tty66'
list='' service=EXEC
16:26:47: AAA/AUTHOR/EXEC: tty66 (2667327940) user='user'
16:26:47: tty66 AAA/AUTHOR/EXEC (2667327940): send AV
service=shell
16:26:47: tty66 AAA/AUTHOR/EXEC (2667327940): send AV cmd*
16:26:47: tty66 AAA/AUTHOR/EXEC (2667327940): found list
"default"
16:26:47: tty66 AAA/AUTHOR/EXEC (2667327940): Method=tacacs+
(tacacs+)
16:26:47: AAA/AUTHOR/TAC+: (2667327940): user=user
16:26:47: AAA/AUTHOR/TAC+: (2667327940): send AV service=shell
16:26:47: AAA/AUTHOR/TAC+: (2667327940): send AV cmd*
16:26:47: AAA/AUTHOR (2667327940): Post authorization status =
PASS_ADD
16:26:47: AAA/AUTHOR/EXEC: Authorization successful
```

<Output omitted>

```
16:28:21: AAA/MEMORY: free_user (0x822A7244) user='user'
ruser='NULL' port='tty6
6' rem_addr='10.5.160.2' authen_type=ASCII service=LOGIN
priv=1
```

- Step 10** Disable AAA authorization debugging at the central router.
- Step 11** Proceed to Task 6.

## Task 6: Configuring and Testing the Central Router AAA EXEC Accounting

This task configures and tests the central router AAA EXEC accounting.

### Exercise Procedure

Complete these steps:

- Step 1** Enable AAA accounting debugging at the central router and observe the debug output while completing the next steps.
- Step 2** Configure the central router to enable AAA accounting for the starting and stopping of EXEC mode processes for the default accounting list. The accounting information should be logged to the Cisco Secure ACS server, where a report will be generated when a user starts and stops the EXEC process where commands are issued.
- Step 3** Establish a Telnet session from the branch router to the central router using the username **user** and the password **letmein**. When the user **user** has been authenticated, EXEC processes are started and will be logged.
- Step 4** Exit to the branch router.
- Step 5** Establish a Telnet session from the branch router the central router using the username **superuser** and the password **root**. Note that the privileged EXEC level is not indicated in the accounting debug output. This result is because the central router has been configured to log only the start and stop of the EXEC process, the equivalent of a user successfully logging into and out of the router.
- Step 6** Verify that as you performed the previous steps, the central site router generated AAA TACACS+ and accounting debug output similar to the following:

```
01:47:51: TAC+: 10.1.0.200 req=62A306A4 Qd id=1071385788
ver=192 handle=0x6298CD54 (ESTAB) expire=5 ACCT/REQUEST/START
queued
01:47:51: TAC+: 10.1.0.200 (1071385788) ACCT/REQUEST/START
queued
01:47:51: TAC+: 10.1.0.200 ESTAB id=1071385788 wrote 78 of 78
bytes
01:47:51: TAC+: 10.1.0.200 req=62A306A4 Qd id=1071385788
ver=192 handle=0x6298CD54 (ESTAB) expire=4 ACCT/REQUEST/START
sent
```

<Output omitted>

```
01:47:51: TAC+: req=62A306A4 Tx id=1071385788 ver=192
handle=0x6298CD54 (ESTAB) expire=4 ACCT/REQUEST/START
processed
01:47:51: TAC+: (1071385788) ACCT/REQUEST/START processed
01:47:51: TAC+: periodic timer stopped (queue empty)
01:47:51: TAC+: (1071385788): received acct response status =
SUCCESS
```



<Output omitted>

```
01:47:57: TAC+: 10.1.0.200 req=62A3036C Qd id=3937240687
ver=192 handle=0x6298D1F0 (ESTAB) expire=5 ACCT/REQUEST/STOP
queued
01:47:57: TAC+: 10.1.0.200 (3937240687) ACCT/REQUEST/STOP
queued
01:47:57: TAC+: 10.1.0.200 ESTAB id=3937240687 wrote 177 of
177 bytes
01:47:57: TAC+: 10.1.0.200 req=62A3036C Qd id=3937240687
ver=192 handle=0x6298D1F0 (ESTAB) expire=4 ACCT/REQUEST/STOP
sent
```

<Output omitted>

