Connecting Networks v6

Companion Guide

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Connecting Networks v6 Companion Guide

Cisco Networking Academy

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing September 2017

Library of Congress Control Number: 2017950140

ISBN-13: 978-1-58713-432-6

ISBN-10: 1-58713-432-2

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Connecting Networks course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.netacad.com

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Ron Fligge

Product Line Manager
Brett Bartow

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Christopher Cleveland

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Technical Editor
Rick McDonald

Editorial Assistant
Vanessa Evans

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Lisa Stumpf

Proofreader
H S Rupa

Trademark Acknowledgments

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

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

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

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

We greatly appreciate your assistance.

CISCO™

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Contributing Authors

Bob Vachon is a professor at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. Since 2002, he has collaborated on various CCNA, CCNA Security, CCNP, Cybersecurity, and IoT projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing guitar and being outdoors.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an MEd in training and development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as Curriculum Lead.

Contents at a Glance

Introduction xix

Chapter 1 WAN Concepts 1

Chapter 2 Point-to-Point Connections 49

Chapter 3 Branch Connections 101

Chapter 4 Access Control Lists 155

Chapter 5 Network Security and Monitoring 215

Chapter 6 Quality of Service 269

Chapter 7 Network Evolution 303

Chapter 8 Network Troubleshooting 347

Appendix A Answers to the “Check Your Understanding” Questions 431

Glossary 443

Index 471

Contents

Introduction xix

Chapter 1 WAN Concepts 1

Objectives 1

Key Terms 1

Introduction (1.0) 3

WAN Technologies Overview (1.1) 3

Purpose of WANs (1.1.1) 3

Why a WAN? (1.1.1.1) 3
Are WANs Necessary? (1.1.1.2) 4
WAN Topologies (1.1.1.3) 5
Evolving Networks (1.1.1.4) 8
Small Office (1.1.1.5) 8
Campus Network (1.1.1.6) 9
Branch Networks (1.1.1.7) 10
Distributed Network (1.1.1.8) 11

WAN Operations (1.1.2) 13

WANs in the OSI Model (1.1.2.1) 13
Common WAN Terminology (1.1.2.2) 14
WAN Devices (1.1.2.3) 16
Circuit Switching (1.1.2.4) 17
Packet Switching (1.1.2.5) 18

Selecting a WAN Technology (1.2) 20

WAN Services (1.2.1) 20

WAN Link Connection Options (1.2.1.1) 20
Service Provider Network Infrastructure (1.2.1.2) 21

Private WAN Infrastructures (1.2.2) 23

Leased Lines (1.2.2.1) 23
Dialup (1.2.2.2) 25
ISDN (1.2.2.3) 26
Frame Relay (1.2.2.4) 28
ATM (1.2.2.5) 29
Ethernet WAN (1.2.2.6) 30
MPLS (1.2.2.7) 32
VSAT (1.2.2.8) 32

Public WAN Infrastructure (1.2.3) 33

DSL (1.2.3.1) 34
Cable (1.2.3.2) 35

Wireless (1.2.3.3) 36
3G/4G Cellular (1.2.3.4) 37
VPN Technology (1.2.3.5) 38

Selecting WAN Services (1.2.4) 39

Choosing a WAN Link Connection (1.2.4.1) 40
Choosing a WAN Link Connection (Cont.) (1.2.4.2) 41

Summary (1.3) 43

Practice 44

Check Your Understanding Questions 44

Chapter 2 Point-to-Point Connections 49

Objectives 49

Key Terms 49

Introduction (2.0) 51

Serial Point-to-Point Overview (2.1) 51

Serial Communications (2.1.1) 52

Serial and Parallel Ports (2.1.1.1) 52
Point-to-Point Communication Links (2.1.1.2) 53
Serial Bandwidth (2.1.1.3) 54

HDLC Encapsulation (2.1.2) 56

WAN Encapsulation Protocols (2.1.2.1) 56
HDLC Encapsulation (2.1.2.2) 57
Configuring HDLC Encapsulation (2.1.2.3) 58
Troubleshooting a Serial Interface (2.1.2.4) 59

PPP Operation (2.2) 63

Benefits of PPP (2.2.1) 63

Introducing PPP (2.2.1.1) 64
Advantages of PPP (2.2.1.2) 65

LCP and NCP (2.2.2) 65

PPP-Layered Architecture (2.2.2.1) 65
PPP: Link Control Protocol (LCP) (2.2.2.2) 66
PPP: Network Control Protocol (NCP) (2.2.2.3) 66
PPP Frame Structure (2.2.2.4) 67

PPP Sessions (2.2.3) 68

Establishing a PPP Session (2.2.3.1) 68
LCP Operation (2.2.3.2) 69
PPP Configuration Options (2.2.3.3) 72
NCP Explained (2.2.3.4) 72

PPP Implementation (2.3) 74

Configure PPP (2.3.1) 74

PPP Configuration Options (2.3.1.1) 74
PPP Basic Configuration Command (2.3.1.2) 76
PPP Compression Commands (2.3.1.3) 76
PPP Link Quality Monitoring Command (2.3.1.4) 77
PPP Multilink Commands (2.3.1.5) 78
Verifying PPP Configuration (2.3.1.6) 81

Configure PPP Authentication (2.3.2) 82

PPP Authentication Protocols (2.3.2.1) 83
Password Authentication Protocol (PAP) (2.3.2.2) 83
Challenge Handshake Authentication Protocol (CHAP) (2.3.2.3) 85
PPP Authentication Command (2.3.2.4) 86
Configuring PPP with Authentication (2.3.2.5) 87

Troubleshoot WAN Connectivity (2.4) 89

Troubleshoot PPP (2.4.1) 89

Troubleshooting PPP Serial Encapsulation (2.4.1.1) 90
Debugging PPP (2.4.1.2) 91
Troubleshooting a PPP Configuration with Authentication (2.4.1.3) 94

Summary 96

Practice 97

Check Your Understanding Questions 98

Chapter 3 Branch Connections 101

Objectives 101

Key Terms 101

Introduction (3.0) 103

Remote-Access Connections (3.1) 104

Broadband Connections (3.1.1) 104

What Is a Cable System? (3.1.1.1) 104
Cable Components (3.1.1.2) 105
What Is DSL? (3.1.1.3) 107
DSL Connections (3.1.1.4) 107
Wireless Connection (3.1.1.5) 109

Select a Broadband Connection (3.1.2) 112

Comparing Broadband Solutions (3.1.2.1) 112

PPPoE (3.2) 113

PPPoE Overview (3.2.1) 113

PPPoE Motivation (3.2.1.1) 113
PPPoE Concepts (3.2.1.2) 114

Implement PPPoE (3.2.2) 115

PPPoE Configuration (3.2.2.1) 115
PPPoE Verification (3.2.2.2) 116
PPPoE Troubleshooting (3.2.2.3) 118
PPPoE Negotiation (3.2.2.4) 118
PPPoE Authentication (3.2.2.5) 119
PPPoE MTU Size (3.2.2.6) 120

VPNs (3.3) 122

Fundamentals of VPNs (3.3.1) 122

Introducing VPNs (3.3.1.1) 123
Benefits of VPNs (3.3.1.2) 124

Types of VPNs (3.3.2) 125

Site-to-Site VPNs (3.3.2.1) 125
Remote-Access VPNs (3.3.2.2) 126
DMVPN (3.3.2.3) 127

GRE (3.4) 128

GRE Overview (3.4.1) 129

GRE Introduction (3.4.1.1) 129
GRE Characteristics (3.4.1.2) 130

Implement GRE (3.4.2) 131

Configure GRE (3.4.2.1) 131
Verify GRE (3.4.2.2) 133
Troubleshoot GRE (3.4.2.3) 134

eBGP (3.5) 136

BGP Overview (3.5.1) 136

IGP and EGP Routing Protocols (3.5.1.1) 137
eBGP and iBGP (3.5.1.2) 138

BGP Design Considerations (3.5.2) 139

When to Use BGP (3.5.2.1) 139
When Not to Use BGP (3.5.2.2) 140
BGP Options (3.5.2.3) 140

eBGP Branch Configuration (3.5.3) 142

Steps to Configure eBGP (3.5.3.1) 142
BGP Sample Configuration (3.5.3.2) 143
Verify eBGP (3.5.3.3) 145

Summary (3.6) 148

Practice 149

Check Your Understanding Questions 150

Chapter 4 Access Control Lists 155

Objectives 155

Key Terms 155

Introduction (4.0.1.1) 156

Standard ACL Operation and Configuration Review (4.1) 156

ACL Operation Overview (4.1.1) 156

ACLs and the Wildcard Mask (4.1.1.1) 156

Applying ACLs to an Interface (4.1.1.2) 158

A TCP Conversation (4.1.1.3) 159

ACL Packet Filtering (4.1.1.4) 160

Types of IPv4 ACLs (4.1.2) 162

Standard and Extended IPv4 ACLs (4.1.2.1) 162

Numbered and Named ACLs (4.1.2.2) 163

Where to Place ACLs (4.1.2.3) 163

Standard ACL Placement Example (4.1.2.4) 165

Extended ACL Placement Example (4.1.2.5) 166

Standard IPv4 ACL Implementation (4.1.3) 167

Configure a Standard IPv4 ACL (4.1.3.1) 167

Apply a Standard IPv4 ACL (4.1.3.2) 169

Standard Named IPv4 ACLs (4.1.3.3) 170

Verify ACLs (4.1.3.4) 171

Extended IPv4 ACLs (4.2) 173

Structure of an Extended IPv4 ACLs (4.2.1) 173

Extended ACLs (4.2.1.1) 173

Filtering Ports and Services (4.2.1.2) 173

Configure Extended IPv4 ACLs (4.2.2) 175

Configuring Extended ACLs (4.2.2.1) 175

Applying Extended ACLs to Interfaces (4.2.2.2) 177

Filtering Traffic with Extended ACLs (4.2.2.3) 178

Creating Extended Named ACLs (4.2.2.4) 180

Verifying Extended ACLs (4.2.2.5) 181

Editing Extended ACLs (4.2.2.6) 182

IPv6 ACLs (4.3) 184

IPv6 ACL Creation (4.3.1) 184

Types of IPv6 ACLs (4.3.1.1) 184

Comparing IPv4 and IPv6 ACLs (4.3.1.2) 185

Configuring IPv6 ACLs (4.3.2) 186

Configuring IPv6 Topology (4.3.2.1) 186

Configuring IPv6 ACLs (4.3.2.2) 188

Applying an IPv6 ACL to an Interface (4.3.2.3) 189

IPv6 ACL Examples (4.3.2.4) 190
Verifying IPv6 ACLs (4.3.2.5) 192

Troubleshoot ACLs (4.4) 194

Processing Packets with ACLs (4.4.1) 194

Inbound and Outbound ACL Logic (4.4.1.1) 194
ACL Logic Operations (4.4.1.2) 195
Standard ACL Decision Process (4.4.1.3) 196
Extended ACL Decision Process (4.4.1.4) 197

Common ACL Errors (4.4.2) 197

Troubleshooting IPv4 ACLs: Example 1 (4.4.2.1) 197
Troubleshooting IPv4 ACLs: Example 2 (4.4.2.2) 198
Troubleshooting IPv4 ACLs: Example 3 (4.4.2.3) 199
Troubleshooting IPv4 ACLs: Example 4 (4.4.2.4) 200
Troubleshooting IPv4 ACLs: Example 5 (4.4.2.5) 200
Troubleshooting IPv6 ACLs: Example 1 (4.4.2.6) 201
Troubleshooting IPv6 ACLs: Example 2 (4.4.2.7) 203
Troubleshooting IPv6 ACLs: Example 3 (4.4.2.8) 205

Summary (4.5) 208

Practice 209

Check Your Understanding Questions 210

Chapter 5 Network Security and Monitoring 215

Objectives 215

Key Terms 215

Introduction (5.0.1.1) 217

LAN Security (5.1) 217

LAN Security Attacks (5.1.1) 218

Common LAN Attacks (5.1.1.1) 218
CDP Reconnaissance Attack (5.1.1.2) 219
Telnet Attacks (5.1.1.3) 220
MAC Address Table Flooding Attack (5.1.1.4) 222
VLAN Attacks (5.1.1.5) 225
DHCP Attacks (5.1.1.6) 226

LAN Security Best Practices (5.1.2) 227

Secure the LAN (5.1.2.1) 227
Mitigate MAC Address Flooding Table Attacks (5.1.2.2) 228
Mitigate VLAN Attacks (5.1.2.3) 229
Mitigate DHCP Attacks (5.1.2.4) 230
Secure Administrative Access Using AAA (5.1.2.5) 231
Secure Device Access Using 802.1X (5.1.2.6) 233

SNMP (5.2) 234

SNMP Operation (5.2.1) 234

Introduction to SNMP (5.2.1.1) 235
SNMP Operation (5.2.1.2) 236
SNMP Agent Traps (5.2.1.3) 237
SNMP Versions (5.2.1.4) 238
Community Strings (5.2.1.5) 241
Management Information Base Object ID (5.2.1.6) 243
SNMPv3 (5.2.1.7) 246

Configuring SNMP (5.2.2) 248

Steps for Configuring SNMP (5.2.2.1) 248
Verifying SNMP Configuration (5.2.2.2) 249
SNMP Best Practices (5.2.2.3) 252
Steps for Configuring SNMPv3 (5.2.2.4) 254
Verifying SNMPv3 Configuration (5.2.2.5) 254

Cisco Switch Port Analyzer (5.3) 255

SPAN Overview (5.3.1) 256

Port Mirroring (5.3.1.1) 256
Analyzing Suspicious Traffic (5.3.1.2) 257
Local SPAN (5.3.1.3) 257
Remote SPAN (5.3.1.4) 259

SPAN Configuration (5.3.2) 260

Configuring Local SPAN (5.3.2.1) 260
Verifying Local SPAN (5.3.2.2) 261

SPAN as a Troubleshooting Tool (5.3.3) 262

Troubleshooting with SPAN Overview (5.3.3.1) 262

Summary (5.4) 264

Practice 264

Check Your Understanding Questions 265

Chapter 6 Quality of Service 269

Objectives 269

Key Terms 269

Introduction (6.0.1.1) 271

QoS Overview (6.1) 271

Network Transmission Quality (6.1.1) 271

Prioritizing Traffic (6.1.1.1) 271
Bandwidth, Congestion, Delay, and Jitter (6.1.1.2) 272
Packet Loss (6.1.1.3) 273

Traffic Characteristics (6.1.2) 275

Network Traffic Trends (6.1.2.1) 275
Voice (6.1.2.2) 276
Video (6.1.2.3) 276
Data (6.1.2.4) 277

Queueing Algorithms (6.1.3) 278

Queuing Overview (6.1.3.1) 279
First-In First-Out (FIFO) (6.1.3.2) 279
Weighted Fair Queuing (WFQ) (6.1.3.3) 280
Class-Based Weighted Fair Queuing (CBWFQ) (6.1.3.4) 281
Low Latency Queuing (LLQ) (6.1.3.5) 282

QoS Mechanisms (6.2) 283

QoS Models (6.2.1) 283

Selecting an Appropriate QoS Policy Model (6.2.1.1) 283
Best Effort (6.2.1.2) 284
Integrated Services (6.2.1.3) 285
Differentiated Services (6.2.1.4) 286

QoS Implementation Techniques (6.2.2) 288

Avoiding Packet Loss (6.2.2.1) 288
QoS Tools (6.2.2.2) 289
Classification and Marking (6.2.2.3) 290
Marking at Layer 2 (6.2.2.4) 291
Marking at Layer 3 (6.2.2.5) 292
Trust Boundaries (6.2.2.6) 295
Congestion Avoidance (6.2.2.7) 296
Shaping and Policing (6.2.2.8) 297

Summary (6.3) 299

Practice 300

Check Your Understanding Questions 300

Chapter 7 Network Evolution 303

Objectives 303

Key Terms 303

Introduction (7.0.1.1) 305

Internet of Things (7.1) 305

IoT Elements (7.1.1) 305

What Is the IoT? (7.1.1.1) 305
The Converged Network and Things (7.1.1.2) 305
Challenges to Connecting Things (7.1.1.3) 306
The Six Pillars of the Cisco IoT System (7.1.1.4) 307

IoT Pillars (7.1.2) 307

The Network Connectivity Pillar (7.1.2.1) 308
The Fog Computing Pillar (7.1.2.2) 308
The Security Pillar (7.1.2.3) 311
Data Analytics Pillar (7.1.2.4) 312
Management and Automation Pillar (7.1.2.5) 313
Application Enablement Platform Pillar (7.1.2.6) 313

Cloud and Virtualization (7.2) 314

Cloud Computing (7.2.1) 314

Cloud Overview (7.2.1.2) 314
Cloud Services (7.2.1.3) 315
Cloud Models (7.2.1.4) 315
Cloud Computing versus Data Center (7.2.1.5) 316

Virtualization (7.2.2) 317

Cloud Computing and Virtualization (7.2.2.1) 317
Dedicated Servers (7.2.2.2) 318
Server Virtualization (7.2.2.3) 319
Advantages of Virtualization (7.2.2.4) 320
Abstraction Layers (7.2.2.5) 321
Type 2 Hypervisors (7.2.2.6) 321

Virtual Network Infrastructure (7.2.3) 323

Type 1 Hypervisors (7.2.3.1) 323
Installing a VM on a Hypervisor (7.2.3.2) 324
Network Virtualization (7.2.3.3) 324

Network Programming (7.3) 326

Software-Defined Networking (7.3.1) 326

Control Plane and Data Plane (7.3.1.1) 326
Virtualizing the Network (7.3.1.2) 327
SDN Architecture (7.3.1.3) 329

Controllers (7.3.2) 331

SDN Controller and Operations (7.3.2.1) 331
Cisco Application Centric Infrastructure (7.3.2.2) 332
Core Components of ACI (7.3.2.3) 332
Spine-Leaf Topology (7.3.2.4) 333
SDN Types (7.3.2.5) 334
APIC-EM Features (7.3.2.6) 336
APIC-EM ACL Analysis (7.3.2.7) 337

Summary (7.4) 340

Practice 341

Check Your Understanding Questions 341

Chapter 8 Network Troubleshooting 347

Objectives 347

Key Terms 347

Introduction (8.0.1.1) 349

Troubleshooting Methodology (8.1) 349

Network Documentation (8.1.1) 349

Documenting the Network (8.1.1.1) 349

Network Topology Diagrams (8.1.1.2) 352

Establishing a Network Baseline (8.1.1.3) 355

Steps to Establish a Network Baseline (8.1.1.4) 355

Measuring Data (8.1.1.5) 358

Troubleshooting Process (8.1.2) 360

General Troubleshooting Procedures (8.1.2.1) 360

Gathering Symptoms (8.1.2.2) 362

Questioning End Users (8.1.2.3) 364

Isolating the Issue Using Layered Models (8.1.3) 365

Using Layered Models for Troubleshooting (8.1.3.1) 365

Troubleshooting Methods (8.1.3.2) 367

Other Troubleshooting Methods (8.1.3.3) 370

Guidelines for Selecting a Troubleshooting Method (8.1.3.4) 371

Troubleshooting Scenarios (8.2) 372

Using IP SLA (8.2.1) 372

IP SLA Concepts (8.2.1.1) 372

IP SLA Configuration (8.2.1.2) 373

Sample IP SLA Configuration (8.2.1.3) 375

Verifying an IP SLA Configuration (8.2.1.4) 376

Troubleshooting Tools (8.2.2) 377

Software Troubleshooting Tools (8.2.2.1) 377

Protocol Analyzers (8.2.2.2) 379

Hardware Troubleshooting Tools (8.2.2.3) 380

Using a Syslog Server for Troubleshooting (8.2.2.4) 385

Symptoms and Causes of Network Troubleshooting (8.2.3) 387

Physical Layer Troubleshooting (8.2.3.1) 387

Data Link Layer Troubleshooting (8.2.3.2) 390

Network Layer Troubleshooting (8.2.3.3) 392

Transport Layer Troubleshooting: ACLs (8.2.3.4) 394

Transport Layer Troubleshooting: NAT for IPv4 (8.2.3.5) 396

Application Layer Troubleshooting (8.2.3.6) 397

Troubleshooting IP Connectivity (8.2.4) 398

Components of Troubleshooting End-to-End Connectivity (8.2.4.1) 398

End-to-End Connectivity Problem Initiates Troubleshooting (8.2.4.2) 400

Step 1: Verify the Physical Layer (8.2.4.3) 402

Step 2: Check for Duplex Mismatches (8.2.4.4) 404

Step 3: Verify Layer 2 and Layer 3 Addressing on the Local Network (8.2.4.5) 406

Step 4: Verify Default Gateway (8.2.4.6) 411

Step 5: Verify Correct Path (8.2.4.7) 415

Step 6: Verify the Transport Layer (8.2.4.8) 418

Step 7: Verify ACLs (8.2.4.9) 420

Step 8: Verify DNS (8.2.4.10) 422

Summary (8.3) 425

Practice 426

Check Your Understanding Questions 427

Appendix A Answers to the "Check Your Understanding" Questions 431

Glossary 443

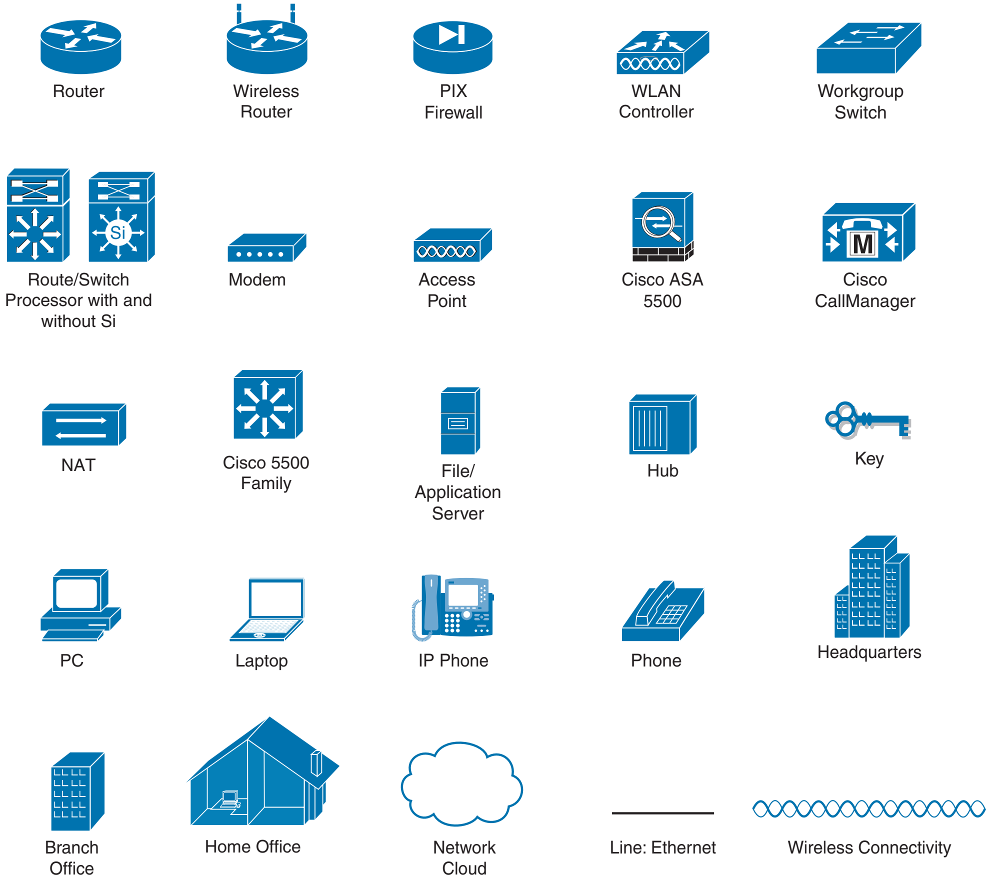
Index 471

Reader Services

Register your copy at www.ciscopress.com/title/9781587134326 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587134326 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Connecting Networks v6 Companion Guide is the official supplemental textbook for the Cisco Network Academy CCNA Connecting Networks course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses, as well as enterprise and service provider environments.