```
01:47:57: TAC+: req=62A3036C Tx id=3937240687 ver=192
handle=0x6298D1F0 (ESTAB) expire=4 ACCT/REQUEST/STOP processed
01:47:57: TAC+: (3937240687) ACCT/REQUEST/STOP processed
01:47:57: TAC+: periodic timer stopped (queue empty)
01:47:57: TAC+: (3937240687): received acct response status =
SUCCESS
```

```
15:22:44: AAA/ACCT/EXEC/START User user, port tty66
15:22:44: AAA/ACCT/EXEC: Found list "default"
15:22:44: AAA/ACCT/EXEC/START User user, Port tty66,
task_id=2 timezone=UTC service=shell
15:22:44: AAA/ACCT: user user, acct type 0 (1677691259):
Method=tacacs+ (tacacs)
```

**Step 7** Proceed to Task 7.

## Task 7: Configuring and Testing the Central Router AAA Network Accounting

This task configures and tests the central router AAA network accounting.

### Exercise Procedure

Complete these steps:

- Step 1** Configure the central router to enable AAA accounting for the use of network services for the default accounting list. The accounting information should be logged to the Cisco Secure ACS server, where a report will be generated when a user starts and stops the use of network services.
- Step 2** On the branch router, shut down the WAN interface to the central router and observe the AAA accounting debug output to verify AAA network accounting.
- Step 3** On the branch router, reactivate the WAN interface to the central router and observe the AAA accounting debug output to verify AAA network accounting.
- Step 4** Verify that as you performed the previous steps, the central router generated AAA TACACS+ and accounting debug output similar to the following:

TACACS+ output

```
01:55:40: TAC+: 10.1.0.200 req=62696434 Qd id=3579209361
ver=192 handle=0x62A1B784 (ESTAB) expire=5 ACCT/REQUEST/START
queued
01:55:40: TAC+: 10.1.0.200 (3579209361) ACCT/REQUEST/START
queued
01:55:40: TAC+: 10.1.0.200 ESTAB id=3579209361 wrote 78 of 78
bytes
01:55:40: TAC+: 10.1.0.200 req=62696434 Qd id=3579209361
ver=192 handle=0x62A1B784 (ESTAB) expire=4 ACCT/REQUEST/START
sent
```

<Output omitted>

```
01:55:40: TAC+: req=62696434 Tx id=3579209361 ver=192
handle=0x62A1B784 (ESTAB) expire=4 ACCT/REQUEST/START
processed
01:55:40: TAC+: (3579209361) ACCT/REQUEST/START processed
01:55:40: TAC+: periodic timer stopped (queue empty)
01:55:40: TAC+: (3579209361): received acct response status =
SUCCESS
```

<Output omitted>

```
01:56:19: TAC+: 10.1.0.200 req=626963E0 Qd id=1283237260
ver=192 handle=0x62A1BC20 (ESTAB) expire=5 ACCT/REQUEST/STOP
queued
01:56:19: TAC+: 10.1.0.200 (1283237260) ACCT/REQUEST/STOP
queued
01:56:19: TAC+: 10.1.0.200 req=626963E0 Qd id=1283237260
ver=192 handle=0x62A1BC20 (ESTAB) expire=4 ACCT/REQUEST/STOP
sent
```

<Output omitted>

```
01:56:19: TAC+: req=626963E0 Tx id=1283237260 ver=192
handle=0x62A1BC20 (ESTAB) expire=4 ACCT/REQUEST/STOP processed
01:56:19: TAC+: (1283237260) ACCT/REQUEST/STOP processed
01:56:19: TAC+: periodic timer stopped (queue empty)
01:56:19: TAC+: (1283237260): received acct response status =
SUCCESS
```

<Output omitted>

```
01:56:36: TAC+: 10.1.0.200 req=626963C4 Qd id=1548704104
ver=192 handle=0x62A1C0BC (ESTAB) expire=5 ACCT/REQUEST/STOP
queued
01:56:36: TAC+: 10.1.0.200 (1548704104) ACCT/REQUEST/STOP
queued
01:56:36: TAC+: 10.1.0.200 ESTAB id=1548704104 wrote 366 of
366 bytes
01:56:36: TAC+: 10.1.0.200 req=626963C4 Qd id=1548704104
ver=192 handle=0x62A1C0BC (ESTAB) expire=4 ACCT/REQUEST/STOP
sent
```

The following shows AAA accounting debug output on shutdown:

```
16:17:16: %LINK-3-UPDOWN: Interface Serial0/0, changed state
to down
16:17:16: AAA/ACCT/ACCT_DISC: Found list "default"
16:17:16: Serial0/0 AAA/DISC: 2/"Lost Carrier"
16:17:16: AAA/ACCT/ACCT_DISC: Found list "default"
16:17:16: Serial0/0 AAA/DISC/EXT: 1011/"Lost Carrier"
16:17:16: AAA/ACCT/ACCT_DISC: Found list "default"
16:17:16: Serial0/0 AAA/DISC: 2/"Lost Carrier"
16:17:16: AAA/ACCT/ACCT_DISC: Found list "default"
16:17:16: Serial0/0 AAA/DISC/EXT: 1011/"Lost Carrier"
16:17:16: AAA/ACCT: no attribute "pre-bytes-in" to replace,
adding it
```

```

16:17:16: AAA/ACCT: no attribute "pre-bytes-out" to replace,
adding it
16:17:16: AAA/ACCT: no attribute "pre-paks-in" to replace,
adding it
16:17:16: AAA/ACCT: no attribute "pre-paks-out" to replace,
adding it
16:17:16: AAA/ACCT: no attribute "bytes_in" to replace, adding
it
16:17:16: AAA/ACCT: no attribute "bytes_out" to replace,
adding it
16:17:16: AAA/ACCT: no attribute "paks_in" to replace, adding
it
16:17:16: AAA/ACCT: no attribute "paks_out" to replace, adding
it
16:17:16: AAA/ACCT: no attribute "pre-session-time" to
replace, adding it
16:17:16: AAA/ACCT: no attribute "elapsed_time" to replace,
adding it
16:17:16: AAA/ACCT non-ISDN xmit=0 recv=0 hwidb=823847C4 tty=0
16:17:16: AAA/ACCT/NET/STOP User branch_5, Port Serial0/0:
 task_id=7 timezone=UTC service=ppp protocol=ip
addr=10.5.160.2 disc-cau
se=2 disc-cause-ext=1011 pre-bytes-in=145 pre-bytes-out=133
pre-paks-in=7 pre-pa
ks-out=6 bytes_in=3595 bytes_out=3927 paks_in=153 paks_out=150
pre-session-time=
58031 connect-progress=60 elapsed_time=605 nas-rx-speed=0 nas-
tx-speed=0
16:17:16: AAA/ACCT: user branch_5, acct type 2 (3107486732):
Method=tacacs+ (tac
acs+)

```

The following shows AAA accounting debug output on reactivation:

```

16:21:54: %LINK-3-UPDOWN: Interface Serial0/0, changed state
to up
16:21:54: AAA/ACCT/PROG: Could not determine ds0 to update
Connect Progress
16:21:54: voice_parse_intf_name: Using the old NAS_PORT string
16:21:54: AAA: parse name=Serial0/0 idb type=56 tty=-1
16:21:54: AAA: name=Serial0/0 flags=0x15 type=3 shelf=0 slot=0
adapter=0 port=0
channel=0
16:21:54: voice_parse_intf_name: Using the old NAS_PORT string
16:21:54: AAA: parse name=<no string> idb type=-1 tty=-1
16:21:54: AAA/MEMORY: create_user (0x823E0BB0) user='branch_5'
ruser='NULL' ds0=

```

```

0 port='Serial0/0' rem_addr='' authen_type=CHAP service=PPP
priv=1 initial_task_
id='0'
16:21:54: AAA/MEMORY: free_user (0x823E0BB0) user='branch_5'
ruser='NULL' port='
Serial0/0' rem_addr='' authen_type=CHAP service=PPP priv=1
16:21:54: voice_parse_intf_name: Using the old NAS_PORT string
16:21:54: AAA: parse name=Serial0/0 idb type=56 tty=-1
16:21:54: AAA: name=Serial0/0 flags=0x15 type=3 shelf=0 slot=0
adapter=0 port=0
channel=0
16:21:54: voice_parse_intf_name: Using the old NAS_PORT string
16:21:54: AAA: parse name=<no string> idb type=-1 tty=-1
16:21:54: AAA/MEMORY: create_user (0x823E0BB0) user='branch_5'
ruser='NULL' ds0=
0 port='Serial0/0' rem_addr='' authen_type=CHAP service=PPP
priv=1 initial_task_
id='0'
16:21:54: AAA/ACCT/NET/START User branch_5, Port Serial0/0,
List ""
16:21:54: AAA/ACCT/NET: Found list "default"
16:21:54: AAA/ACCT: no attribute "service" to replace, adding
it
16:21:54: AAA/ACCT/NET/START User branch_5, Port Serial0/0,
task_id=9 timezone=UTC service=ppp
16:21:54: AAA/ACCT: user branch_5, acct type 2 (1512055031):
Method=tacacs+ (tac
acs+)
16:21:54: TAC+: Using default tacacs server-group "tacacs+"
list.
16:21:54: TAC+: Opening TCP/IP to 10.5.0.200/49 timeout=5
16:21:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0
to 67
16:21:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0
to 60
16:21:54: AAA/ACCT: no attribute "protocol" to replace, adding
it
16:21:54: AAA/ACCT: no attribute "addr" to replace, adding it
16:21:54: AAA/ACCT/PROG: Updating Connect Progress for ds0 0
to 60

```

**Step 5** Disable all debugging.

## Exercise Verification

You have completed this exercise when you attain these results:

- You can log in from the branch router using a ACS server to authenticate the username localuser
- You can log in from the branch router using a ACS server to authorize for username user privilege level 1 and superuser privilege level 15
- You can log in from the branch router using a ACS server to send EXEC accounting start-stop messages

Your configuration should have had lines added. On the central router, verify that your configuration contains lines similar to the following:

```
aaa new-model ! Task 1 Step 2
aaa authentication login no_tacacs enable ! Task 1 Step 3

aaa authentication login telnet-order group tacacs+ local
! Task 4 Step 3

aaa authorization exec default group tacacs+
! Task 5 Step 4
aaa accounting exec default start-stop group tacacs+
! Task 6 Step 2
aaa accounting network default start-stop group tacacs+ !
Task 7 Step 1

username localuser password cisco ! Task 3 Step
5

tacacs-server host 10.1.0.200 key cisco ! Task 4 Step
1
radius-server host 10.1.0.200 key cisco ! Task 4 Step
2

line con 0
 login authentication no_tacacs ! Task 1 Step 4

line vty 0 4
 login authentication telnet-order ! Task 4 Step 4
```

# Lab Exercise Answer Key

## Lab Exercise 11-1: Using AAA to Scale Access Control

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1YF.9$X9uj9fWvTn/4BFKlVaSUF.
!
username central_3 password 0 cisco
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface BRI0
no ip address
shutdown
no cdp enable
!
interface FastEthernet0
description This is the ethernet network for the branch
router
ip address 10.3.10.2 255.255.255.0
```

```

speed auto
no cdp enable
!
interface Serial0
description This link goes from branch to central
bandwidth 128
ip address 10.3.160.2 255.255.255.0
encapsulation ppp
no cdp enable
ppp authentication chap
!
interface Serial1
no ip address
shutdown
no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.160.1
no ip http server
ip pim bidir-enable
!
!
no cdp run
!
banner motd ^
Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11
Lab11 Lab11
branch branch branch branch branch branch branch branch

-
Notes from the instructor:
All local passwords should be set to "cisco"

-
branch branch branch branch branch branch branch branch
Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11
Lab11 Lab11
^
!
line con 0
exec-timeout 30 0
logging synchronous level all

```



```
 history size 200
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login
 history size 200
!
end
```

### Central Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
aaa new-model
aaa authentication login no_tacacs enable
aaa authentication login telnet-order group tacacs+ local
aaa authorization exec default group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
enable secret 5 1b8L5$Nd51tIYhJhXnvJVeLQqW..
!
username localuser password 0 cisco
username branch_3 password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
!
call rsvp-sync
!
!
!
!
```

```

!
controller T1 1/0
 framing sf
 linecode ami
!
!
!
interface Ethernet0/0
 description This is the ethernet network for the central
router
 ip address 10.3.0.1 255.255.255.0
 half-duplex
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
 no cdp enable
!
interface Serial3/0
 description This link goes from central to Branch
 bandwidth 128
 ip address 10.3.160.1 255.255.255.0
 encapsulation ppp
 clockrate 128000
 no cdp enable
 ppp authentication chap
!
interface Serial3/1
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/2
 no ip address
 shutdown
 no cdp enable
!
interface Serial3/3
 no ip address

```

```

shutdown
no cdp enable
!
ip classless
no ip http server
!
no cdp run
!
tacacs-server host 10.3.0.200 key cisco
radius-server host 10.3.0.200 auth-port 1645 acct-port 1646
key cisco
radius-server retransmit 3
!
dial-peer cor custom
!
!
!
!
banner motd ^
Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11
Lab11 Lab11
central central central central central central central
central

```