This textbook provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses, and preparation for the CCNA Routing and Switching certification.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the Companion Guide encourages you to think about finding the answers as you read the chapter.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of chapter, there is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with 347 terms.

Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

Packet Tracer ☐ Activity

Video

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, a practice section collects a list of all the labs and activities to provide practice with the topics introduced in this chapter. The labs, class activities, and Packet Tracer instructions are available in the companion *Connecting Networks v6 Labs & Study Guide* (ISBN 9781587134296). The Packet Tracer PKA files are found in the online course.
- **Page references to online course:** After headings, you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

Lab Study Guide

The supplementary book *Connecting Networks v6 Labs & Study Guide*, by Allan Johnson (ISBN 9781587134296), includes a Study Guide section and a Lab section for each chapter. The Study Guide section offers exercises that help you learn the concepts, configurations, and troubleshooting skills crucial to your success as a CCNA exam candidate. Some chapters include unique Packet Tracer activities available for download from the book's companion website. The Labs and Activities section contains all the labs, class activities, and Packet Tracer instructions from the course.

Packet Tracer ☐ Activity

About Packet Tracer Software and Activities

Interspersed throughout the chapters, you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Academy Introduction to Networking course and is divided into eight chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "WAN Concepts":** This chapter discusses basic WAN operations and services including private and public WAN technologies. It also discusses how to select the appropriate WAN protocol and service for a specific network requirement.

- **Chapter 2, "Point-to-Point Connections":** This chapter examines point-to-point serial communications using the PPP and HDLC protocols. It describes the features and benefits of PPP over HDLC and examines the PPP-layered architecture and the functions of LCP and NCP. PPP configuration and PPP authentication commands are also covered.
- **Chapter 3, "Branch Connections":** This chapter discusses how users and enterprises connect to the Internet using cable, DSL, and wireless broadband solutions. It explains how ISPs use PPPoE to provide the authentication, accounting, and link management features to their customers. It introduces how VPNs are implemented to address Internet security concerns and how GRE is used to create a virtual point-to-point connection between two remote points. Finally, the chapter discusses BGP as the routing protocol used between service providers and how to implement BGP on a single-homed network.
- **Chapter 4, "Access Control Lists":** This chapter describes how to use ACLs to filter traffic. Configuration, verification, and troubleshooting of standard and extended IPv4 ACLs are covered. Securing remote access with an ACL is also discussed.
- **Chapter 5, "Network Security and Monitoring":** This chapter discusses common Layer 2 network attacks and how they can be mitigated. Network monitoring is discussed next using SNMP. Finally, SPAN is discussed to provide network traffic mirroring to packet analyzers or IPS devices.
- **Chapter 6, "Quality of Service":** This chapter discusses QoS tools used to guarantee that certain traffic types are prioritized over traffic that is not as time-sensitive. Specifically, the chapter describes network transmission quality, traffic characteristics, queueing algorithms, QoS models, and QoS implementation techniques.
- **Chapter 7, "Network Evolution":** This chapter discusses how network must evolve to support new technology such as the IoT using innovative new technology including cloud computing, virtualization, and SDN.
- **Chapter 8, "Network Troubleshooting":** This chapter discusses how network documentation is used to troubleshoot network issues. It describes the general troubleshooting problems using a systematic layered approach to troubleshooting.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The glossary provides you with definitions for all the key terms identified in each chapter.

CHAPTER 1

WAN Concepts

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What is the purpose of a WAN?
- How do WANs operate?
- What WAN services are available?
- What are the differences between private WAN technologies?
- What are the differences between public WAN technologies?
- What is the appropriate WAN protocol and service for a specific network requirement?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

service provider   *Page 4*

point-to-point topology   *Page 5*

hub-and-spoke topology   *Page 5*

full mesh topology   *Page 5*

dual-homed topology   *Page 5*

leased line   *Page 5*

T1   *Page 5*

E1   *Page 5*

hub   *Page 6*

single-homed topology   *Page 7*

voice over IP (VoIP)   *Page 9*

broadband service   *Page 9*

digital subscriber line (DSL)   *Page 9*

dedicated lines   *Page 11*

enterprise network   *Page 11*

teleworking   *Page 12*

virtual private networks (VPNs)   *Page 12*

Telecommunications Industry Association (TIA)   *Page 13*

Electronic Industries Alliance (EIA)   *Page 13*

International Organization for Standardization (ISO)   *Page 13*

Institute of Electrical and Electronics Engineers (IEEE)   *Page 13*

Point-to-Point Protocol (PPP)   *Page 14*

Frame Relay   *Page 14*

Asynchronous Transfer Mode (ATM)   *Page 14*

High-Level Data Link Control (HDLC)   *Page 14*

customer premises equipment (CPE)   *Page 14*

data communications equipment (DCE)   *Page 15*

data terminal equipment (DTE)   *Page 15*

demarcation point   *Page 15*

local loop   *Page 15*

last-mile Page 15

central office (CO) Page 15

toll network Page 16

dialup modem Page 16

modulates Page 16

demodulates Page 16

Access server Page 16

broadband modem Page 16

channel service unit/data service unit (CSU/DSU) Page 17

WAN switch Page 17

circuit-switched network Page 17

public switched telephone network (PSTN) Page 18

Integrated Services Digital Network (ISDN) Page 18

packet-switched network (PSN) Page 18

virtual circuit (VC) Page 19

data-link connection identifiers (DLCIs) Page 19

latency Page 19

jitter Page 19

private WAN infrastructure Page 21

public WAN infrastructure Page 21

broadband connections Page 21

Synchronous Optical Networking (SONET) Page 22

Synchronous Digital Hierarchy (SDH) Page 22

light-emitting diodes (LEDs) Page 22

dense wavelength division multiplexing (DWDM) Page 22

multiplex Page 22

E3 Page 24

optical carrier (OC) Page 24

time-division multiplexed (TDM) Page 26

Basic Rate Interface (BRI) Page 26

Primary Rate Interface (PRI) Page 27

nonbroadcast multi-access (NBMA) Page 28

permanent virtual circuits (PVCs) Page 28

Metropolitan Ethernet (MetroE) Page 30

Ethernet over MPLS (EoMPLS) Page 31

Virtual Private LAN Service (VPLS) Page 31

Multiprotocol Label Switching (MPLS) Page 32

very small aperture terminal (VSAT) Page 33

DSL modem Page 34

DSL access multiplexer (DSLAM) Page 34

point of presence (POP) Page 34

cable modems (CM) Page 35

headend Page 35

cable modem termination system (CMTS) Page 35

municipal Wi-Fi Page 36

WiMAX Page 36

satellite Internet Page 36

3G/4G wireless Page 38

Long-Term Evolution (LTE) Page 38

teleworker Page 38

site-to-site VPNs Page 38

remote-access VPNs Page 39

Introduction (1.0)

Businesses must connect LANs to provide communications between them, even when these LANs are far apart. Wide-area networks (WANs) are used to connect remote LANs. A WAN may cover a city, country, or global region. A WAN is owned by a service provider, and a business pays a fee to use the provider's WAN network services.

Different technologies are used for WANs than for LANs. This chapter introduces WAN standards, technologies, and purposes. It covers selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise.

Class Activity 1.0.1.2: Branching Out

Your medium-sized company is opening a new branch office to serve a wider, client-based network. This branch will focus on regular, day-to-day network operations but will also provide TelePresence, web conferencing, IP telephony, video on demand, and wireless services.

Although you know that an ISP can provide WAN routers and switches to accommodate the branch office connectivity for the network, you prefer to use your own customer premises equipment (CPE). To ensure interoperability, Cisco devices have been used in all other branch-office WANs.

As the branch-office network administrator, you are responsible for researching possible network devices for purchase and use over the WAN.

WAN Technologies Overview (1.1)

In this section, you learn about WAN access technologies available to small- to medium-sized business networks.

Purpose of WANs (1.1.1)

In this topic, you learn the purpose of the WAN.

Why a WAN? (1.1.1.1)

A WAN operates beyond the geographic scope of a LAN. As shown Figure 1-1, WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.

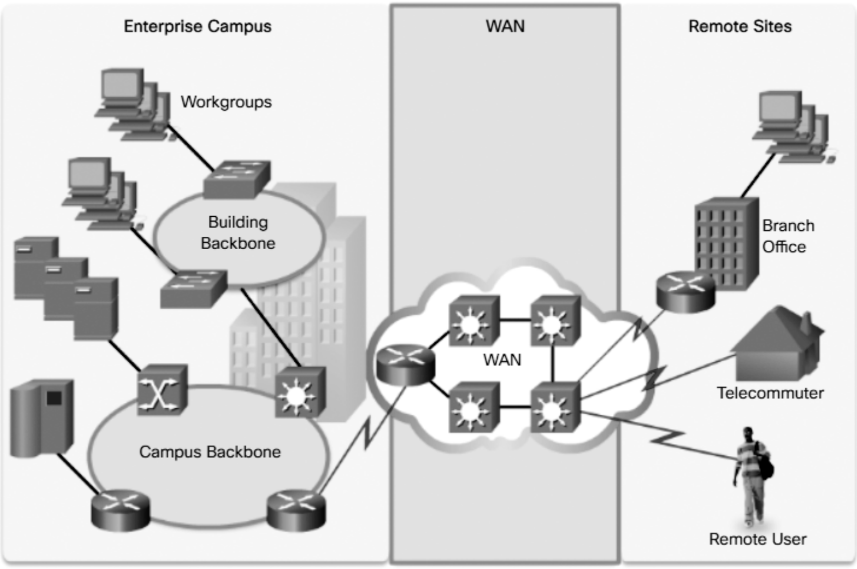


Figure 1-1 WANs Interconnect Users and LANs

A WAN is owned by a *service provider*. A user must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide links to interconnect remote sites for the purpose of transporting data, voice, and video.

In contrast, LANs are typically owned by an organization. They are used to connect local computers, peripherals, and other devices within a single building or other small geographic area.

Are WANs Necessary? (1.1.1.2)

Without WANs, LANs would be a series of isolated networks. LANs provide both speed and cost-efficiency for transmitting data over relatively small geographic areas. However, as organizations expand, businesses require communication among geographically separated sites. The following are some examples:

- Regional or branch offices of an organization need to be able to communicate and share data with the central site.
- Organizations need to share information with other customer organizations. For example, software manufacturers routinely communicate product and promotional information to distributors that sell their products to end users.
- Employees who travel on company business frequently need to access information that resides on their corporate networks.

Home computer users also need to send and receive data across increasingly larger distances. Here are some examples:

- Consumers now commonly communicate over the Internet with banks, stores, and a variety of providers of goods and services.
- Students do research for classes by accessing library indexes and publications located in other parts of their country and in other parts of the world.

It is not feasible to connect computers across a country, or around the world, with physical cables. Therefore, different technologies have evolved to support this communication requirement. Increasingly, the Internet is being used as an inexpensive alternative to enterprise WANs. New technologies are available to businesses to provide security and privacy for their Internet communications and transactions. WANs used by themselves, or in concert with the Internet, allow organizations and individuals to meet their wide-area communication needs.

WAN Topologies (1.1.1.3)

Interconnecting multiple sites across WANs can involve a variety of service provider technologies and WAN topologies. Common WAN topologies are

- *Point-to-point topology*
- *Hub-and-spoke topology*
- *Full mesh topology*
- *Dual-homed topology*

Point-to-Point

A point-to-point topology, as shown in Figure 1-2, employs a point-to-point circuit between two endpoints. Typically involving dedicated *leased-line* connections like a *T1* or an *E1* line, a point-to-point connection provides a Layer 2 transport service through the service provider network. Packets sent from one site are delivered to the other site and vice versa. A point-to-point connection is transparent to the customer network, as if there was a direct physical link between two endpoints.

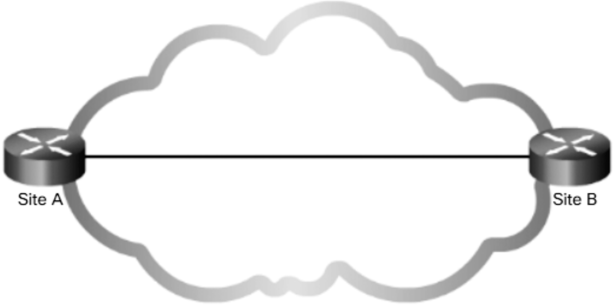


Figure 1-2 Point-to-Point Topology

Hub-and-Spoke

If a private network connection between multiple sites is required, a point-to-point topology with multiple point-to-point circuits is one option. Each point-to-point circuit requires its own dedicated hardware interface that will require multiple routers with multiple WAN interface cards. This interface can be expensive. A less expensive option is a point-to-multipoint topology, also known as a hub-and-spoke topology.

With a hub-and-spoke topology, all spoke circuits can share a single interface to the ***hub***. For example, spoke sites can be interconnected through the hub site using virtual circuits and routed subinterfaces at the hub. A hub-and-spoke topology is also an example of a single-homed topology. Figure 1-3 displays a sample hub-and-spoke topology consisting of four routers with one router as a hub connected to the other three spoke routers across a WAN cloud.

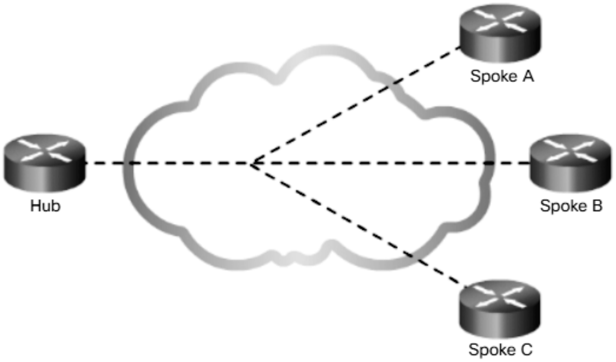


Figure 1-3 Hub-and-Spoke Topology

Full Mesh

One of the disadvantages of hub-and-spoke topologies is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site. The disadvantage here is the large number of virtual circuits that need to be configured and maintained. Figure 1-4 displays a sample full mesh topology consisting of four routers connected to each other across a WAN cloud.

Dual-homed Topology

A dual-homed topology provides redundancy. As shown in Figure 1-5, the spoke routers are dual-homed and redundantly attached to two hub routers across a WAN cloud. The disadvantage to dual-homed topologies is that they are more expensive to implement than a ***single-homed topology***. The reason is that they require additional networking hardware, like additional routers and switches. Dual-homed topologies are also more difficult to implement because they require additional, and more complex, configurations. However, the advantage of dual-homed topologies is that they offer enhanced network redundancy, load balancing, distributed computing or processing, and the ability to implement backup service provider connections.

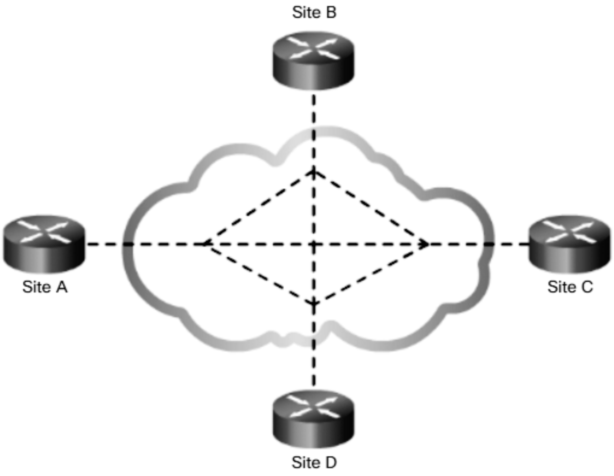


Figure 1-4 Full Mesh Topology

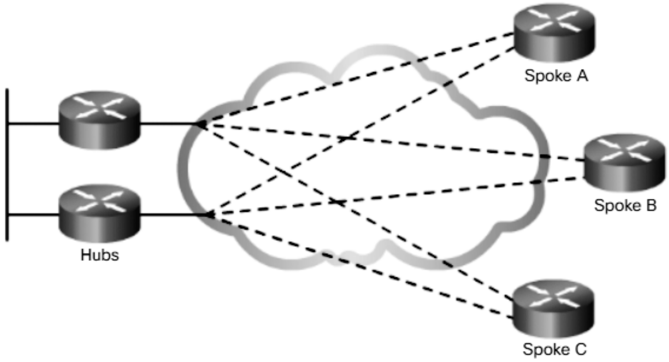


Figure 1-5 Dual-Homed Topology

Evolving Networks (1.1.1.4)

Every business is unique, so how an organization grows depends on many factors. These factors include the types of products or services the business sells, the management philosophy of the owners, and the economic climate of the country in which the business operates.

In slow economic times, many businesses focus on increasing their profitability by improving the efficiency of their existing operations, increasing employee productivity, and lowering operating costs. Establishing and managing networks can represent significant installation and operating expenses. To justify such a large expense, companies expect their networks to perform optimally and to be able to deliver an ever-increasing array of services and applications to support productivity and profitability.

The example used in this chapter and shown in Figure 1-6 is of a fictitious company called SPAN Engineering. This topic will illustrate how SPAN's network requirements change as the company grows from a small, local business into a global enterprise.

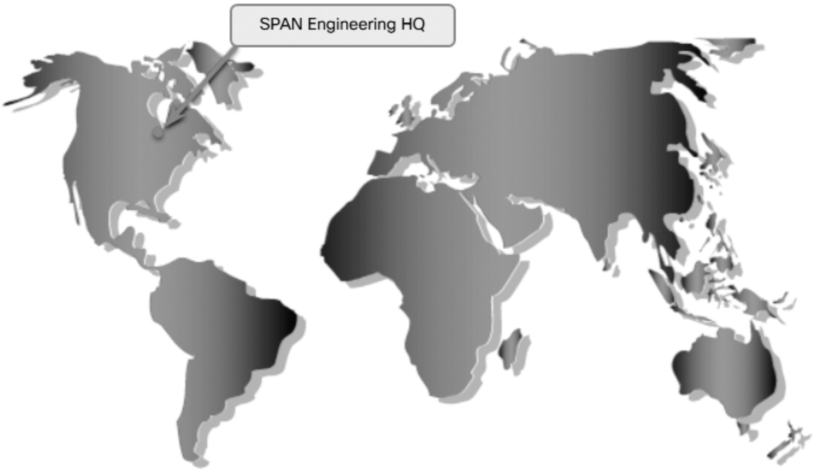


Figure 1-6 SPAN Engineering

Small Office (1.1.1.5)

SPAN Engineering, an environmental consulting firm, has developed a special process for converting household waste into electricity and is developing a small pilot project for a municipal government in its local area. The company, which has been in business for four years, is a small office consisting of 15 employees: six engineers, four computer-aided drawing (CAD) designers, a receptionist, two senior partners, and two office assistants.

SPAN Engineering's management is working to win full-scale contracts after the pilot project successfully demonstrates the feasibility of the company's process. Until then, the company must manage its costs carefully.

As shown in Figure 1-7, SPAN Engineering uses a single LAN to share information between computers and to share peripherals, such as a printer, a large-scale plotter (to print engineering drawings), and fax equipment.

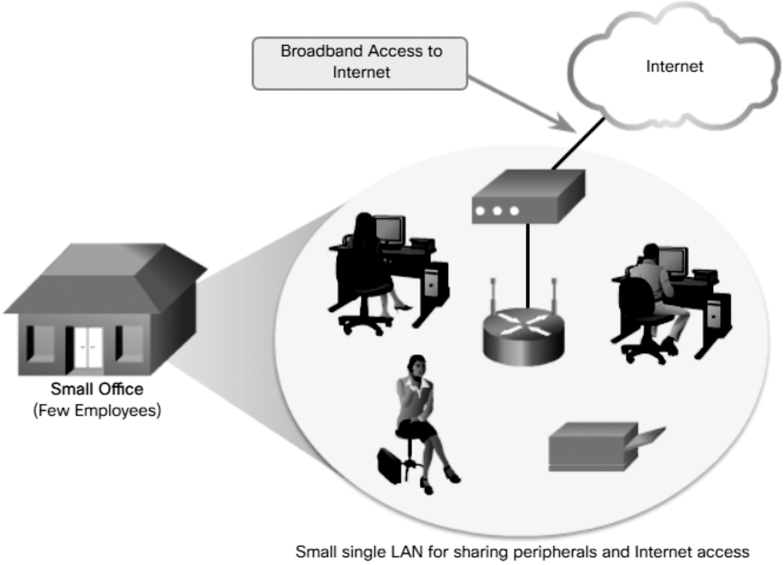

Broadband Access to Internet
Internet
Small Office
(Few Employees)
Small single LAN for sharing peripherals and Internet access

Figure 1-7 Connecting a Small Office

The company has recently upgraded its LAN to provide inexpensive *voice over IP (VoIP)* service to save on the costs of separate phone lines for employees.

Internet connectivity is provided using a common *broadband service* called *digital subscriber line (DSL)*, which is supplied by the local telephone service provider. Because SPAN has so few employees, bandwidth is not a significant problem.

The company cannot afford in-house IT support staff, so it uses support services purchased from the DSL provider. The company also uses a hosting service rather than purchasing and operating its own FTP and email servers.

Campus Network (1.1.1.6)

Five years later, SPAN Engineering has grown rapidly. The company was contracted to design and implement a full-size waste conversion facility soon after the successful implementation of its first pilot plant. Since then, SPAN has won other projects in neighboring municipalities and in other parts of the country.

To handle the additional workload, the business has hired more staff and leased more office space. It is now a small- to medium-sized business with several hundred employees. Many projects are being developed at the same time, and each requires a project manager and support staff. The company has organized itself into functional departments, with each department having its own organizational team. To meet its growing needs, the company has moved into several floors of a larger office building.

As the business has expanded, the network has also grown. Instead of a single small LAN, the network now consists of several subnetworks, each devoted to a different department. For example, all the engineering staff is on one LAN, while the marketing staff is on another LAN. These multiple LANs are joined to create a company-wide network, or campus, which spans several floors of the building.

Figure 1-8 shows an example of SPAN's campus network.

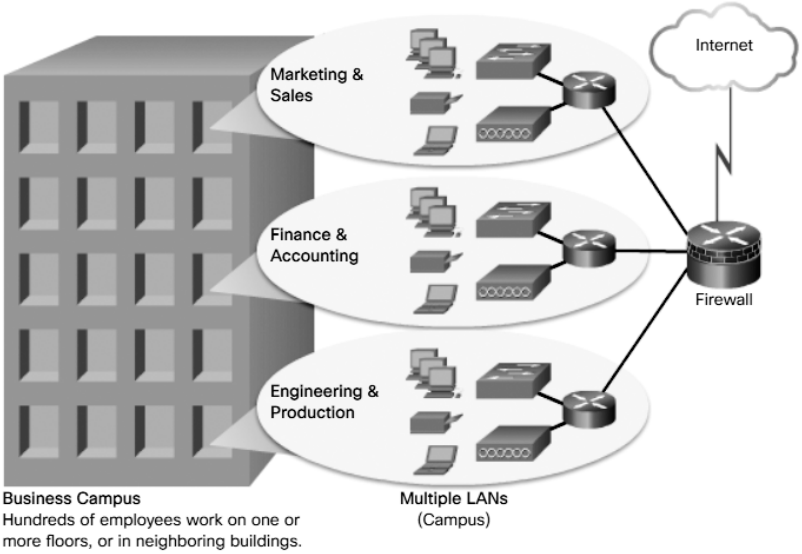


Figure 1-8 Connecting a Campus Network

The business now has in-house IT staff to support and maintain the network. The network includes dedicated servers for email, data transfer, and file storage, and web-based productivity tools and applications. In addition, a company intranet provides in-house documents and information to employees. An extranet provides project information to designated customers.

Branch Networks (1.1.1.7)

Another six years later, SPAN Engineering has been so successful with its patented process that demand for its services has skyrocketed. New projects are underway in multiple cities. To manage those projects, the company has opened small branch offices closer to the project sites.

This situation presents new challenges to the IT team. To manage the delivery of information and services throughout the company, SPAN Engineering now has a data center, which houses the various databases and servers of the company. To ensure that all parts of the business are able to access the same services and applications regardless of where the offices are located, the company must now implement a WAN.

For its branch offices that are in nearby cities, the company decides to use private *dedicated lines* through a local service provider, as shown in Figure 1-9. However, for those offices that are located in other countries, the Internet is an attractive WAN connection option. Although connecting offices through the Internet is economical, this approach introduces security and privacy issues that the IT team must address.

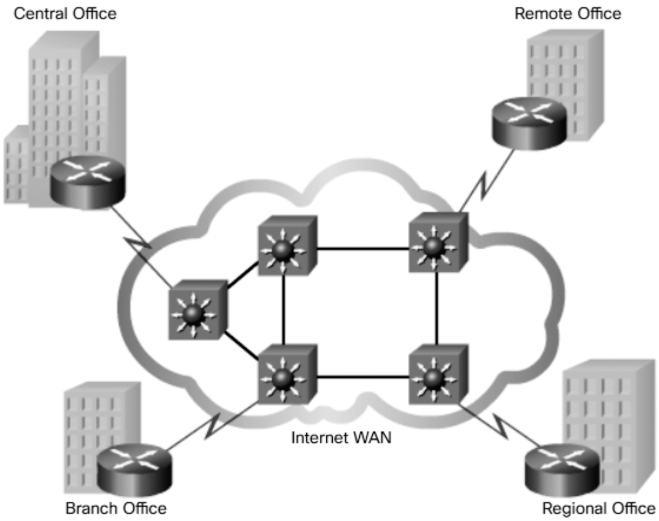


Figure 1-9 Connecting Branch Networks

Distributed Network (1.1.1.8)

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide, as shown in Figure 1-10.

The cost of the *enterprise network* and its related services is a significant expense. The company is looking to provide its employees with the best network services at the lowest cost. Optimized network services would allow each employee to work at a high rate of efficiency.

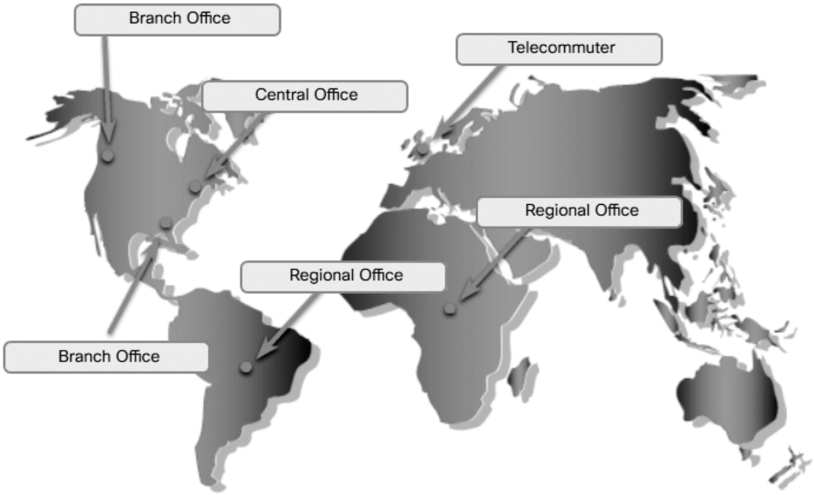


Figure 1-10 SPAN Engineering

To increase profitability, SPAN Engineering must reduce its operating expenses. It has relocated some of its office facilities to less expensive areas. The company is also encouraging ***teleworking*** and virtual teams. Web-based applications, including web conferencing, e-learning, and online collaboration tools, are being used to increase productivity and reduce costs. Site-to-site and remote-access ***virtual private networks (VPNs)*** enable the company to use the Internet to connect easily and securely with employees and facilities around the world. To meet these requirements, the network must provide the necessary converged services and secure Internet WAN connectivity to remote offices and individuals, as shown in Figure 1-11.

As seen in this example, network requirements of a company can change dramatically as the company grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network.

A network not only must meet the day-to-day operational needs of the business but also must be able to adapt and grow as the company changes. Network designers and administrators meet these challenges by carefully choosing network technologies, protocols, and service providers. They must also optimize their networks by using many of the network design techniques and architectures described in this course.

Interactive Graphic

Activity 1.1.1.9: Identify WAN Topologies

Refer to the online course to complete this activity.

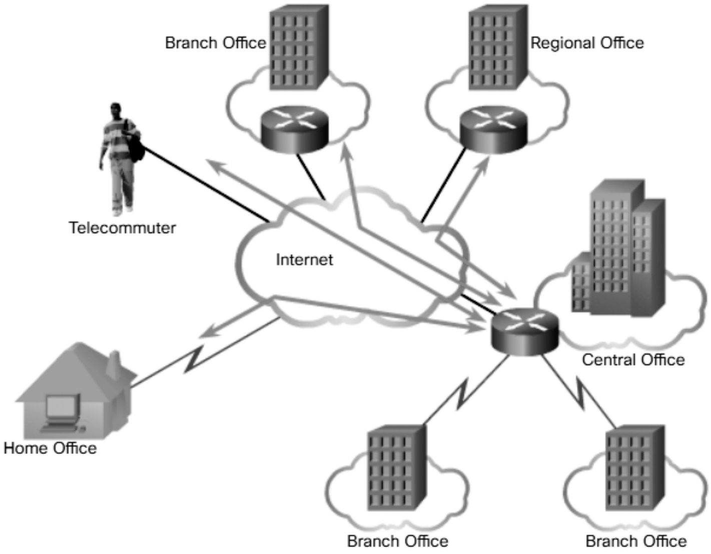


Figure 1-11 Connecting a Global Enterprise Network

WAN Operations (1.1.2)

In this topic, you learn how WANs operate.

WANs in the OSI Model (1.1.2.1)

WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2), as illustrated in Figure 1-12. WAN access standards typically describe both physical layer delivery methods and data link layer requirements. The data link layer requirements include physical addressing, flow control, and encapsulation.

WAN access standards are defined and managed by a number of recognized authorities:

- *Telecommunications Industry Association (TIA)*
- *Electronic Industries Alliance (EIA)*
- *International Organization for Standardization (ISO)*
- *Institute of Electrical and Electronics Engineers (IEEE)*

Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

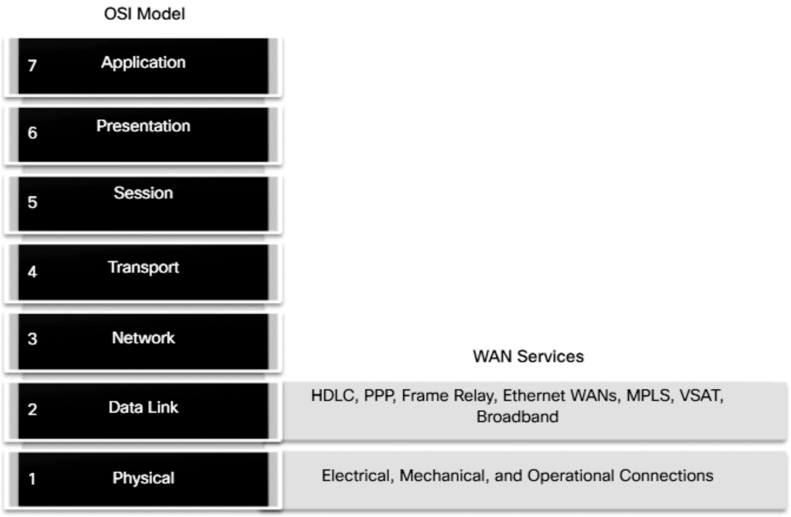

OSI Model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
WAN Services
HDLC, PPP, Frame Relay, Ethernet WANs, MPLS, VSAT, Broadband
Electrical, Mechanical, and Operational Connections

Figure 1-12 WANs Operate in Layers 1 and 2

Layer 2 protocols define how data is encapsulated for transmission toward a remote location and the mechanisms for transferring the resulting frames. A variety of different technologies are used, such as the ***Point-to-Point Protocol (PPP)***, ***Frame Relay***, and ***Asynchronous Transfer Mode (ATM)***. Some of these protocols use the same basic framing or a subset of the ***High-Level Data Link Control (HDLC)*** mechanism.

Most WAN links are point-to-point. For this reason, the address field in the Layer 2 frame is usually not used.

Common WAN Terminology (1.1.2.2)

One primary difference between a WAN and a LAN is that a company or organization must subscribe to an outside WAN service provider to use WAN carrier network services. A WAN uses data links provided by carrier services to access the Internet and connect different locations of an organization to each other. These data links also connect to locations of other organizations, to external services, and to remote users.

The physical layer of a WAN describes the physical connections between the company network and the service provider network. Figure 1-13 illustrates the terminology commonly used to describe WAN connections:

- ***Customer premises equipment (CPE)***: The CPE consists of the devices and inside wiring located on the enterprise edge connecting to a carrier link. The subscriber (that is, customer) either owns the CPE or leases the CPE from the service provider. A subscriber, in this context, is a company that arranges for WAN services from a service provider.

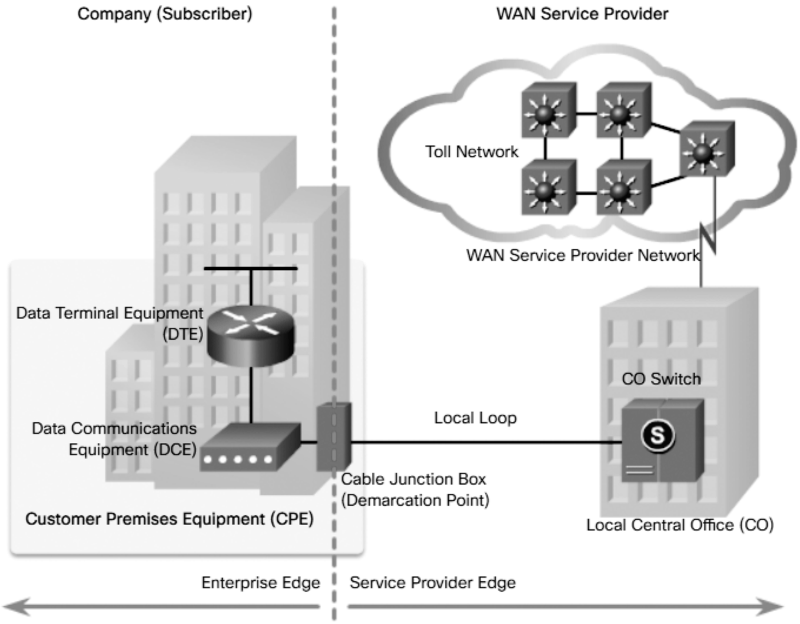

Company (Subscriber)
WAN Service Provider
Toll Network
WAN Service Provider Network
Data Terminal Equipment (DTE)
Data Communications Equipment (DCE)
CO Switch
Local Loop
Cable Junction Box (Demarcation Point)
Customer Premises Equipment (CPE)
Local Central Office (CO)
Enterprise Edge
Service Provider Edge

Figure 1-13 WAN Terminology

- *Data communications equipment (DCE)*: This is an EIA term. Also called data circuit-terminating equipment by the ITU. The DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.
- *Data terminal equipment (DTE)*: These customer devices pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.
- *Demarcation point*: This point is established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed so that a technician can access it easily. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.
- *Local loop*: This loop is the actual copper or fiber cable that connects the CPE to the CO of the service provider. The local loop is also sometimes called the *last-mile*.
- *Central office (CO)*: The CO is the local service provider facility or building that connects the CPE to the provider network.

- *Toll network*: This network consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

WAN Devices (1.1.2.3)

Many types of devices are specific to WAN environments, as shown in Figure 1-14, and are described in the list that follows.

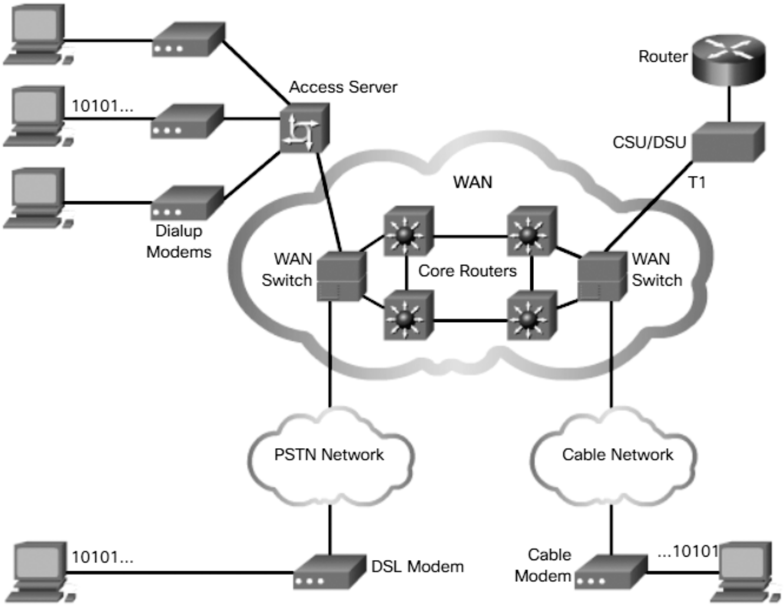


Figure 1-14 Common WAN Devices

- *Dialup modem*: Voiceband modems are considered to be a legacy WAN technology. A voiceband modem *modulates* (that is, converts) the digital signals produced by a computer into voice frequencies. These frequencies are then transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem *demodulates* the sounds back into a digital signal for input to a computer or network connection.
- *Access server*: This server controls and coordinates dialup modem, dial-in, and dial-out user communications. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.
- *Broadband modem*: This type of digital modem is used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem but use higher broadband frequencies to achieve higher transmission speeds.

- ***Channel service unit/data service unit (CSU/DSU)*****:** Digital leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem, or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa.

- ***WAN switch*****:** This multiport internetworking device is used in service provider networks. These devices typically switch traffic, such as Frame Relay or ATM, and operate at Layer 2.

- **Router:** This device provides internetworking and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or DSL), is required to connect the router to the local service provider.

- **Core router/Multilayer switch:** This router or multilayer switch resides within the middle or backbone of the WAN, rather than at its periphery. To fulfill this role, a router or multilayer switch must be able to support multiple telecommunications interfaces of the highest speed used in the WAN core. It must also be able to forward IP packets at full speed on all of those interfaces. The router or multilayer switch must also support the routing protocols being used in the core.

Note

The preceding list is not exhaustive, and other devices may be required, depending on the WAN access technology chosen.

WAN technologies are either circuit-switched or packet-switched. The type of device used depends on the WAN technology implemented.

Circuit Switching (1.1.2.4)

A ***circuit-switched network*** is one that establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate. Specifically, circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver. Before communication can start, it is necessary to establish the connection through the network of the service provider, as shown in Figure 1-15.

As an example, when a subscriber makes a telephone call, the dialed number is used to set switches in the exchanges along the route of the call so that there is a continuous circuit from the caller to the called party. Because of the switching operation used to establish the circuit, the telephone system is called a circuit-switched network. If the telephones are replaced with modems, the switched circuit is able to carry computer data.

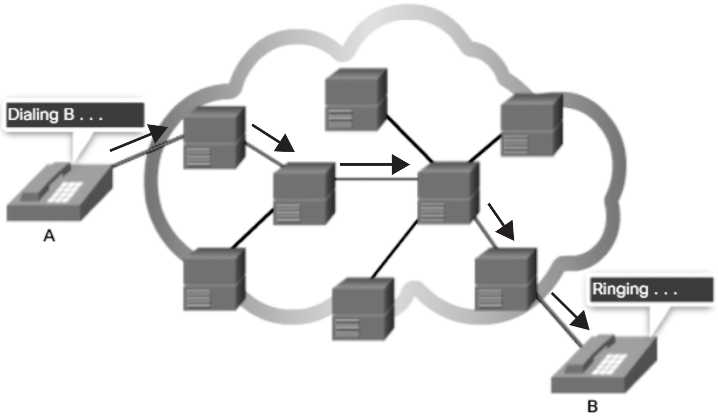


Figure 1-15 Circuit-Switched Network

If the circuit carries computer data, the usage of this fixed capacity may not be efficient. For example, if the circuit is used to access the Internet, a burst of activity occurs on the circuit while a web page is transferred. This burst could be followed by no activity while the user reads the page and then another burst of activity while the next page is transferred. This variation in usage between none and maximum is typical of computer network traffic. Because the subscriber has sole use of the fixed capacity allocation, switched circuits are generally an inefficient way of moving data.

The two most common types of circuit-switched WAN technologies are the *public switched telephone network (PSTN)* and the *Integrated Services Digital Network (ISDN)*.

Packet Switching (1.1.2.5)

In contrast to circuit switching, a *packet-switched network (PSN)* splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

The switches in a PSN determine the links that packets must be sent over based on the addressing information in each packet. The following are two approaches to this link determination:

- **Connectionless systems:** Full addressing information must be carried in each packet. Each switch must evaluate the address to determine where to send the packet. An example of a connectionless system is the Internet.
- **Connection-oriented systems:** The network predetermines the route for a packet, and each packet only has to carry an identifier. The switch determines

the onward route by looking up the identifier in tables held in memory. The set of entries in the tables identifies a particular route or circuit through the system. When the circuit is established temporarily while a packet is traveling through it and then breaks down again, it is called a ***virtual circuit (VC)***. An example of a connection-oriented system is Frame Relay. In the case of Frame Relay, the identifiers used are called ***data-link connection identifiers (DLCIs)***.