```

-
Notes from the instructor:

```

```

All local passwords should be set to "cisco"

-

```

```

central central central central central central central
central
Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11 Lab11
Lab11 Lab11
^
!
line con 0
exec-timeout 30 0
logging synchronous level all
login authentication no_tacacs
history size 200
line 65 70
flush-at-activation
line aux 0

```

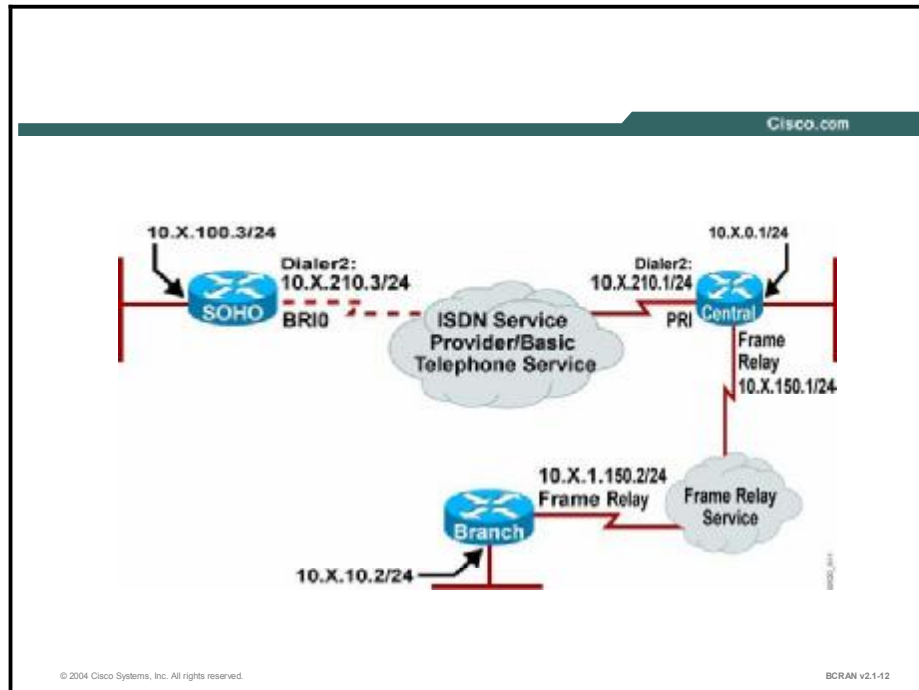
```
line vty 0 4
 exec-timeout 30 0
 password cisco
 logging synchronous
 login authentication telnet-order
 history size 200
!
end
```

# Super Lab

Complete the following lab exercise to practice what you learned in the BCRAN course.

## Visual Objective

The figure displays the configuration that you will complete in this exercise.



## Scenario

A small real estate company called ABC has hired you to set up the network infrastructure. After analyzing the requirements of ABC, you have decided to connect the small office, home office (SOHO) of the owner back to the central office (CO) with an ISDN BRI connection. Frame Relay will connect the ABC branch to the CO. The CO is currently connected to a Frame Relay provider and a serial T1 for ISDN connectivity.

# Setup

Gather the information shown in this table prior to starting this lab.

| Pod Number ____ | Information Required                   | Example (where X is your pod number) all subnet masks are 255.255.255.0 | Write in your information for your pod ____ |
|-----------------|----------------------------------------|-------------------------------------------------------------------------|---------------------------------------------|
| Central Router  | Your (first) LAN interface type        | Ethernet 0/0                                                            |                                             |
| Central Router  | Your (first) LAN interface IP          | 10.X.0.1                                                                |                                             |
| Central Router  | Your (first) ISDN controller           | T1 1/0                                                                  |                                             |
| Central Router  | ISDN interface IP to Branch            | 10.X.200.1                                                              |                                             |
| Central Router  | ISDN switch type                       | primary-5ess                                                            |                                             |
| Central Router  | ISDN Number                            | 555X100                                                                 |                                             |
| Central Router  | Dialer 2 IP to SOHO                    | 10.X.210.1                                                              |                                             |
| Central Router  | Your (second) WAN Interface Type       | Serial 0/1<br>Serial 3/1                                                |                                             |
| Central Router  | Your (second) WAN Interface IP Address | 10.X.150.1                                                              |                                             |
| Central Router  | Frame-Rely DLCI                        | X12                                                                     |                                             |
| Branch Router   | Your (first) LAN interface type        | FastEthernet0                                                           |                                             |
| Branch Router   | Your (first) LAN interface IP          | 10.X.10.2                                                               |                                             |
| Branch Router   | Your (second) WAN Interface Type       | Serial 1                                                                |                                             |
| Branch Router   | Your (second) WAN Interface IP Address | 10.X.150.2                                                              |                                             |
| Branch Router   | Frame-Rely DLCI                        | X21                                                                     |                                             |
| SOHO Router     | Your (first) LAN interface type        | Ethernet 0                                                              |                                             |
| SOHO Router     | Your (first) LAN interface IP          | 10.X.100.3                                                              |                                             |
| SOHO Router     | ISDN switch type                       | basic-5ess                                                              |                                             |
| SOHO Router     | Your (first) ISDN interface type       | Bri0                                                                    |                                             |
| SOHO Router     | ISDN Number                            | 555X300                                                                 |                                             |
| SOHO Router     | Dialer 2 IP to Central                 | 10.X.210.3                                                              |                                             |