Note

Frame Relay systems are commonly being replaced by Ethernet WANs.

Because the internal links between the switches are shared between many users, the cost of packet switching is lower than that of circuit switching. However, ***latency*** (delays) and ***jitter*** (variability of delay) are greater in packet-switched networks than in circuit-switched networks. The reason is that the links are shared, and packets must be entirely received at one switch before moving to the next. Despite the latency and jitter inherent in shared networks, modern technology allows satisfactory transport of voice and video communications on these networks.

In Figure 1-16, SRV1 is sending data to SRV2. As packets traverse the provider network, they arrive at the first provider switch. Packets are added to the queue and forwarded after other packets in the queue have been forwarded. Eventually, the packets reach SRV2.

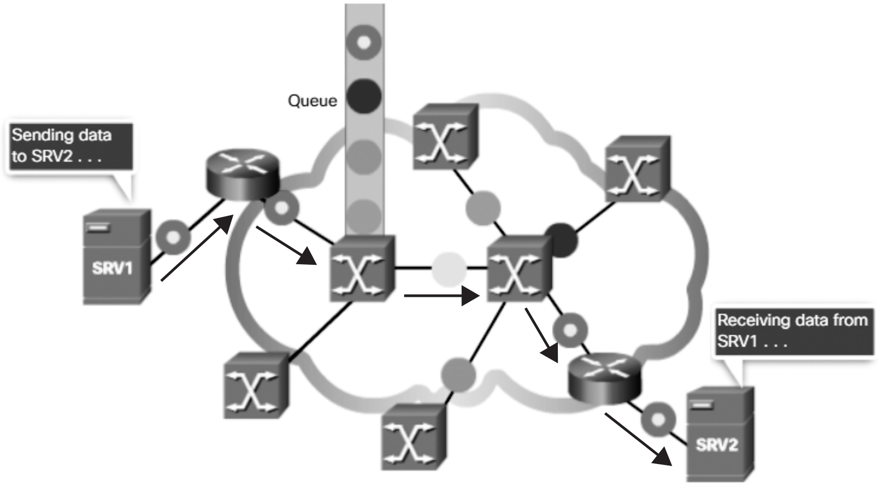


Figure 1-16 Packet-Switched Network

Interactive Graphic

Activity 1.1.2.6: Identify WAN Terminology

Refer to the online course to complete this activity.

Selecting a WAN Technology (1.2)

In this section, you learn how to select WAN access technologies to satisfy business requirements.

WAN Services (1.2.1)

In this topic, you learn about different WAN services available.

WAN Link Connection Options (1.2.1.1)

ISPs can use are several WAN access connection options to connect the local loop to the enterprise edge. These WAN access options differ in technology, speed, and cost. Each has distinct advantages and disadvantages. Familiarity with these technologies is an important part of network design.

As shown in Figure 1-17 and described in the list that follows, an enterprise can get WAN access in two ways.

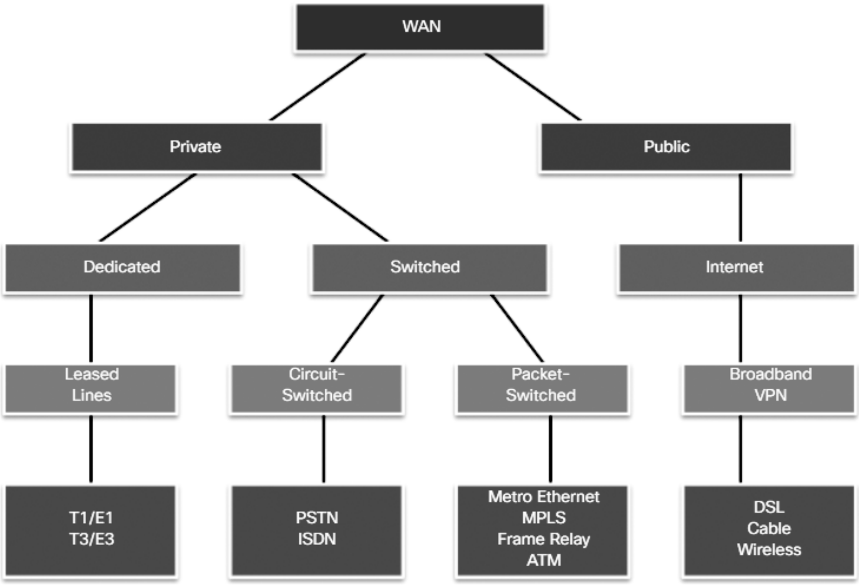


Figure 1-17 WAN Access Options

- *Private WAN infrastructure*: Service providers may offer dedicated point-to-point leased lines, circuit-switched links, such as PSTN or ISDN, and packet-switched links, such as Ethernet WAN, ATM, or Frame Relay.
- *Public WAN infrastructure*: Service providers provide Internet access using broadband services such as DSL, cable, and satellite access. *Broadband connections* are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.

Note

Frame Relay systems are commonly being replaced by Ethernet WANs.

The topology in Figure 1-18 illustrates some of these WAN access technologies.

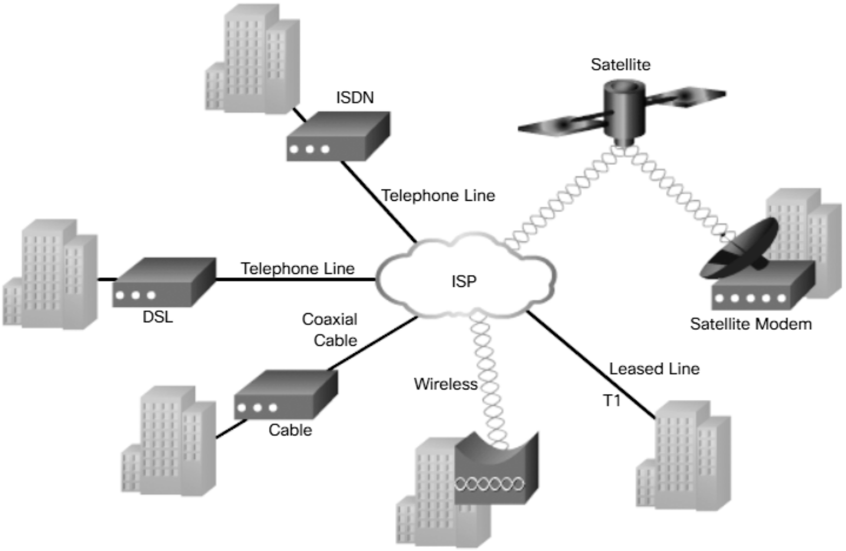


Figure 1-18 WAN Access Technologies

Service Provider Network Infrastructure (1.2.1.2)

When a WAN service provider receives data from a client at a site, it must forward the data to the remote site for final delivery to the recipient. In some cases, the remote site may be connected to the same service provider as the originating site. In other cases, the remote site may be connected to a different ISP, and the originating ISP must pass the data to the connecting ISP.

Long-range communications are usually those connections between ISPs, or between branch offices in very large companies.

Service provider networks are complex. They consist mostly of high-bandwidth fiber-optic media, using either the *Synchronous Optical Networking (SONET)* or *Synchronous Digital Hierarchy (SDH)* standard. These standards define how to transfer multiple data, voice, and video traffic over optical fiber using lasers or *light-emitting diodes (LEDs)* over great distances.

Note

SONET is an American-based ANSI standard, while SDH is a European-based ETSI and ITU standard. Both are essentially the same and, therefore, often listed as SONET/SDH.

A newer fiber-optic media development for long-range communications is called *dense wavelength division multiplexing (DWDM)*. DWDM multiplies the amount of bandwidth that a single strand of fiber can support, as illustrated in Figure 1-19.

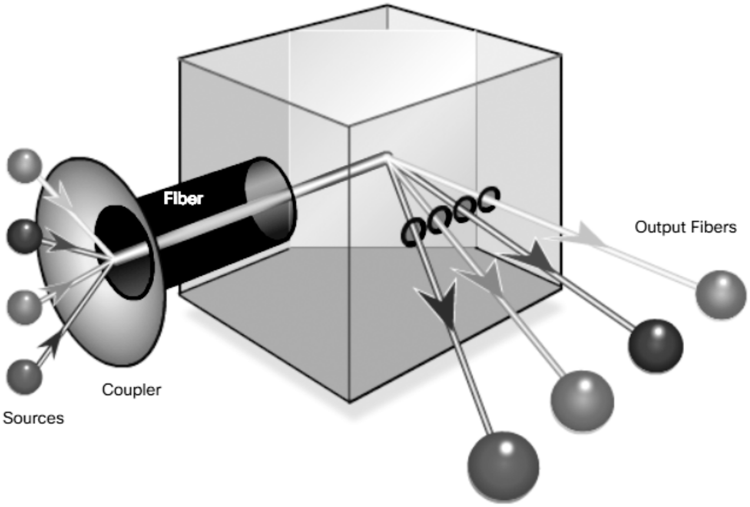


Figure 1-19 DWDM

DWDM enables long-range communication in several ways:

- DWDM enables bidirectional (for example, two-way) communications over one strand of fiber.
- It can *multiplex* more than 80 different channels of data (that is, wavelengths) onto a single fiber.

- Each channel is capable of carrying a 10 Gb/s multiplexed signal.
- It assigns incoming optical signals to specific wavelengths of light (that is, frequencies).
- It can amplify these wavelengths to boost the signal strength.
- It supports SONET and SDH standards.

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits, as illustrated in Figure 1-20.

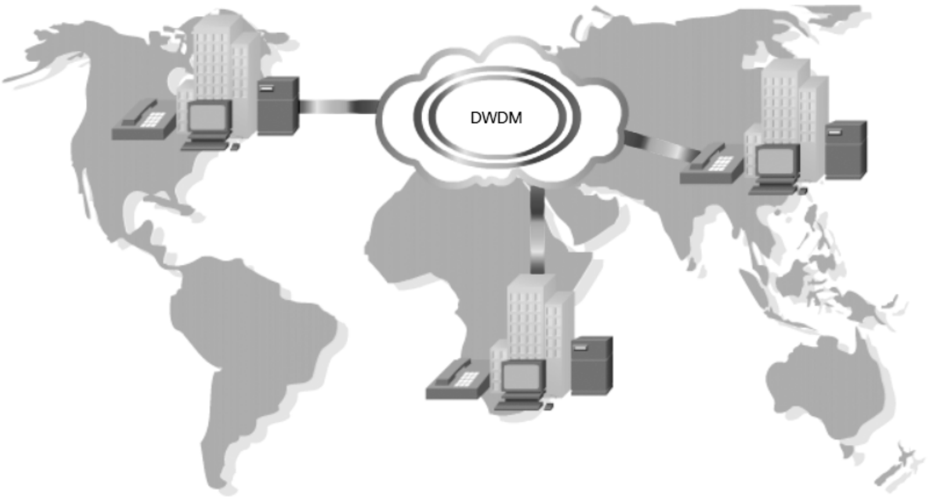


Figure 1-20 Service Provider Networks Use DWDM

Interactive Graphic

Activity 1.2.1.3: Classify WAN Access Options

Refer to the online course to complete this activity.

Private WAN Infrastructures (1.2.2)

In this topic, you compare private WAN technologies.

Leased Lines (1.2.2.1)

When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines are usually leased from a service provider and are called leased lines.

Leased lines have existed since the early 1950s; for this reason, they are referred to by different names such as leased circuits, serial link, serial line, point-to-point link, and T1/E1 or T3/*E3* lines.

The term *leased line* refers to the fact that the organization pays a monthly lease fee to a service provider to use the line. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

In North America, service providers use the T-carrier system to define the digital transmission capability of a serial copper media link, while Europe uses the E-carrier system, as shown in Figure 1-21. For instance, a T1 link supports 1.544 Mb/s, an E1 supports 2.048 Mb/s, a T3 supports 43.7 Mb/s, and an E3 connection supports 34.368 Mb/s. *Optical carrier (OC)* transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

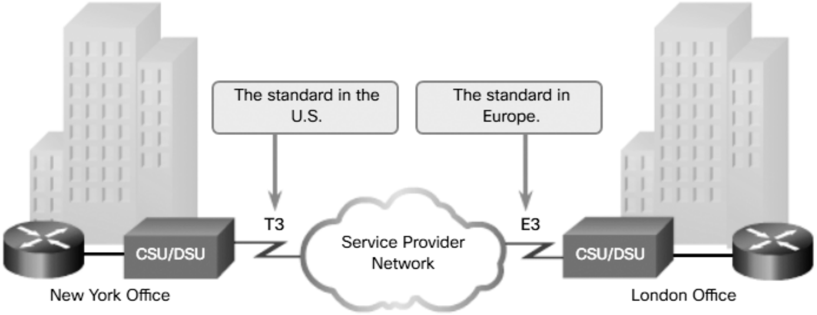


Figure 1-21 Sample Leased-Line Topology

Table 1-1 describes the advantages and disadvantages of using leased lines.

Table 1-1 Advantages/Disadvantages of Leased Lines

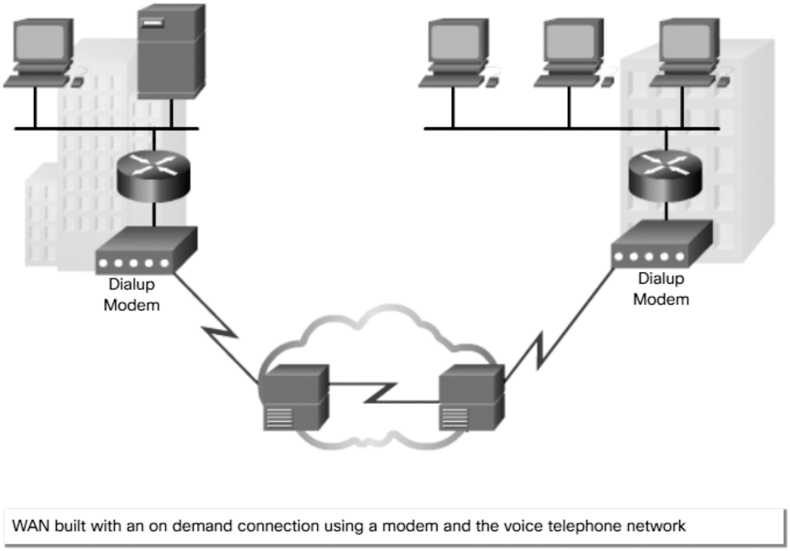
Advantages	Disadvantages
Simplicity: Point-to-point communication links require minimal expertise to install and maintain.	**Cost:** Point-to-point links are generally the most expensive type of WAN access. The cost of leased-line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.

Advantages	Disadvantages
Quality: Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.	**Limited flexibility:** WAN traffic is often variable, and leased lines have a fixed capacity, so the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.
Availability: Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP.	

The Layer 2 protocol is usually HDLC or PPP.

Dialup (1.2.2.2)

Dialup WAN access may be required when no other WAN technology is available. For example, a remote location could use modems and analog dialed telephone lines to provide low capacity and dedicated switched connections, as shown in Figure 1-22. Dialup access is suitable when intermittent, low-volume data transfers are needed.



WAN built with an on demand connection using a modem and the voice telephone network

Figure 1-22 Sample Dialup Topology

Traditional telephony uses a copper cable, called the local loop, to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber voice into an analog signal.

Traditional local loops can transport binary computer data through the voice telephone network using a dialup modem. The modem modulates the binary data into an analog signal at the source and demodulates the analog signal to binary data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 kb/s.

For small businesses, these relatively low-speed dialup connections are adequate for the exchange of sales figures, prices, routine reports, and email. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak rates. These rates, often referred to as tariffs or toll charges, are based on the distance between the endpoints, time of day, and the duration of the call.

The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time. The dedicated circuit has little delay or jitter for point-to-point traffic, but voice or video traffic does not operate adequately at these low bit rates.

Note

Although very few enterprises support dialup access, it is still a viable solution for remote areas with limited WAN access options.

ISDN (1.2.2.3)

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher capacity switched connections.

ISDN changes the internal connections of the PSTN from carrying analog signals to ***time-division multiplexed (TDM)*** digital signals. TDM allows two or more signals, or bit streams, to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously; but physically, the signals are taking turns on the channel.

Figure 1-23 displays a sample ISDN topology. The ISDN connection may require a terminal adapter (TA), which is a device used to connect ISDN ***Basic Rate Interface (BRI)*** connections to a router.

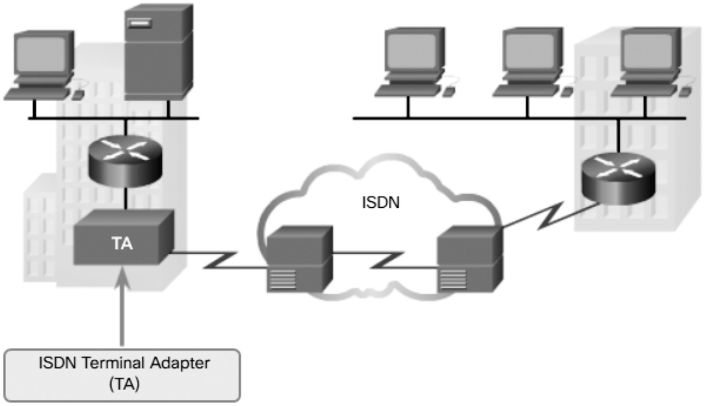


Figure 1-23 Sample ISDN Topology

The two types of ISDN interfaces are as follows:

- **Basic Rate Interface (BRI):** ISDN BRI is intended for the home and small enterprise and provides two 64 kb/s bearer channels (B) for carrying voice and data and a 16 kb/s delta channel (D) for signaling, call setup, and other purposes. The BRI D channel is often underused because it has only two B channels to control (see Figure 1-24).

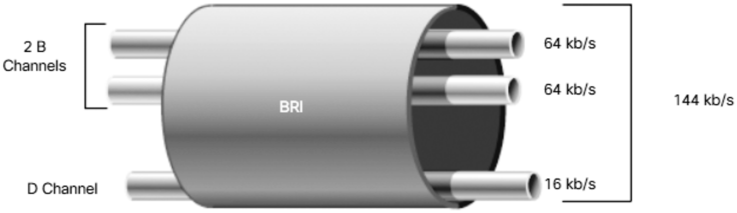


Figure 1-24 ISDN BRI

- ***Primary Rate Interface (PRI)***: ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 kb/s and one D channel with 64 kb/s for a total bit rate of up to 1.544 Mb/s. This includes some additional overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mb/s, including synchronization overhead (see Figure 1-25).

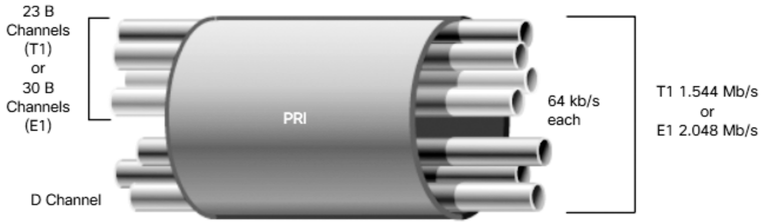


Figure 1-25 ISDN PRI

BRI has a call setup time that is less than a second, and the 64 kb/s B channel provides greater capacity than an analog modem link. In comparison, the call setup time of a dialup modem is approximately 30 or more seconds with a theoretical maximum of 56 kb/s. With ISDN, if greater capacity is required, a second B channel can be activated to provide a total of 128 kb/s. This permits several simultaneous voice conversations, a voice conversation and data transfer, or a video conference using one channel for voice and the other for video.

Another common application of ISDN is to provide additional capacity as needed on a leased-line connection. The leased line is sized to carry average traffic loads while ISDN is added during peak demand periods. ISDN is also used as a backup if the leased line fails. ISDN tariffs are based on a per-B channel basis and are similar to those of analog voice connections.

With PRI ISDN, multiple B channels can be connected between two endpoints. This allows for videoconferencing and high-bandwidth data connections with no latency or jitter. However, multiple connections can be very expensive over long distances.

Note

Although ISDN is still an important technology for telephone service provider networks, it has declined in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.

Frame Relay (1.2.2.4)

Frame Relay is a simple Layer 2 ***nonbroadcast multi-access (NBMA)*** WAN technology used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using ***permanent virtual circuits (PVCs)***. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mb/s, with some providers offering even higher rates.

An edge router requires only a single interface, even when multiple VCs are used. The leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay creates PVCs, which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication from one DTE device to another.

For instance, in Figure 1-26, R1 will use DLCI 102 to reach R2 while R2 will use DLCI 201 to reach R1.

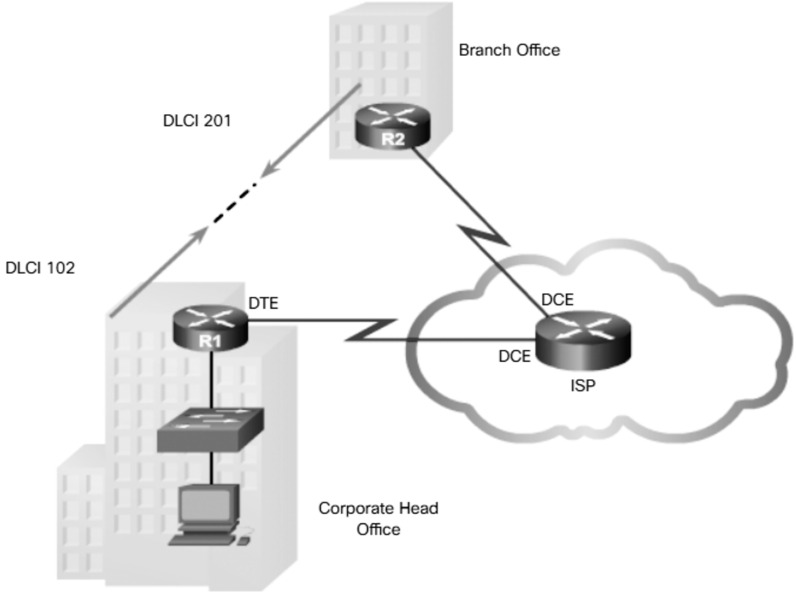


Figure 1-26 Sample Frame Relay Topology

ATM (1.2.2.5)

Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small, fixed-length cells are well suited for carrying voice and video traffic because this traffic is intolerant of delay. Video and voice traffic do not have to wait for larger data packets to be transmitted, as shown in Figure 1-27.

The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is higher because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent greater bandwidth than Frame Relay to carry the same volume of network layer data.

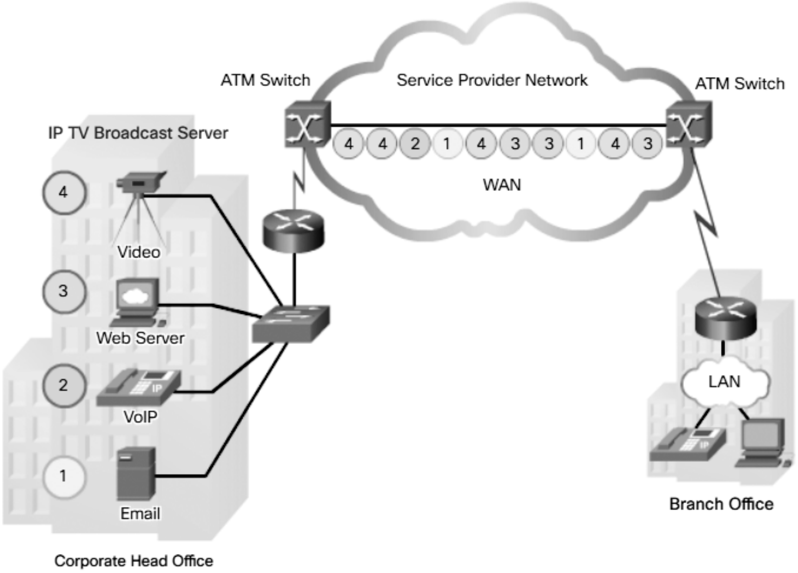


Figure 1-27 Sample ATM Topology

ATM was designed to be extremely scalable and to support link speeds of T1/E1 to OC-12 (622 Mb/s) and faster.

As with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.

Note

ATM networks are now considered to be a a legacy technology.

Ethernet WAN (1.2.2.6)

Ethernet was originally developed to be a LAN access technology. Originally, Ethernet was not suitable as a WAN access technology because at that time, the maximum cable length was one kilometer. However, newer Ethernet standards using fiber-optic cables have made Ethernet a reasonable WAN access option. For instance, the IEEE 1000BASE-LX standard supports fiber-optic cable lengths of 5 km, while the IEEE 1000BASE-ZX standard supports cable lengths up to 70 km.

Service providers now offer Ethernet WAN service using fiber-optic cabling. The Ethernet WAN service can go by many names, including ***Metropolitan Ethernet***

(MetroE), *Ethernet over MPLS (EoMPLS)*, and *Virtual Private LAN Service (VPLS)*. A sample Ethernet WAN topology is shown in Figure 1-28.

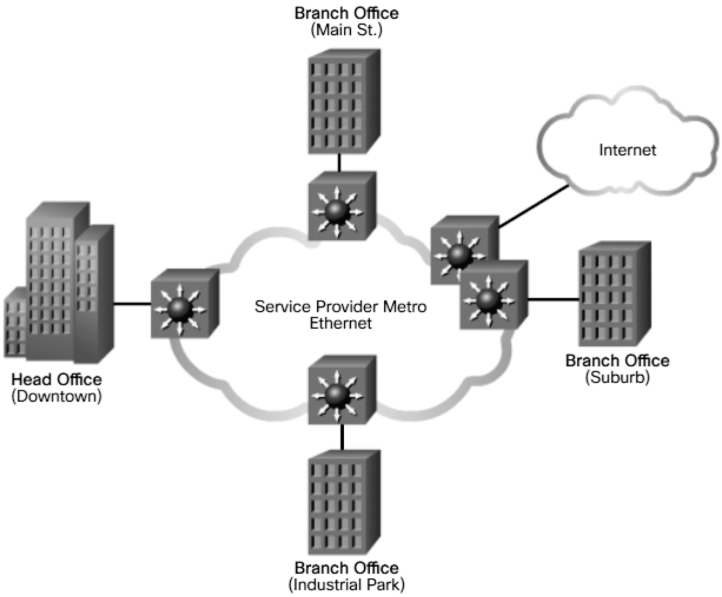


Figure 1-28 Sample Ethernet WAN Topology

An Ethernet WAN offers several benefits:

- **Reduced expenses and administration:** Ethernet WAN provides a switched, high-bandwidth Layer 2 network capable of managing data, voice, and video all on the same infrastructure. This characteristic increases bandwidth and eliminates expensive conversions to other WAN technologies. The technology enables businesses to inexpensively connect numerous sites in a metropolitan area, to each other, and to the Internet.
- **Easy integration with existing networks:** Ethernet WAN connects easily to existing Ethernet LANs, reducing installation costs and time.
- **Enhanced business productivity:** Ethernet WAN enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.

Note

Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional Frame Relay and ATM WAN links.

MPLS (1.2.2.7)

Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next. MPLS is based on short path labels rather than IP network addresses.

MPLS has several defining characteristics. It is multiprotocol, meaning it has the ability to carry any payload including IPv4, IPv6, Ethernet, ATM, DSL, and Frame Relay traffic. It uses labels that tell a router what to do with a packet. The labels identify paths between distant routers rather than endpoints, and while MPLS actually routes IPv4 and IPv6 packets, everything else is switched.

MPLS is a service provider technology. Leased lines deliver bits between sites, and Frame Relay and Ethernet WAN deliver frames between sites. However, MPLS can deliver any type of packet between sites. MPLS can encapsulate packets of various network protocols. It supports a wide range of WAN technologies including T-carrier/E-carrier links, Carrier Ethernet, ATM, Frame Relay, and DSL.

The sample topology in Figure 1-29 illustrates how MPLS is used. Notice that the different sites can connect to the MPLS cloud using different access technologies.

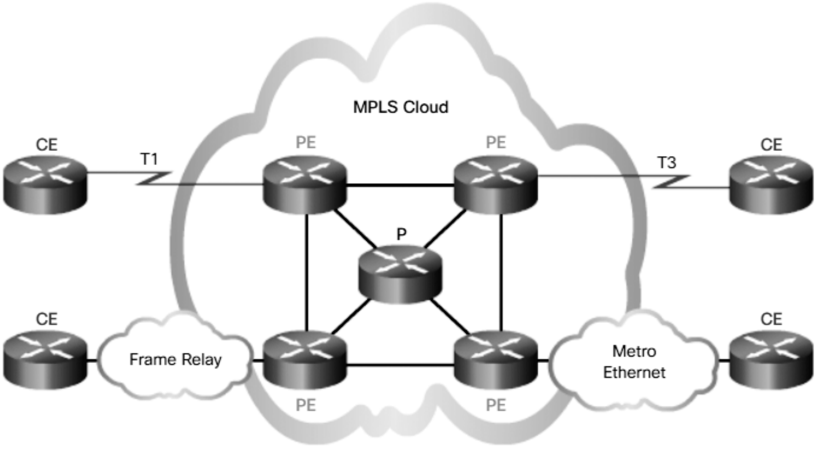


Figure 1-29 Sample MPLS Topology

In the Figure 1-29, CE refers to the customer edge; PE is the provider edge router, which adds and removes labels; and P is an internal provider router, which switches MPLS labeled packets.

VSAT (1.2.2.8)

All private WAN technologies discussed so far used either copper or fiber-optic media. What if an organization needed connectivity in a remote location where no service providers offer WAN service?

Very small aperture terminal (VSAT) is a solution that creates a private WAN using satellite communications. A VSAT is a small satellite dish similar to those used for home Internet and TV. VSATs create a private WAN while providing connectivity to remote locations.

Specifically, a router connects to a satellite dish that is pointed to a service provider's satellite. This satellite is in geosynchronous orbit in space. The signals must travel approximately 35,786 kilometers (22,236 miles) to the satellite and back.

The example in Figure 1-30 displays a VSAT dish on the roofs of the buildings communicating with a satellite thousands of kilometers away in space.

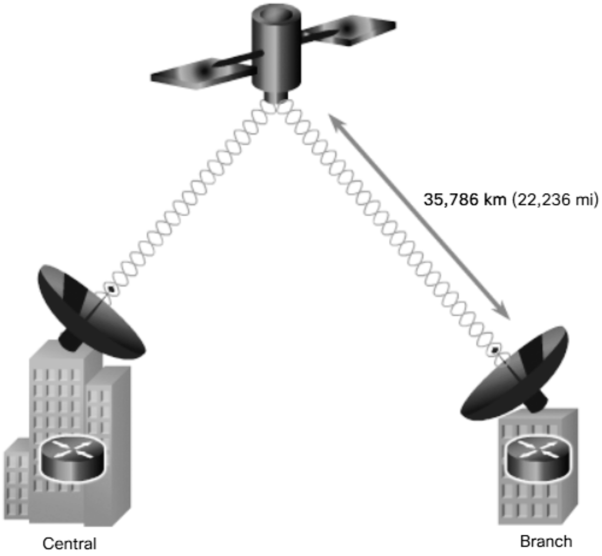


Figure 1-30 Sample VSAT Topology

Interactive Graphic

Activity 1.2.2.9: Identify Private WAN Infrastructure Terminology

Refer to the online course to complete this activity.

Public WAN Infrastructure (1.2.3)

In this topic, you compare public WAN technologies.

DSL (1.2.3.1)

DSL technology is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. A ***DSL modem*** converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the central office.

Multiple DSL subscriber lines are multiplexed into a single, high-capacity link using a ***DSL access multiplexer (DSLAM)*** at the provider location referred to as the ***point of presence (POP)***. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 connection. Current DSL technologies use sophisticated coding and modulation techniques to achieve fast data rates.

There is a wide variety of DSL types, standards, and emerging standards. DSL is now a popular choice for enterprise IT departments to support home workers. Generally, a subscriber cannot choose to connect to an enterprise network directly but must first connect to an ISP, and then an IP connection is made through the Internet to the enterprise. Security risks are incurred in this process but can be mediated with security measures.

The topology in Figure 1-31 displays a sample DSL WAN connection.

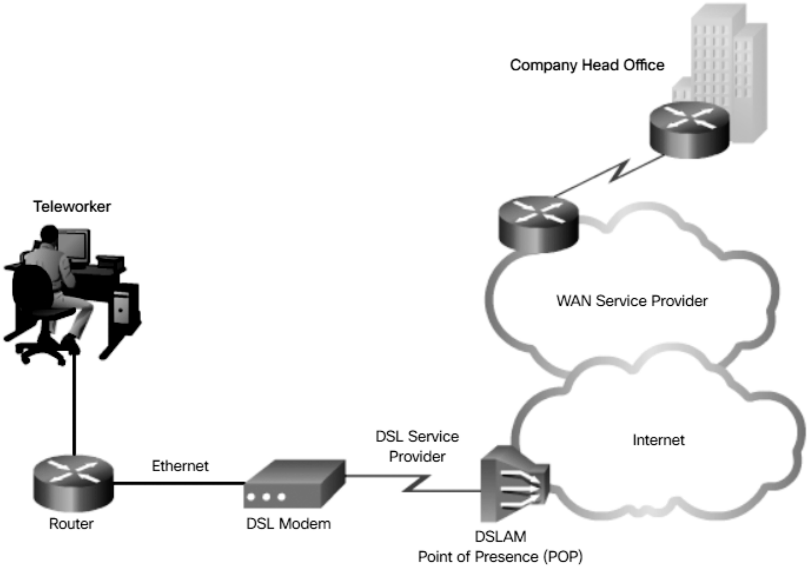


Figure 1-31 Sample DSL Topology

Cable (1.2.3.2)

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This access allows for greater bandwidth than the conventional telephone local loop.

Cable modems (CMs) provide an always-on connection and a simple installation. A subscriber connects a computer or LAN router to the cable modem, which translates the digital signals into the broadband frequencies used for transmitting on a cable television network. The local cable TV office, which is called the cable ***headend***, contains the computer system and databases needed to provide Internet access. The most important component located at the headend is the ***cable modem termination system (CMTS)***, which sends and receives digital cable modem signals on a cable network and is necessary for providing Internet services to cable subscribers.

Cable modem subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may drop below the expected rate.

The topology in Figure 1-32 displays a sample cable WAN connection.

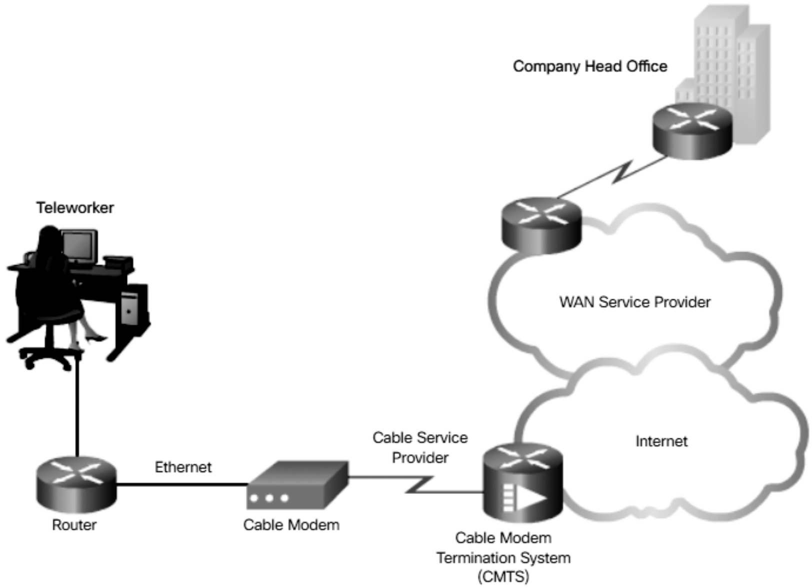


Figure 1-32 Sample Cable Topology

Wireless (1.2.3.3)

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device he or she is using.

Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the Internet. The following new developments in broadband wireless technology are changing this situation:

- ***Municipal Wi-Fi***: Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other broadband services. Others are for city use only, allowing police and fire departments and other city employees to do certain aspects of their jobs remotely. To connect to a municipal Wi-Fi, a subscriber typically needs a wireless modem, which provides a stronger radio and directional antenna than conventional wireless adapters. Most service providers provide the necessary equipment for free or for a fee, much like they do with DSL or cable modems.

- ***WiMAX***: Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use. It is described in the IEEE standard 802.16. WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers. To access a WiMAX network, subscribers must subscribe to an ISP with a WiMAX tower within 30 miles of their location. They also need some type of WiMAX receiver and a special encryption code to get access to the base station.

- ***Satellite Internet***: Typically, rural users use this type of technology where cable and DSL are not available. A VSAT provides two-way (upload and download) data communications. The upload speed is about one-tenth of the 500 kb/s download speed. Cable and DSL have higher download speeds, but satellite systems are about 10 times faster than an analog modem. To access satellite Internet services, subscribers need a satellite dish, two modems (uplink and downlink), and coaxial cables between the dish and the modem.

Figure 1-33 displays an example of a WiMAX network.

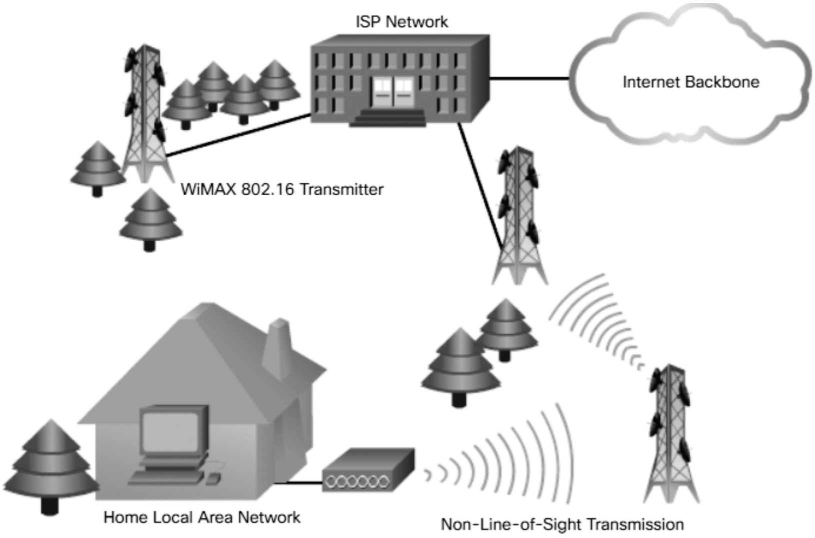


Figure 1-33 Sample Wireless Topology

3G/4G Cellular (1.2.3.4)

Increasingly, cellular service is another wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available, as shown in Figure 1-34. Many users with smartphones and tablets can use cellular data to email, surf the web, download apps, and watch videos.

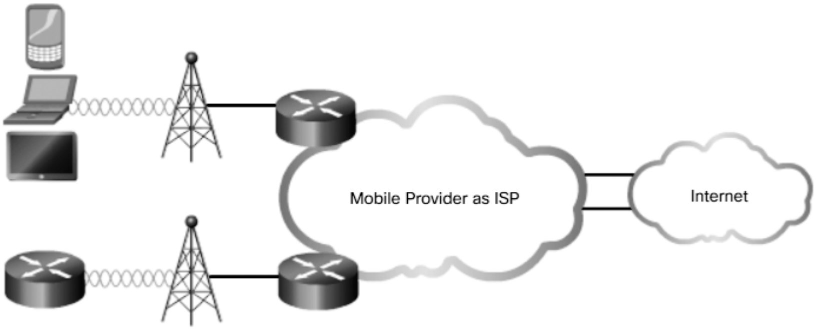


Figure 1-34 Sample Cellular Topology

Phones, tablet computers, laptops, and even some routers can communicate through to the Internet using cellular technology. These devices use radio waves to communicate through a nearby mobile phone tower. The device has a small radio antenna, and the provider has a much larger antenna sitting at the top of a tower somewhere within miles of the phone.

These are two common cellular industry terms:

- ***3G/4G Wireless***: Abbreviation for third-generation and fourth-generation cellular access. These technologies support wireless Internet access.
- ***Long-Term Evolution (LTE)***: Refers to a newer and faster technology and is considered to be part of fourth-generation (4G) technology.

VPN Technology (1.2.3.5)

Security risks are incurred when a ***teleworker*** or a remote office worker uses a broadband service to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using VPN connections to a network device that accepts VPN connections, which are typically located at the corporate site.

A VPN is an encrypted connection between private networks over a public network, such as the Internet. Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host.

Using VPN offers several benefits:

- **Cost savings:** VPNs enable organizations to use the global Internet to connect remote offices, and to connect remote users to the main corporate site. This eliminates expensive, dedicated WAN links and modem banks.
- **Security:** VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability:** Because VPNs use the Internet infrastructure within ISPs and devices, it is easy to add new users. Corporations are able to add large amounts of capacity without adding significant infrastructure.
- **Compatibility with broadband technology:** VPN technology is supported by broadband service providers such as DSL and cable. VPNs allow mobile workers and telecommuters to take advantage of their home high-speed Internet service to access their corporate networks. Business-grade, high-speed broadband connections can also provide a cost-effective solution for connecting remote offices.

There are two types of VPN access:

- ***Site-to-site VPNs***: Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network, as shown in Figure 1-35. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. In the Figure 1-35, a remote branch office uses a site-to-site-VPN to connect with the corporate head office.

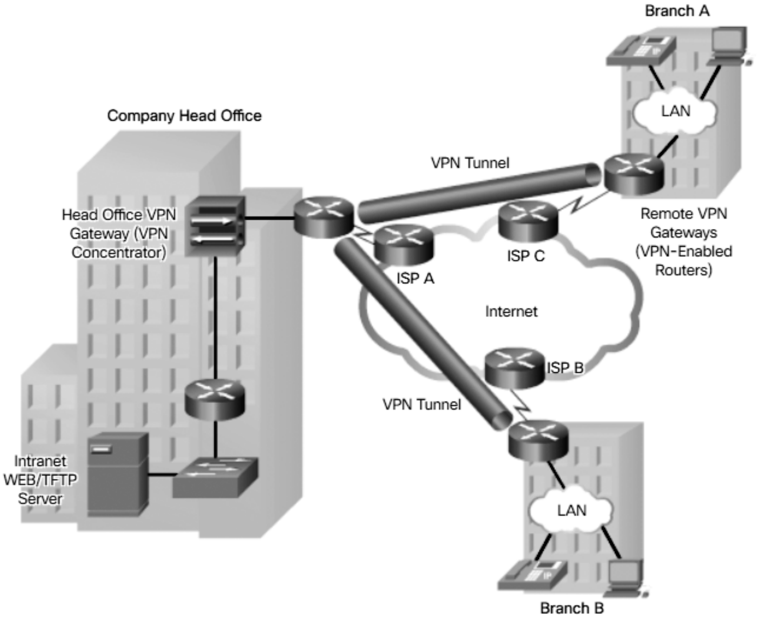


Figure 1-35 Sample Site-to-Site VPN Topology

- *Remote-access VPNs*: Remote-access VPNs enable individual hosts, such as telecommuters, mobile users, and extranet consumers, to access a company network securely over the Internet. Each host (Teleworker 1 and Teleworker 2) typically has VPN client software loaded or uses a web-based client, as shown in Figure 1-36.