| SOHO Router     | initial config file name               | pXc10                                                                   | □                                           |

## Setup Tasks

From your PC, Telnet to the terminal server and open a console connection to the branch router of your pod.

From your PC, Telnet to the terminal server again and open a second console connection to the central router of your pod.

You will now be able to configure and observe output on both routers simultaneously.

Erase the central, branch, and SOHO routers and reload the routers.

## Task 1: Basic Configuration Considerations

Properly configure your routers for identification, connectivity, and basic authentication access. For this task and the following tasks, all local passwords should be set to “cisco” and names should follow the conventions that have been used throughout the course labs. To limit the number of typos and misconfiguration, it may be wise not to make use of capitalization or unusual characters, and to keep names simple and provide meaningful descriptions on interfaces.

## Task 2: Frame Relay Considerations

Because of the possibility of future expansion of additional branch offices, you have to implement Frame Relay using point-to-point subinterfaces. You would also like to ensure that traffic shaping is enabled to respond to backward explicit congestion notification (BECN). When configuring traffic shaping, keep in mind that the CO uses a link speed of 128 kbps and the branch office uses a link speed of 32 kbps, and that there are defaults that may or may not be suitable for your WAN network.

## Task 3: ISDN Considerations

Because of the possibility of future expansion of ABC, you will implement dialer profiles for the connections between the SOHO and CO.

The connection between the CO and SOHO will use CHAP authentication.

## Task 4: Routing Considerations

It is not necessary for the branch and SOHO users to have IP connectivity between each other.

Because of the limited bandwidth on the ISDN connection between the SOHO and central router, do not use a routing protocol between these sites. (Hint: You will need only one static route at the SOHO and the central router.)

Use Enhanced Interior Gateway Routing Protocol (EIGRP) with an autonomous system (AS) of 100 between the branch and central sites. Ensure that the dialer interface between the central and SOHO routers is not brought up by an EIGRP broadcast. (Hint: How do you suppress a routing update on an interface?) Also, you will want to ensure that EIGRP does not automatically summarize the routes.

## Task 5: Bandwidth Considerations

ABC is concerned about critical web traffic from the central site, so it was decided that at least 50 percent of the Frame Relay bandwidth be guaranteed for web traffic. Create and enforce a policy to meet this requirement.

## Task 6: Security Considerations

ABC has critical applications that are used between the branch and CO networks. It wishes to use IP Security (IPSEC) to secure transmissions between the branch and central LAN subnets. It has been agreed that Internet Security Association and Key Management Protocol (ISAKMP) will be used for key negotiations, Data Encryption Standard (DES) will be used for encryption, Secure Hash Algorithm 1 (SHA-1) will be used as the hash algorithm, and a preshared key will accomplish the authentication. IPSEC will use Encapsulating Security Payload (ESP) with DES encryption.

## Exercise Verification

You have completed this lab exercise if you were able to accomplish the following:

1. From the SOHO router, you can successfully execute an extended ping (using the SOHO LAN interface IP as the source) to the LAN interface IP of the central router.
2. From the branch router, you can successfully execute an extended ping (using the branch LAN interface IP as the source) to the LAN interface IP of the central router.
3. At the central router, use the **show frame-relay pvc** command and verify that traffic shaping is enabled for BECN.
4. At the central router, you can verify that HTTP traffic is configured to receive 50 percent of the Frame Relay bandwidth.
5. At the central router, you can successfully execute an extended ping between the LAN interface IP addresses. A security association will be established.



# Lab Exercise Answer Key

## Super Lab

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod.

### Branch Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname branch_3
!
enable secret 5 1CW/6$iGU8nsLWMUIJzZaWeLlPS0
!
memory-size iomem 25
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 100
 authentication pre-share
crypto isakmp key cisco1234 address 10.3.150.1
!
!
crypto ipsec transform-set myset esp-des
!
crypto map mymap 110 ipsec-isakmp
 set peer 10.3.150.1
 set transform-set myset
 match address 101
!
!
```

```

!
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 ip address 10.3.10.2 255.255.255.0
 speed auto
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 description This is the Frame Relay interface to the Frame
 Relay switch
 bandwidth 32
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay class shape
 frame-relay traffic-shaping
!
interface Serial1.1 point-to-point
 description This is the Frame Relay PVC to Central
 ip address 10.3.150.2 255.255.255.0
 frame-relay interface-dlci 321
 crypto map mymap
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
ip pim bidir-enable
!
!