Interactive Graphic

Activity 1.2.3.6: Identify Public WAN Infrastructure Terminology

Refer to the online course to complete this activity.

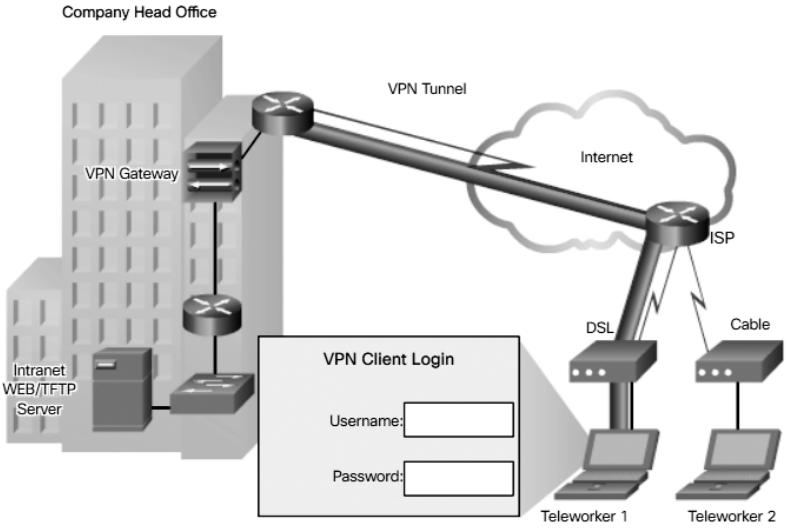


Figure 1-36 Sample Remote-Access VPN Topology

Selecting WAN Services (1.2.4)

In this topic, you learn how to select the appropriate WAN protocol and service for a specific network requirement.

Choosing a WAN Link Connection (1.2.4.1)

There are many important factors to consider when choosing an appropriate WAN connection. For a network administrator to decide which WAN technology best meets the requirements of a specific business, he or she must answer the following questions:

What is the purpose of the WAN?

There are a few issues to consider:

- Will the enterprise connect local branches in the same city area, connect remote branches, or connect to a single branch?
- Will the WAN be used to connect internal employees, or external business partners and customers, or all three?
- Will the enterprise connect to customers, connect to business partners, connect to employees, or some combination of these?
- Will the WAN provide authorized users limited or full access to the company intranet?

What is the geographic scope?

There are a few issues to consider:

- Is the WAN local, regional, or global?
- Is the WAN one-to-one (single branch), one-to-many branches, or many-to-many (distributed)?

What are the traffic requirements?

There are a few issues to consider:

- What type of traffic must be supported (data only, VoIP, video, large files, streaming files)? This determines the quality and performance requirements.
- What volume of traffic type (voice, video, or data) must be supported for each destination? This determines the bandwidth capacity required for the WAN connection to the ISP.
- What Quality of Service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.
- What are the security requirements (data integrity, confidentiality, and security)? These are important factors if the traffic is of a highly confidential nature, or if it provides essential services, such as emergency response.

Choosing a WAN Link Connection (Cont.) (1.2.4.2)

In addition to gathering information about the scope of the WAN, the administrator must also determine the following:

- **Should the WAN use a private or public infrastructure?** A private infrastructure offers the best security and confidentiality, whereas the public Internet infrastructure offers the most flexibility and lowest ongoing expense. The choice depends on the purpose of the WAN, the types of traffic it carries, and available operating budget. For example, if the purpose is to provide a nearby branch with high-speed secure services, a private dedicated or switched connection may be best. If the purpose is to connect many remote offices, a public WAN using the Internet may be the best choice. For distributed operations, a combination of options may be the solution.
- **For a private WAN, should it be dedicated or switched?** Real-time, high-volume transactions have special requirements that could favor a dedicated line, such as traffic flowing between the data center and the corporate head office. If the enterprise is connecting to a local single branch, a dedicated leased line could

be used. However, that option would become very expensive for a WAN connecting multiple offices. In that case, a switched connection might be better.

- **For a public WAN, what type of VPN access is required?** If the purpose of the WAN is to connect a remote office, a site-to-site VPN may be the best choice. To connect teleworkers or customers, remote-access VPNs are a better option. If the WAN is serving a mixture of remote offices, teleworkers, and authorized customers, such as a global company with distributed operations, a combination of VPN options may be required.

- **Which connection options are available locally?** In some areas, not all WAN connection options are available. In this case, the selection process is simplified, although the resulting WAN may provide less than optimal performance. For example, in a rural or remote area, the only option may be VSAT or cellular access.

- **What is the cost of the available connection options?** Depending on the option chosen, the WAN can be a significant ongoing expense. The cost of a particular option must be weighed against how well it meets the other requirements. For example, a dedicated leased line is the most expensive option, but the expense may be justified if it is critical to ensure secure transmission of high volumes of real-time data. For less demanding applications, a less expensive switched or Internet connection option may be more suitable.

Using the preceding guidelines, as well as those described by the Cisco Enterprise Architecture, a network administrator should be able to choose an appropriate WAN connection to meet the requirements of different business scenarios.

Lab 1.2.4.3: Researching WAN Technologies

In this lab, you will complete the following objectives:

Part 1: Investigate Dedicated WAN Technologies and Providers

Part 2: Investigate a Dedicated Leased-Line Service Provider in Your Area

Summary (1.3)

Class Activity 1.3.1.1: WAN Device Modules

Your medium-sized company is upgrading its network. To make the most of the equipment currently in use, you decide to purchase WAN modules instead of new equipment.

All branch offices use either Cisco 1900 or 2911 series ISRs. You will be updating these routers in several locations. Each branch has its own ISP requirements to consider.

To update the devices, focus on the following WAN module access types:

- Ethernet
- Broadband
- T1/E1 and ISDN PRI
- BRI
- Serial
- T1 and E1 Trunk Voice and WAN
- Wireless LANs and WANs

A business can use private lines or the public network infrastructure for WAN connections. A public infrastructure connection can be a cost-effective alternative to a private connection between LANs, as long as security is also planned.

WAN access standards operate at Layers 1 and 2 of the OSI model, and are defined and managed by the TIA/EIA, ISO, and IEEE. A WAN may be circuit-switched or packet-switched.

There is common terminology used to identify the physical components of WAN connections and who, the service provider or the customer, is responsible for which components.

Service provider networks are complex, and the service provider's backbone networks consist primarily of high-bandwidth fiber-optic media. The device used for interconnection to a customer is specific to the WAN technology that is implemented.

Permanent, dedicated point-to-point connections are provided by using leased lines. Dialup access, although slow, is still viable for remote areas with limited WAN options. Other private connection options include ISDN, Frame Relay, ATM, Ethernet WAN, MPLS, and VSAT.

Public infrastructure connections include DSL, cable, wireless, and 3G/4G cellular. Security over public infrastructure connections can be provided by using remote-access or site-to-site VPNs.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Connecting Networks Labs & Study Guide* (ISBN 9781587134296). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

Class Activity 1.0.1.2: Branching Out

Class Activity 1.3.1.1: WAN Device Modules

Labs

Lab 1.2.4.3: Researching WAN Technologies

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix "Answers to the 'Check Your Understanding' Questions" lists the answers.

1. A small company with 10 employees uses a single LAN to share information between computers. Which type of connection to the Internet would be appropriate for this company?

   A. A broadband service, such as DSL, through the company's local service provider

   B. A dialup connection that is supplied by the local telephone service provider

   C. Private dedicated lines through the local service provider

   D. A VSAT connection to a service provider

2. Which network scenario will require the use of a WAN?

   A. Employee workstations need to obtain dynamically assigned IP addresses.

   B. Employees in the branch office need to share files with the headquarters office that is located in a separate building on the same campus network.

   C. Employees need to access web pages that are hosted on the corporate web servers in the DMZ within their building.

   D. Employees need to connect to the corporate email server through a VPN while traveling.

3. Which statement describes a characteristic of a WAN?

   A. A WAN operates within the same geographic scope of a LAN but has serial links.

   B. A WAN provides end-user network connectivity to the campus backbone.

   C. All serial links are considered WAN connections.

   D. WAN networks are owned by service providers.

4. Which two devices are needed when a digital leased line is used to provide a connection between the customer and the service provider? (Choose two.)

   A. Access server

   B. CSU

   C. Dialup modem

   D. DSU

   E. Layer 2 switch

5. What is a requirement of a connectionless packet-switched network?

   A. A virtual circuit is created for the duration of the packet delivery.

   B. Each packet has to carry only an identifier.

   C. Full addressing information must be carried in each data packet.

   D. The network predetermines the route for a packet.

6. What is an advantage of packet-switched technology over circuit-switched technology?

   A. Packet-switched networks are less susceptible to jitter than circuit-switched networks are.

   B. Packet-switched networks can efficiently use multiple routes inside a service provider network.

C. Packet-switched networks do not require an expensive permanent connection to each endpoint.

D. Packet-switched networks usually experience lower latency than circuit-switched networks experience.

7. What is a long-distance fiber-optic media technology that supports both SONET and SDH, and assigns incoming optical signals to specific wavelengths of light?

A. ATM

B. DWDM

C. ISDN

D. MPLS

8. What is the recommended technology to use over a public WAN infrastructure when a branch office is connected to the corporate site?

A. ATM

B. ISDN

C. Municipal Wi-Fi

D. VPN

9. What are two common high-bandwidth fiber-optic media standards? (Choose two.)

A. ANSI

B. ATM

C. ITU

D. SDH

E. SONET

10. Which WAN technology establishes a dedicated constant point-to-point connection between two sites?

A. ATM

B. Frame Relay

C. ISDN

D. Leased lines

11. A hospital is looking for a solution to connect multiple, newly established remote branch medical offices. Which consideration is important when selecting a private WAN connection rather than a public WAN connection?

    A. Data security and confidentiality during transmission

    B. Higher data transmission rate

    C. Lower cost

    D. Website and file exchange service support

12. A new corporation needs a data network that must meet certain requirements. The network must provide a low-cost connection to salespeople dispersed over a large geographical area. Which two types of WAN infrastructure would meet the requirements? (Choose two.)

    A. Dedicated

    B. Internet

    C. Private infrastructure

    D. Public infrastructure

    E. Satellite

13. Which wireless technology provides Internet access through cellular networks?

    A. LTE

    B. Municipal Wi-Fi

    C. Satellite

    D. WiMAX

14. Which equipment is needed for an ISP to provide Internet connections through cable service?

    A. Access server

    B. CMTS

    C. CSU/DSU

    D. DSLAM

15. A customer needs a WAN virtual connection that provides high-speed, dedicated bandwidth between two sites. Which type of WAN connection would best fulfill this need?

    A. Circuit-switched network

    B. Ethernet WAN

    C. MPLS

    D. Packet-switched network

CHAPTER 2

Point-to-Point Connections

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are the fundamentals of point-to-point serial communication across a WAN?
- How do you configure HDLC encapsulation on a point-to-point serial link?
- What are differences between PPP and HDLC?
- What is the PPP-layered architecture?
- What are the functions of LCP and NCP?
- How does PPP establish a session?
- How do you configure PPP encapsulation on a point-to-point serial link?
- How do you configure PPP authentication?
- How do you troubleshoot PPP using **show** and **debug** commands?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

High-Level Data Link Control (HDLC)   *Page 51*

Point-to-Point Protocol (PPP)   *Page 51*

serial connection   *Page 52*

parallel connection   *Page 52*

clock skew   *Page 53*

parallel ports   *Page 53*

RS-232 serial ports   *Page 53*

universal serial bus (USB) interfaces   *Page 53*

digital signal level (DS)   *Page 54*

synchronous circuits   *Page 57*

asynchronous circuits   *Page 57*

Password Authentication Protocol (PAP)   *Page 57*

Challenge Handshake Authentication Protocol (CHAP)   *Page 57*

Serial Line Internet Protocol (SLIP)   *Page 57*

X.25   *Page 57*

Link Access Procedure, Balanced (LAPB)   *Page 57*

bit-oriented   *Page 57*

Synchronous Data Link Control (SDLC)   *Page 57*

Carrier Detect (CD) signal   *Page 60*

keepalives   *Page 60*

trunk lines   *Page 64*

Link Control Protocol (LCP)   *6 Page 4*

Network Control Protocols (NCPs)   *Page 64* *link quality management (LQM)* *Page 65*

IP Control Protocol (IPCP) *Page 66*

IPv6 uses IPv6 Control Protocol (IPv6CP) *Page 66*

link-establishment frames *Page 69*

link-maintenance frames *Page 69*

link-termination frames *Page 69*

PPP callback *Page 74*

Multilink PPP *Page 74*

Message Digest 5 (MD5) *Page 85*

Introduction (2.0)

One of the most common types of WAN connections, especially in long-distance communications, is a point-to-point connection, also called a serial or leased-line connection. Because these connections are typically provided by a carrier, such as a telephone company, boundaries between what is managed by the carrier and what is managed by the customer must be clearly established.

This chapter covers the terms, technology, and protocols used in serial connections. The ***High-Level Data Link Control (HDLC)*** and ***Point-to-Point Protocol (PPP)*** are introduced. HDLC is the default protocol on a Cisco router serial interface. PPP is a protocol that is able to handle authentication, compression, and error detection; monitor link quality; and logically bundle multiple serial connections together to share the load.

Class Activity 2.0.1.2: PPP Persuasion

Your network engineering supervisor recently attended a networking conference where Layer 2 protocols were discussed. He knows that you have Cisco equipment on the premises, but he would also like to offer security and advanced TCP/IP options and controls on that same equipment by using the Point-to-Point Protocol (PPP).

After researching the PPP protocol, you find it offers some advantages over the HDLC protocol, currently used on your network.

Create a matrix listing the advantages and disadvantages of using the HDLC versus PPP protocols. When comparing the two protocols, include

- Ease of configuration
- Adaptability to nonproprietary network equipment
- Security options
- Bandwidth usage and compression
- Bandwidth consolidation

Share your chart with another student or class. Justify whether or not you would suggest sharing the matrix with the network engineering supervisor to justify a change being made from HDLC to PPP for Layer 2 network connectivity.

Serial Point-to-Point Overview (2.1)

In this section, you learn how to configure HDLC encapsulation.

Serial Communications (2.1.1)

In this topic, you learn the fundamentals of point-to-point serial communication across a WAN.

Serial and Parallel Ports (2.1.1.1)

A common type of WAN connection is the point-to-point connection. As shown in Figure 2-1, point-to-point connections are used to connect LANs to service provider WANs and to connect LAN segments within an enterprise network.

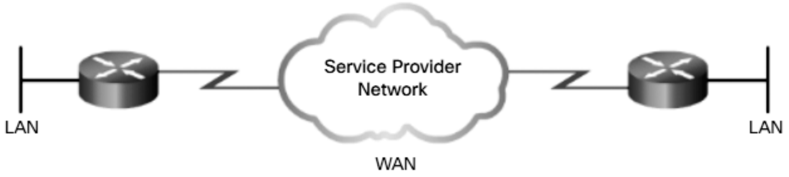


Figure 2-1 Serial Point-to-Point Connection

A LAN-to-WAN point-to-point connection is also referred to as a *serial connection* or *leased-line connection*. The reason is that the lines are leased from a carrier (usually a telephone company) and are dedicated for use by the company leasing the lines. Companies pay for a continuous connection between two remote sites, and the line is continuously active and available. Leased lines are a frequently used type of WAN access, and they are generally priced based on the bandwidth required and the distance between the two connected points.

Understanding how point-to-point serial communication across a leased line works is important to an overall understanding of how WANs function.

Communication across a serial connection is a method of data transmission in which the bits are transmitted sequentially over a single channel. Imagine the task of moving balls from one bin to another via a pipe only wide enough to fit one ball at a time. Multiple balls can go into the pipe, but only one at a time, and they have only one exit point, the other end of the pipe. A serial port is bidirectional and often referred to as a bidirectional port or a communications port.

This serial communication is in contrast to parallel communications in which bits can be transmitted simultaneously over multiple wires. Figure 2-2 illustrates the difference between serial and parallel connections.

A parallel connection theoretically transfers data eight times faster than a *serial connection*. Based on this theory, a *parallel connection* sends a byte (eight bits) in the time that a serial connection sends a single bit. However, parallel communications do have issues with crosstalk across wires, especially as the wire length increases.

Clock skew is also an issue with parallel communications. Clock skew occurs when data across the various wires does not arrive at the same time, creating synchronization issues. Finally, many parallel communications support only one-direction, outbound-only communication, but some support half-duplex communication (two-way communication, but only one way at a time).

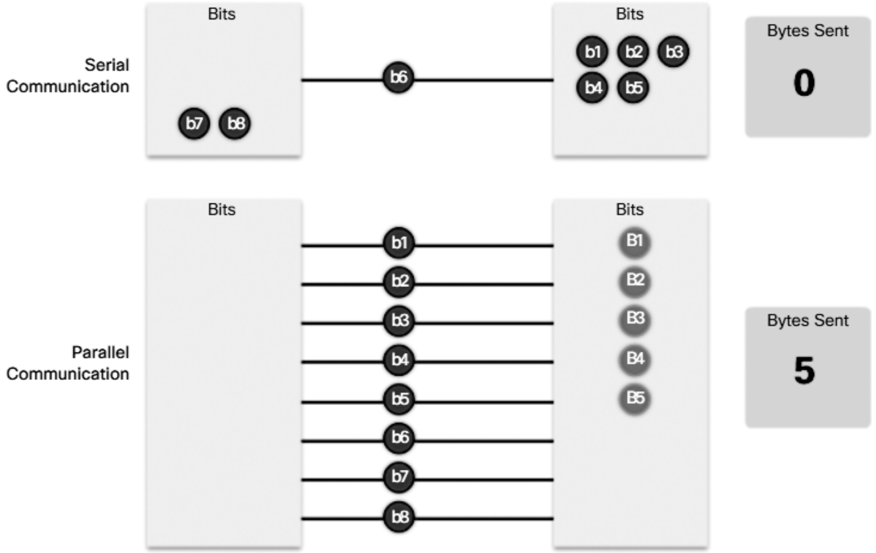


Figure 2-2 Serial and Parallel Communication

At one time, most PCs included both serial and parallel ports. Parallel ports were used to connect printers, computers, and other devices that required relatively high bandwidth. Parallel ports were also used between internal components. For external communications, a serial bus was primarily used to connect to phone lines and devices that could potentially be a further distance than a parallel transfer would allow. Because serial communications are less complex and require simpler circuitry, serial communications are considerably less expensive to implement. Serial communications use fewer wires, cheaper cables, and fewer connector pins.

On most PCs, *parallel ports* and *RS-232 serial ports* have been replaced by the higher speed serial *universal serial bus (USB) interfaces*. For long-distance communication, many WANs also use serial transmission.

Point-to-Point Communication Links (2.1.1.2)

When permanent dedicated connections are required, a point-to-point link is used to provide a single, pre-established WAN communications path. This path goes from the customer premises, through the provider network, to a remote destination, as shown in Figure 2-3.

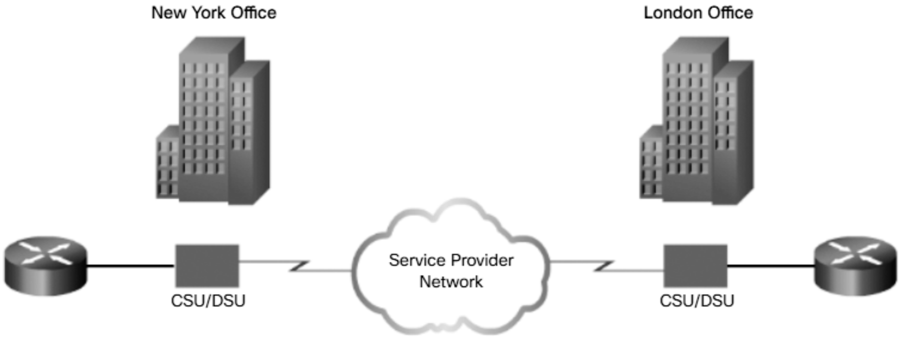


Figure 2-3 Point-to-Point Communication Links

A point-to-point link can connect two geographically distant sites, such as a corporate office in New York and a regional office in London. For a point-to-point line, the carrier dedicates specific resources for a line that is leased by the customer (leased line).

Note

Point-to-point connections are not limited to connections that cross land. Hundreds of thousands of miles of undersea fiber-optic cables connect countries and continents worldwide. An Internet search of "undersea Internet cable map" produces several cable maps of these undersea connections.

Point-to-point links are usually more expensive than shared services. The cost of leased-line solutions can become significant when used to connect many sites over increasing distances; however, sometimes the benefits outweigh the cost of the leased line. The dedicated capacity removes latency or jitter between the endpoints. Constant availability is essential for some applications such as voice or video over IP.

Serial Bandwidth (2.1.1.3)

Bandwidth refers to the rate at which data is transferred over the communication link. The underlying carrier technology will dictate how much bandwidth is available. There is a difference in bandwidth points between the North American (T-carrier) specification and the European (E-carrier) system. Optical networks also use a different bandwidth hierarchy, which again differs between North America and Europe. In the United States, optical carrier (OC) defines the bandwidth points.

In North America, the bandwidth is usually expressed as a ***digital signal level (DS)*** number (DS0, DS1, and so on), which refers to the rate and format of the signal. The most fundamental line speed is 64 kb/s, or DS0, which is the bandwidth required for an uncompressed, digitized phone call. Serial connection bandwidths can be incrementally increased to accommodate the need for faster transmission. For example, 24

DS0s can be bundled to get a DS1 line (also called a T1 line) with a speed of 1.544 Mb/s. Also, 28 DS1s can be bundled to get a DS3 line (also called a T3 line) with a speed of 44.736 Mb/s. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

OC transmission rates are a set of standardized specifications for the transmission of digital signals carried on SONET fiber-optic networks. The designation uses OC, followed by an integer value representing the base transmission rate of 51.84 Mb/s. For example, OC-1 has a transmission capacity of 51.84 Mb/s, whereas an OC-3 transmission medium would be three times 51.84 Mb/s or 155.52 Mb/s.

Table 2-1 lists the most common line types and the associated bit rate capacity of each.

Table 2-1 Serial Line Bandwidth Capacities

Line Type	Bit Rate Capacity
56	56 kb/s
64	64 kb/s
T1	1.544 Mb/s
E1	2.048 Mb/s
J1	2.048 Mb/s
E3	34.064 Mb/s
T3	44.736 Mb/s
OC-1	51.84 Mb/s
OC-3	155.54 Mb/s
OC-9	466.56 Mb/s
OC-12	622.08 Mb/s
OC-18	933.12 Mb/s
OC-24	1.244 Gb/s
OC-36	1.866 Gb/s
OC-48	2.488 Gb/s
OC-96	4.976 Gb/s
OC-192	9.954 Gb/s
OC-768	39.813 Gb/s

Note

E1 (2.048 Mb/s) and E3 (34.368 Mb/s) are European standards like T1 and T3, but with different bandwidths and frame structures.

HDLC Encapsulation (2.1.2)

In this topic, you configure HDLC encapsulation on a point-to-point serial link.

WAN Encapsulation Protocols (2.1.2.1)

On each WAN connection, data is encapsulated into frames before crossing the WAN link. To ensure that the correct protocol is used, you must configure the appropriate Layer 2 encapsulation type. The choice of protocol depends on the WAN technology and the communicating equipment. Figure 2-4 displays the more common WAN protocols and where they are used.

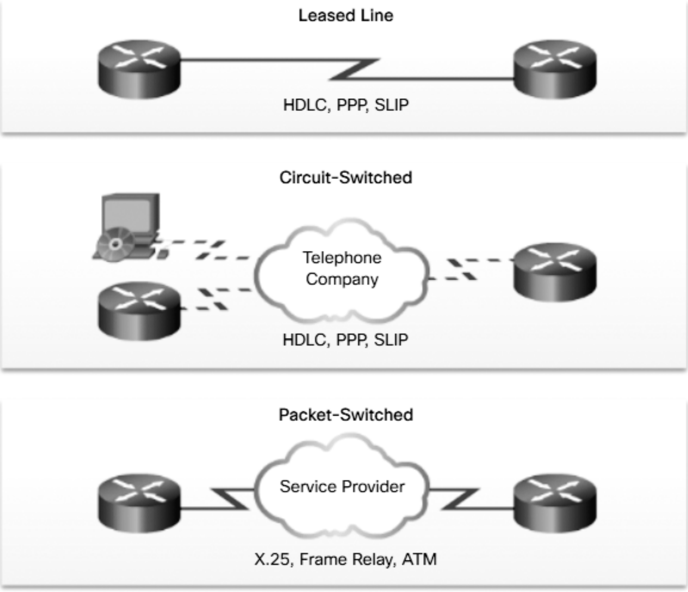


Figure 2-4 WAN Encapsulation Protocols

The following are short descriptions of each type of WAN protocol:

- **HDLC:** This protocol is the default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices. HDLC is now the basis for synchronous PPP used by many servers to connect to a WAN, most commonly the Internet.

- **PPP:** This protocol provides router-to-router and host-to-network connections over *synchronous circuits* and *asynchronous circuits*. PPP works with several network layer protocols, such as IPv4 and IPv6. PPP is based on the HDLC encapsulation protocol but also has built-in security mechanisms such as *Password Authentication Protocol (PAP)* and *Challenge Handshake Authentication Protocol (CHAP).*
- *Serial Line Internet Protocol (SLIP)*: This standard protocol for point-to-point serial connections uses TCP/IP. SLIP has been largely displaced by PPP.
- *X.25*: This ITU-T standard defines how connections between a DTE and DCE are maintained for remote terminal access and computer communications in public data networks. X.25 specifies *Link Access Procedure, Balanced (LAPB)*, a data link layer protocol. X.25 is a predecessor to Frame Relay.
- **Frame Relay:** This industry standard, switched, data link layer protocol handles multiple virtual circuits. Frame Relay is a next-generation protocol after X.25. Frame Relay eliminates some of the time-consuming processes (such as error correction and flow control) employed in X.25.
- **ATM:** This is the international standard for cell relay in which devices send multiple service types, such as voice, video, or data, in fixed-length (53-byte) cells. Fixed-length cells allow processing to occur in hardware, thereby reducing transit delays. ATM takes advantage of high-speed transmission media such as E3, SONET, and T3.

HDLC and PPP are the focus of this course. The other WAN protocols listed are considered either legacy technologies or beyond the scope of this course.

HDLC Encapsulation (2.1.2.2)

HDLC is a *bit-oriented* synchronous data link layer protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC was developed from the *Synchronous Data Link Control (SDLC)* standard proposed in the 1970s. HDLC provides both connection-oriented and connectionless service.

HDLC uses synchronous serial transmission to provide error-free communication between two points. HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments. Each frame has the same format, whether it is a data frame or a control frame.

When frames are transmitted over synchronous or asynchronous links, those links have no mechanism to mark the beginning or end of frames. For this reason, HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame.

Cisco has developed an extension to the HLDC protocol to solve the inability to provide multiprotocol support. Although Cisco HLDC (also referred to as cHDLC) is proprietary, Cisco has allowed many other network equipment vendors to implement it. Cisco HDLC frames contain a field for identifying the network protocol being encapsulated. Figure 2-5 compares standard HLDC to Cisco HLDC.

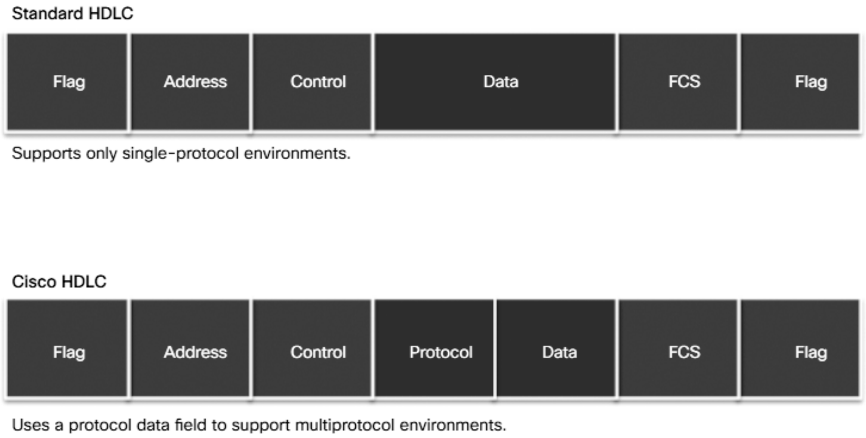

Standard HDLC
Flag
Address
Control
Data
FCS
Flag
Supports only single-protocol environments.
Cisco HDLC
Flag
Address
Control
Protocol
Data
FCS
Flag
Uses a protocol data field to support multiprotocol environments.

Figure 2-5 Standard and Cisco HDLC Frame Format

Configuring HDLC Encapsulation (2.1.2.3)

Cisco HDLC is the default encapsulation method that Cisco devices use on synchronous serial lines.

Use Cisco HDLC as a Point-to-Point Protocol on leased lines between two Cisco devices. If connecting non-Cisco devices, use synchronous PPP.

If the default encapsulation method has been changed, use the **encapsulation hdlc** interface configuration mode command to re-enable HDLC.

Example 2-1 displays how to re-enable HDLC on a serial interface.

Example 2-1 Configuring HDLC Encapsulation

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation hdlc
```

Troubleshooting a Serial Interface (2.1.2.4)

The output of the **show interfaces serial** command displays information specific to serial interfaces. Add the specific interface number you want to investigate, such as **show interface serial 0/0/0**.

When HDLC is configured, “encapsulation HDLC” should be reflected in the output, as highlighted in Example 2-2.

Example 2-2 Verifying a Serial Interface

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:05, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing 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)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 1017 bytes, 0 no buffer
     Received 5 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4 packets output, 395 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

The highlighted section, “Serial 0/0/0 is up, line protocol is up,” indicates that the line is up and functioning while the “encapsulation HDLC” highlighted section indicates that the default serial encapsulation (HDLC) is enabled.

The **show interfaces serial** command returns one of six possible states:

- Serial x is up, line protocol is up
- Serial x is down, line protocol is down (DTE mode)
- Serial x is up, line protocol is down (DTE mode)
- Serial x is up, line protocol is down (DCE mode)
- Serial x is up, line protocol is up (looped)
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

Of the seven possible states, six are problem states. Table 2-2 lists the six possible problem states, the issues associated with the problem states, and how to troubleshoot a problem state.

Table 2-2 Troubleshooting a Serial Interface

Line State	Possible Condition(s)	Problem/Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	■ The router is not sensing a *Carrier Detect (CD) signal*. ■ A WAN service provider problem has occurred, which means the line is down or is not connected to CSU/DSU. ■ Cabling is faulty or incorrect. ■ Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active. 2. Verify that the proper cable and interface are being used. 3. Contact the service provider to see whether a problem has occurred. 4. Swap faulty parts. 5. Use another serial line to see if the connection comes up, indicating the previously connected interface has a problem.
Serial x is up, line protocol is down (DTE mode)	■ A local or remote router is misconfigured. ■ *Keepalives* are not being sent by the remote router. ■ A leased-line or other carrier service problem has occurred, which means a noisy line or misconfigured or failed switch.	1. Many DCE devices (e.g., modems and CSU/DSUs) have a local loopback self-check mechanism to verify the connection between the DCE and DTE (e.g., router). Enable this mechanism and use the **show interfaces serial** command on the router. If the line protocol comes up between the DCE and DTE, the problem is most likely a WAN service provider problem. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote DCE.

Line State	Possible Condition(s)	Problem/Solution
	- A timing problem has occurred on the cable. - A local or remote CSU/DSU has failed. - Router hardware, which could be either local or remote, has failed.	3. Verify that the correct cabling has been used and that the DTE is correctly connected to the DCE and that the DCE is correctly connected to the service provider network-termination point. Use the **show controllers** EXEC command to determine which cable is attached to which interface. 4. Enable the **debug serial interface** EXEC command. 5. If the line protocol comes up and the keepalive counter increments, the problem is not in the local router. 6. If the line protocol does not come up in local loopback mode, and the **debug serial interface** command output does not indicate incrementing keepalives, a router hardware problem is likely. Swap the router interface hardware. 7. If faulty router hardware is suspected, change the serial line to an unused port. If the connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DCE mode)	- The **clockrate** interface configuration command is missing. - The DTE device does not support the DCE timing. - The remote CSU or DSU has failed.	1. Add the **clockrate** *bps* interface configuration command on the serial interface. Use the question mark (**?**) to verify valid *bps* values. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote DCE. 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. 5. Replace faulty parts as necessary.
Serial x is up, line protocol is up (looped)	- A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	1. Use the **show running-config** privileged EXEC command to look for any loopback interface configuration command entries. 2. If there is a loopback interface configuration command entry, use the **no loopback interface** global configuration command to remove the loopback.

Line State	Possible Condition(s)	Problem/Solution
		3. If there is no loopback interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. After disabling loopback mode on the CSU/DSU, reset the CSU/DSU and inspect the line status. If the line protocol comes up, no other action is needed. 5. If, upon inspection, the CSU or DSU cannot be manually set, contact the leased-line or other carrier service for line troubleshooting assistance.
Serial x is up, line protocol is down (disabled)	■ A high error rate has occurred due to a WAN service provider problem. ■ A CSU or DSU hardware problem has occurred. ■ Router hardware (interface) is bad.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a WAN service provider problem. 3. Swap out bad hardware as required (CSU, DSU, switch, local or remote router).
Serial x is administratively down, line protocol is down	■ The router configuration includes the **shutdown** interface configuration command. ■ A duplicate IP address exists.	1. Check the router configuration for the **shutdown** command. 2. Use the **no shutdown** interface configuration command to remove the **shutdown** command. 3. Verify that there are no identical IP addresses using the **show running-config** privileged EXEC command or the **show interfaces** EXEC command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

The **show controllers** command is another important diagnostic tool when troubleshooting serial lines, as shown in Example 2-3.

Example 2-3 Verifying the Controller Settings

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
<output omitted>
```

The output indicates the state of the interface channels and whether a cable is attached to the interface. In the example, interface serial 0/0/0 has a V.35 DCE cable attached. The command syntax varies, depending on the platform.

Note

Cisco 7000 series routers use a cBus controller card for connecting serial links. With these routers, use the **show controllers cbus** command.

If the electrical interface output displays as "UNKNOWN" instead of "V.35," "EIA/TIA-449," or some other electrical interface type, the likely problem is an improperly connected cable. A problem with the internal wiring of the card is also possible. If the electrical interface is unknown, the corresponding display for the **show interfaces serial** command shows that the interface and line protocol are down.

Packet Tracer
□ **Activity**

Packet Tracer 2.1.2.5: Troubleshooting Serial Interfaces

Background/Scenario

You have been asked to troubleshoot WAN connections for a local telephone company (telco). The telco router is supposed to communicate with four remote sites, but none of them are working. Use your knowledge of the OSI model and a few general rules to identify and repair the errors in the network.

PPP Operation (2.2)

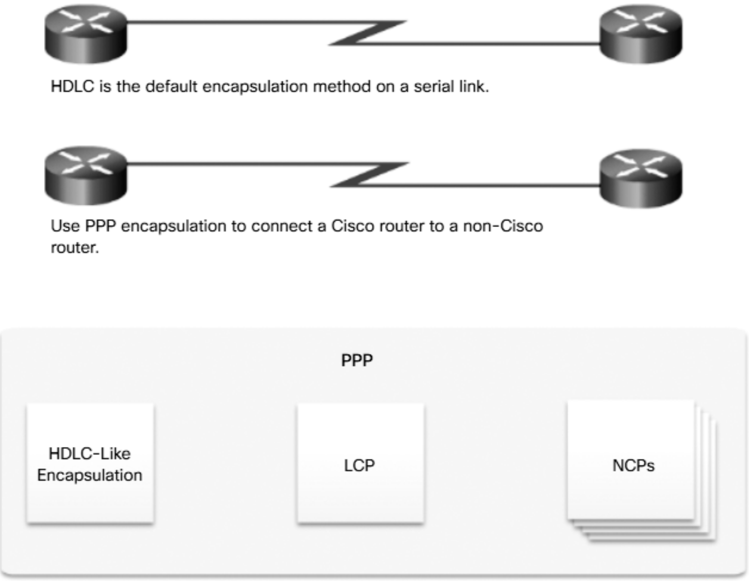
In this section, you learn how PPP operates across a point-to-point serial link.

Benefits of PPP (2.2.1)

In this topic, you learn how to compare PPP with HDLC.

Introducing PPP (2.2.1.1)

HDLC is the default serial encapsulation method when connecting two Cisco routers. With an added protocol type field, the Cisco version of HDLC is proprietary. Therefore, Cisco HDLC can work only with other Cisco devices. However, as shown in Figure 2-6, use PPP encapsulation when you need to connect to a non-Cisco router.



HDLC is the default encapsulation method on a serial link.

Use PPP encapsulation to connect a Cisco router to a non-Cisco router.

Figure 2-6 What Is PPP?

PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits. PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware. PPP encapsulates data frames for transmission over Layer 2 physical links. It establishes a direct connection using serial cables, phone lines, ***trunk lines***, cellular telephones, specialized radio links, or fiber-optic links.

PPP contains three main components:

- HDLC-like framing for transporting multiprotocol packets over point-to-point links.
- *Link Control Protocol (LCP)* for establishing, configuring, and testing the data-link connection.
- Family of *Network Control Protocols (NCPs)* for establishing and configuring different network layer protocols. PPP allows the simultaneous use of multiple network layer protocols. The most common NCPs are IPv4 Control Protocol and IPv6 Control Protocol.

Note

Other NCPs include AppleTalk Control Protocol, Novell IPX Control Protocol, Cisco Systems Control Protocol, SNA Control Protocol, and Compression Control Protocol.

Advantages of PPP (2.2.1.2)

PPP originally emerged as an encapsulation protocol for transporting IPv4 traffic over point-to-point links. It provides a standard method for transporting multiprotocol packets over point-to-point links.

There are many advantages to using PPP, including the fact that it is not proprietary. PPP includes many features not available in HDLC:

- The *link quality management (LQM)* feature monitors the quality of the link. LQM can be configured with the interface command **ppp quality** *percentage*. If the error percentage falls below the configured threshold, the link is taken down and packets are rerouted or dropped.
- PPP supports PAP and CHAP authentication. This feature is explained and configured in the next section.

LCP and NCP (2.2.2)

In this topic, you learn about the PPP-layered architecture and the functions of LCP and NCP.

PPP-Layered Architecture (2.2.2.1)

A layered architecture is a logical model, design, or blueprint that aids in communication between interconnecting layers. Figure 2-7 maps the layered architecture of PPP against the Open System Interconnection (OSI) model. PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently.

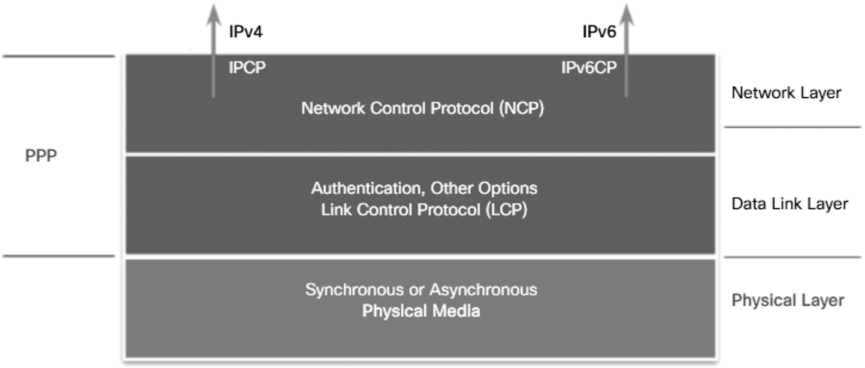

IPv4
IPv6
IPCP
IPv6CP
Network Control Protocol (NCP)
Network Layer
PPP
Authentication, Other Options
Link Control Protocol (LCP)
Data Link Layer
Synchronous or Asynchronous
Physical Media
Physical Layer

Figure 2-7 PPP-Layered Architecture: Physical Layer

At the physical layer, you can configure PPP on a range of interfaces. The only absolute requirement imposed by PPP is that it can operate using a full-duplex circuit. The physical layer standards are transparent to PPP link layer frames. PPP does not impose any restrictions regarding transmission rate.

Most of the work done by PPP happens at the data link and network layers, by LCP and NCPs.

PPP: Link Control Protocol (LCP) (2.2.2.2)

LCP functions within the data link layer and has a role in establishing, configuring, and testing the data link connection. LCP establishes the point-to-point link. LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs, as shown in Figure 2-7.

LCP provides automatic configuration of the interfaces at each end:

- Handling varying limits on packet size
- Detecting common misconfiguration errors
- Terminating the link
- Determining when a link is functioning properly or when it is failing

After the link is established, PPP also uses LCP to agree automatically on encapsulation formats such as authentication, compression, and error detection.

PPP: Network Control Protocol (NCP) (2.2.2.3)

PPP permits multiple network layer protocols to operate on the same communications link. For every network layer protocol used, PPP uses a separate NCP, as shown in Figure 2-7. For example, IPv4 uses *IP Control Protocol (IPCP)* and IPv6 uses *IPv6 Control Protocol (IPv6CP)*.

NCPs include functional fields containing standardized codes to indicate the network layer protocol that PPP encapsulates. Table 2-3 lists the PPP protocol field numbers. Each NCP manages the specific needs required by its respective network layer protocols. The various NCP components encapsulate and negotiate options for multiple network layer protocols.

Table 2-3 Protocol Field Names

Value (in Hex)	Protocol Name
8021	Internet Protocol (IPv4) Control Protocol
8057	Internet Protocol version 6 (IPv6) Control Protocol
8023	OSI Network Layer Control Protocol

Value (in Hex)	Protocol Name
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c223	Challenge Handshake Authentication Protocol

PPP Frame Structure (2.2.2.4)

A PPP frame consists of six fields. The following descriptions summarize the PPP frame fields illustrated in Figure 2-8:

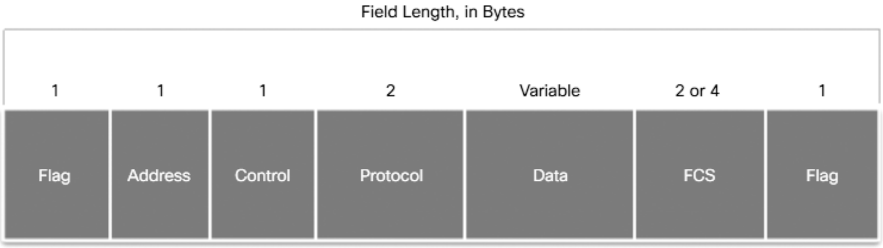


Figure 2-8 PPP Frame Fields

- **Flag:** A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110.
- **Address:** A single byte that contains the binary sequence 11111111, the standard broadcast address. PPP does not assign individual station addresses.
- **Control:** A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
- **Protocol:** Two bytes that identify the protocol encapsulated in the information field of the frame. The 2-byte Protocol field identifies the protocol of the PPP payload.
- **Data:** Zero or more bytes that contain the datagram for the protocol specified in the protocol field.
- **Frame Check Sequence (FCS):** This is normally 16 bits (2 bytes). If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded.