```

```

!
map-class frame-relay shape
 frame-relay cir 28000
 frame-relay be 32000
 frame-relay adaptive-shaping becn
access-list 101 permit ip 10.3.10.0 0.0.0.255 10.3.0.0
0.0.0.255
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

### Central Router End Configuration

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname central_3
!
enable secret 5 1dABY$iojW6oyFakgbawg.8TJDM0
!
username soho_3 password 0 cisco
ip subnet-zero
!
!
!
!
class-map match-all web
 match access-group 100
!
!
policy-map outbound-q
 class web
 bandwidth percent 50
!
!

```

```

crypto isakmp policy 100
 authentication pre-share
crypto isakmp key cisco1234 address 10.3.150.2
!
!
crypto ipsec transform-set myset esp-des
!
crypto map mymap 110 ipsec-isakmp
 set peer 10.3.150.2
 set transform-set myset
 match address 101
!
isdn switch-type primary-5ess
call rsvp-sync
!
!
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
!
interface Ethernet0/0
 ip address 10.3.0.1 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial1/0:23
 no ip address
 encapsulation ppp
 dialer pool-member 2

```

```

 isdn switch-type primary-5ess
 ppp authentication chap
!
interface Serial3/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial3/1
 description This is the Frame Relay interface to the Frame
 Relay switch.
 bandwidth 128
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay class shape
 frame-relay traffic-shaping
!
interface Serial3/1.1 point-to-point
 description This is the Frame Relay PVC to Branch
 ip address 10.3.150.1 255.255.255.0
 frame-relay interface-dlci 312
 crypto map mymap
!
interface Serial3/2
 no ip address
 shutdown
!
interface Serial3/3
 no ip address
 shutdown
!
interface Dialer2
 description This the Dialer to SOHO
 ip address 10.3.210.1 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer remote-name soho_3
 dialer string 5553300
 dialer-group 1
 ppp authentication chap

```

```
!
router eigrp 100
 passive-interface Dialer2
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 10.3.100.0 255.255.255.0 10.3.210.3
ip http server
!
!
map-class frame-relay shape
 frame-relay cir 96000
 frame-relay be 128000
 frame-relay adaptive-shaping becn
 service-policy output outbound-q
access-list 100 permit tcp any eq www any
access-list 101 permit ip 10.3.0.0 0.0.0.255 10.3.10.0
0.0.0.255
dialer-list 1 protocol ip permit
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
line 65 70
 flush-at-activation
line aux 0
line vty 0 4
!
end
```

## SOHO Router End Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname soho_3
!
enable secret 5 1QJ1/$rtAvmCRB9R4rhstjClG5//
!
username central_3 password 0 cisco
ip subnet-zero
!
isdn switch-type basic-5ess
!
!
!
!
interface Ethernet0
 ip address 10.3.100.3 255.255.255.0
!
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 2
 isdn switch-type basic-5ess
 ppp authentication chap
!
interface Dialer2
 ip address 10.3.210.3 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer remote-name central_3
 dialer string 5553100
 dialer-group 1
 ppp authentication chap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.210.1
no ip http server
```

```
!
!
line con 0
line vty 0 4
!
end
```