LCPs can negotiate modifications to the standard PPP frame structure. Modified frames, however, are always distinguishable from standard frames.

Interactive Graphic

Activity 2.2.2.5: Identify PPP Features and Operations

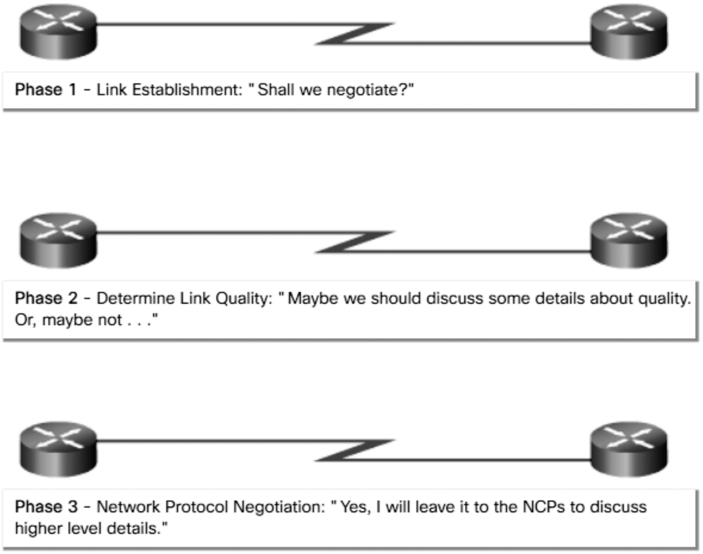
Refer to the online course to complete this activity.

PPP Sessions (2.2.3)

In this topic, you learn how PPP establishes a session.

Establishing a PPP Session (2.2.3.1)

Establishing a PPP session entails three phases, as shown in Figure 2-9 and described in the list that follows.



Phase 1 - Link Establishment: "Shall we negotiate?"

Phase 2 - Determine Link Quality: "Maybe we should discuss some details about quality. Or, maybe not . . ."

Phase 3 - Network Protocol Negotiation: "Yes, I will leave it to the NCPs to discuss higher level details."

Figure 2-9 Establishing a PPP Session

- **Phase 1: Link establishment and configuration negotiation:** Before PPP exchanges any network layer datagrams, such as IP, the LCP must first open the connection and negotiate configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.
- **Phase 2: Link quality determination (optional):** The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.

The LCP can delay transmission of network layer protocol information until this phase is complete.

- **Phase 3: Network layer protocol configuration negotiation:** After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time. If the LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

The link remains configured for communications until explicit LCP or NCP frames close the link, or until some external event occurs such as an inactivity timer expiring or an administrator intervening.

The LCP can terminate the link at any time. This is usually done when one of the routers requests termination but can happen because of a physical event, such as the loss of a carrier or the expiration of an idle-period timer.

LCP Operation (2.2.3.2)

LCP operation includes provisions for link establishment, link maintenance, and link termination. LCP operation uses three classes of LCP frames to accomplish the work of each of the LCP phases:

- *Link-establishment frames* establish and configure a link (Configure-Request, Configure-Ack, Configure-Nak, and Configure-Reject).
- *Link-maintenance frames* manage and debug a link (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request).
- *Link-termination frames* terminate a link (Terminate-Request and Terminate-Ack).

Link Establishment

Link establishment is the first phase of LCP operation, as seen in Figure 2-10. This phase must complete successfully before any network layer packets can be exchanged. During link establishment, the LCP opens the connection and negotiates the configuration parameters. The link-establishment process starts with the initiating device sending a Configure-Request frame to the responder. The Configure-Request frame includes a variable number of configuration options needed to set up on the link.

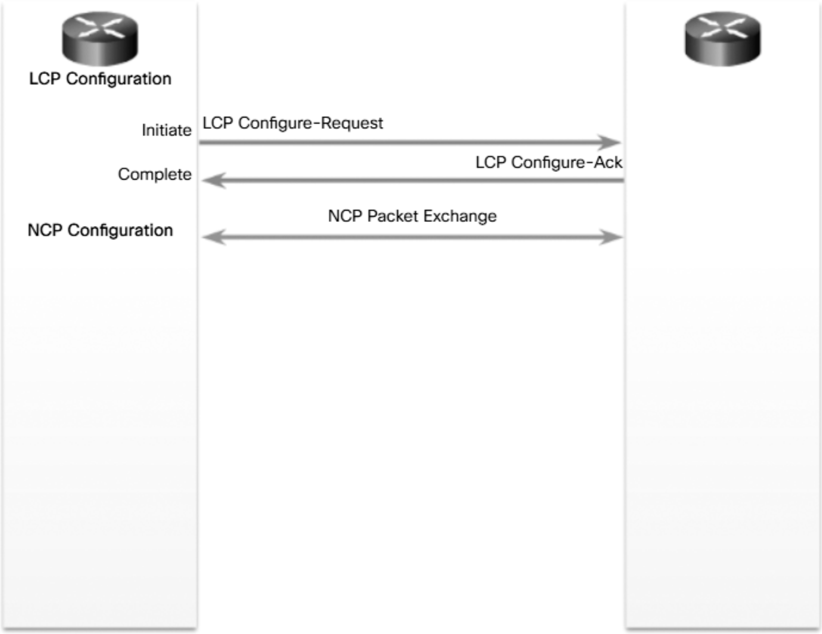


Figure 2-10 PPP Link Establishment

The initiator includes the options for how it wants the link created, including protocol or authentication parameters. The responder processes the request:

- If the options are not acceptable or not recognized, the responder sends a Configure-Nak or Configure-Reject message. If this occurs and the negotiation fails, the initiator must restart the process with new options.
- If the options are acceptable, the responder responds with a Configure-Ack message and the process moves on to the authentication stage. The operation of the link is handed over to the NCP.

When NCP has completed all necessary configurations, including validating authentication if configured, the line is available for data transfer. During the exchange of data, LCP transitions into link maintenance.

Link Maintenance

During link maintenance, LCP can use messages to provide feedback and test the link, as shown in Figure 2-11:

- **Echo-Request, Echo-Reply, and Discard-Request:** These frames can be used for testing the link.

- **Code-Reject and Protocol-Reject:** These frame types provide feedback when one device receives an invalid frame. The sending device will resend the packet.

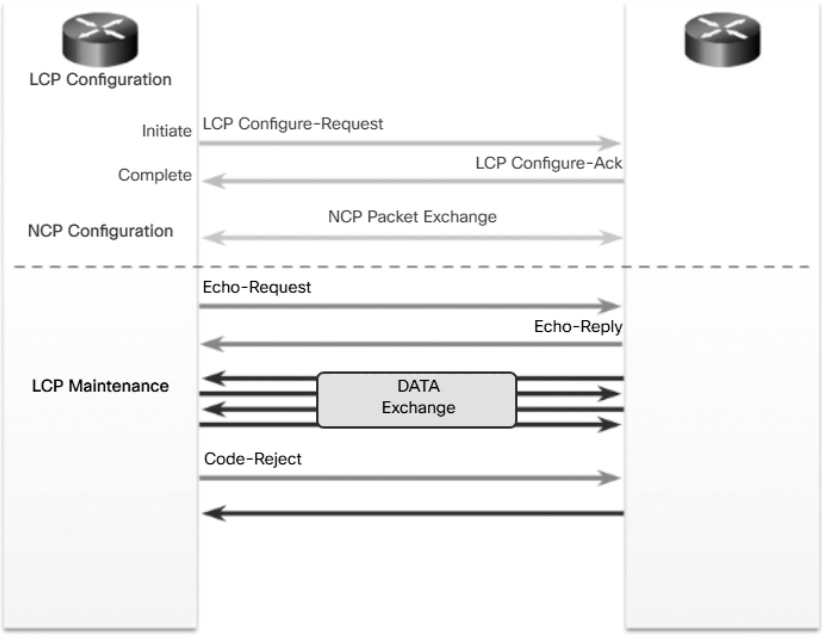


Figure 2-11 PPP Link Maintenance

Link Termination

After the transfer of data at the network layer completes, the LCP terminates the link, as shown in Figure 2-12. NCP terminates only the network layer and NCP link. The link remains open until the LCP terminates it. If the LCP terminates the link before NCP, the NCP session is also terminated.

PPP can terminate the link at any time. This might happen because of the loss of the carrier, authentication failure, link quality failure, the expiration of an idle-period timer, or the administrative closing of the link. The LCP closes the link by exchanging Terminate packets. The device initiating the shutdown sends a Terminate-Request message. The other device replies with a Terminate-Ack. A termination request indicates that the device sending it needs to close the link. When the link is closing, PPP informs the network layer protocols so that they may take appropriate action.

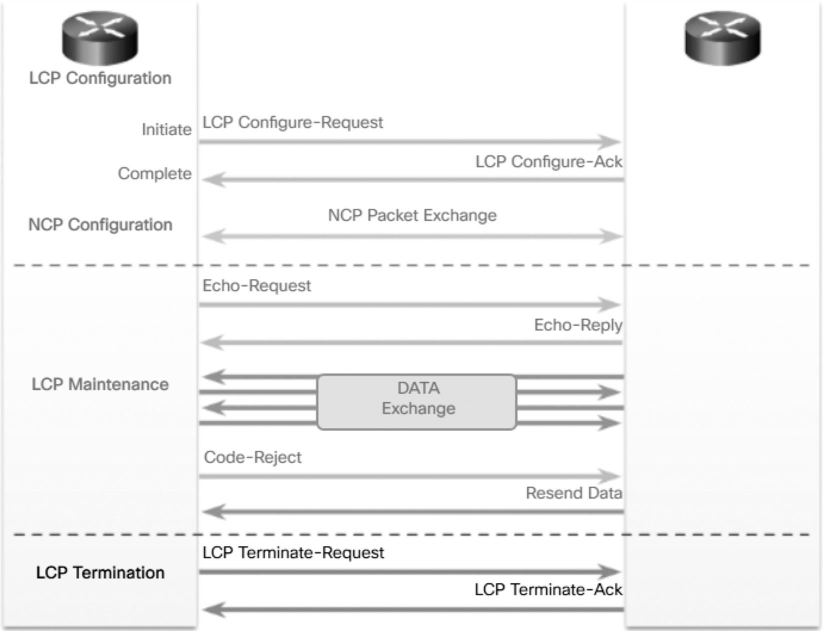


Figure 2-12 PPP Link Termination

PPP Configuration Options (2.2.3.3)

PPP can be configured to support various optional functions. There are three optional functions:

- Authentication using either PAP or CHAP
- Compression using either Stacker or Predictor
- Multilink that combines two or more channels to increase the WAN bandwidth

NCP Explained (2.2.3.4)

After the LCP has configured and authenticated the basic link, the appropriate NCP is invoked to complete the specific configuration of the network layer protocol being used. When the NCP has successfully configured the network layer protocol, the network protocol is in the open state on the established LCP link. At this point, PPP can carry the corresponding network layer protocol packets.

IPCP Example

As an example of how the NCP layer works, Figure 2-13 shows the NCP configuration of IPv4. After LCP has established the link, the routers exchange IPCP messages, negotiating options specific to IPv4. IPCP is responsible for configuring, enabling, and disabling the IPv4 modules on both ends of the link.

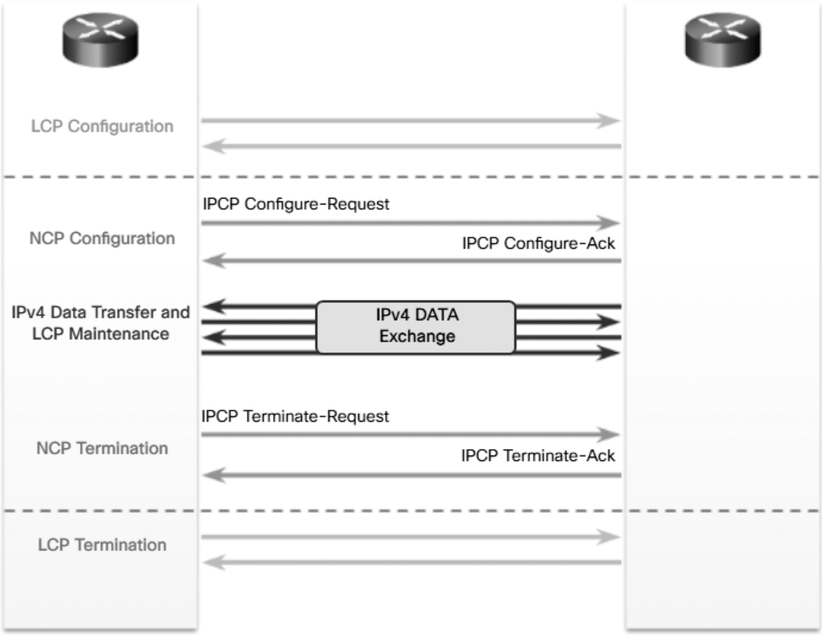


Figure 2-13 PPP NCP Operation

IPCP negotiates two options:

- **Compression:** Allows devices to negotiate an algorithm to compress TCP and IP headers and save bandwidth. The Van Jacobson TCP/IP header compression reduces the size of the TCP/IP headers to as few as 3 bytes. This can be a significant improvement on slow serial lines, particularly for interactive traffic.
- **IPv4-Address:** Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder. Prior to the advent of broadband technologies such as DSL and cable modem services, dialup network devices commonly used the IPv4 address option.

After the NCP process is complete, the link goes into the open state and LCP takes over again in a link maintenance phase. Link traffic consists of any possible combination of LCP, NCP, and network layer protocol packets. When data transfer is complete, NCP terminates the protocol link and LCP terminates the PPP connection.

Interactive Graphic

Activity 2.2.3.5: Identify the Steps in the LCP Link Negotiation Process

Refer to the online course to complete this activity.

PPP Implementation (2.3)

In this section, you learn how to configure PPP encapsulation.

Configure PPP (2.3.1)

In this topic, you configure PPP encapsulation on a point-to-point serial link.

PPP Configuration Options (2.3.1.1)

The previous section introduced configurable LCP options to meet specific WAN connection requirements. PPP may include several LCP options:

- **Authentication:** Peer routers exchange authentication messages. Two authentication choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- **Compression:** This option increases the effective throughput on PPP connections by reducing the number of bits that must travel across the link. The protocol decompresses the frame at its destination. Two compression protocols available in Cisco routers are Stacker and Predictor.
- **Error detection:** This option identifies fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link. The Magic Number field helps in detecting links that are in a looped-back condition. Until the Magic-Number Configuration Option has been successfully negotiated, the Magic-Number must be transmitted as zero. Magic numbers are generated randomly at each end of the connection.
- ***PPP callback*****:** PPP callback is used to enhance security. With this LCP option, a Cisco router can act as a callback client or a callback server. The client makes the initial call, requests that the server call it back, and terminates its initial call. The callback router answers the initial call and makes the return call to the client based on its configuration statements.
- ***Multilink PPP*****:** This alternative provides load balancing over the router interfaces that PPP uses. Multilink PPP, also referred to as MP, MPPP, MLP, or Multilink, provides a method for spreading traffic across multiple physical WAN links while providing packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic.

When options are configured, a corresponding field value is inserted into the LCP option field, as shown in Table 2-4.

Table 2-4 PPP Configuration Options

Option Name	Option Type	Option Length	Description
Maximum Receive Unit (MRU)	1	4	MRU is the maximum size of a PPP frame and cannot exceed 65,535. The default is 1500, and if neither peer is changing the default, it is not negotiated.
Asynchronous Control Character Map (ACCM)	2	6	This is a bitmap that enables character escapes for asynchronous links. By default, character escapes are used.
Authentication Protocol	3	5 or 6	This field indicates the authentication protocol, either PAP or CHAP.
Magic Number	5	6	This is a random number chosen to distinguish a peer and detect looped-back lines.
Protocol Compression	7	2	This flag indicates that the PPP protocol ID be compressed to a single octet when the 2-byte protocol ID is in the range 0x00-00 to 0x00-FF.
Address and Control Field Compression	8	2	This flag indicates that the PPP Address field (always set to 0xFF) and the PPP Control field (always set to 0x03) be removed from the PPP header.
Callback	13 or 0x0D	3	This 1-octet indicator determines how callback is to be determined.

PPP Basic Configuration Command (2.3.1.2)

To set PPP as the encapsulation method used by a serial interface, use the **encapsulation ppp** interface configuration command. The command has no arguments. Remember that if PPP is not configured on a Cisco router, the default encapsulation for serial interfaces is HDLC.

Figure 2-14 shows a two-router topology used to demonstrate PPP configuration.

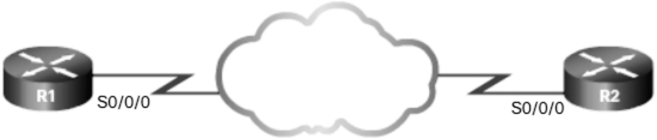


Figure 2-14 PPP Basic Configuration

Example 2-4 shows the configuration for R1 and R2 with both an IPv4 and an IPv6 address on the serial interfaces. PPP is a Layer 2 encapsulation that supports various Layer 3 protocols including IPv4 and IPv6.

Example 2-4 R1 and R2 PPP Basic Configuration

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
```

PPP Compression Commands (2.3.1.3)

Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled. Because this option invokes a software compression process, it can affect system performance. If the traffic already consists of compressed files, such as .zip, .tar, or .mpeg, do not use this option.

Use the **compress** [**predictor** | **stac**] interface configuration command to enable PPP compression.

Table 2-5 shows the options for the **compress** command.

Table 2-5 PPP **compress** Command

Keyword	Description
predictor	(Optional) Specifies that a predicator compression algorithm will be used
stac	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used

Example 2-5 shows the configuration for R1 and R2 to use predictor compression.

Example 2-5 R1 and R2 PPP Compression Configuration

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 compress predictor
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 compress predictor
```

PPP Link Quality Monitoring Command (2.3.1.4)

LCP provides an optional link quality determination phase. In this phase, LCP tests the link to determine whether the link quality is sufficient to use Layer 3 protocols.

The **ppp quality** *percentage* interface configuration command ensures that the link meets the quality requirement set; otherwise, the link closes down. The *percentage* value specifies the link quality threshold using a range between 1 and 100.

The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent, to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.

If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. LQM implements a time lag so that the link does not bounce up and down.

The configuration **ppp quality 80**, shown in Example 2-6, sets minimum quality to 80 percent.

Example 2-6 R1 and R2 PPP Link Quality Configuration

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 compress predictor
 ppp quality 80
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 compress predictor
 ppp quality 80
```

PPP Multilink Commands (2.3.1.5)

Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) provides a method for spreading traffic across multiple physical WAN links. Multilink PPP also provides packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic.

MPPP allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address. The multiple physical links come up in response to a user-defined load threshold. MPPP can measure the load on just inbound traffic or on just outbound traffic, but not on the combined load of both inbound and outbound traffic.

Figure 2-15 shows a PPP multilink topology.

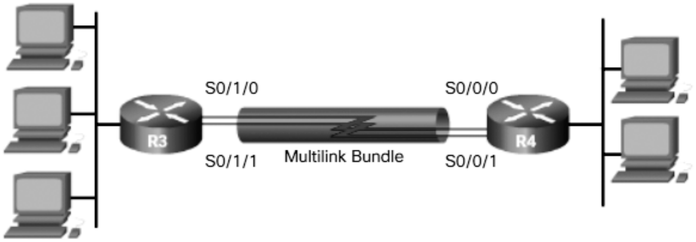


Figure 2-15 PPP Multilink

Configuring MPPP requires two steps:

Step 1. Create a multilink bundle.

- Use the **interface multilink** *number* global configuration command to create the multilink interface.
- In interface configuration mode, assign an IPv4 and/or IPv6 address to the multilink interface.
- Use the **ppp multilink** interface configuration command to enable multilink PPP.
- Use the **ppp multilink group** *number* interface configuration command to assign the multilink group number.

Step 2. Assign each physical interface to the multilink bundle.

- Use the **ppp encapsulation** interface configuration command to enable PPP.
- Use the **ppp multilink** interface configuration command to enable multilink PPP.
- Use the **ppp multilink group** *number* interface configuration command to assign the multilink group number.

Example 2-7 shows the configuration for R3 and R4.

Example 2-7 R3 and R4 PPP Multilink Configuration

```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

To disable PPP multilink, use the **no ppp multilink** interface configuration command on each of the bundled interfaces.

Verifying PPP Configuration (2.3.1.6)

Use the **show interfaces serial** command to verify proper configuration of HDLC or PPP encapsulation. The command output in Example 2-8 shows a PPP configuration.

Example 2-8 Verifying the Serial PPP Encapsulation Configuration

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing 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)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1944 packets input, 67803 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1934 packets output, 67718 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     1 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     8 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

R2#
```

When you configure HDLC, the output of the **show interfaces serial** command should display “encapsulation HDLC.” When PPP is configured, the command also displays the LCP and NCP states. Notice that NCPs IPCP and IPV6CP are open for IPv4 and IPv6 because R1 and R2 were configured with both IPv4 and IPv6 addresses.

Table 2-6 summarizes commands used when verifying PPP.

Table 2-6 PPP Verification Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router
show interfaces serial	Displays information about a serial interface
show ppp multilink	Displays information about a PPP multilink interface

The **show ppp multilink** command verifies that PPP multilink is enabled on R3, as shown in Example 2-9. The output indicates the interface Multilink 1, the hostnames of both the local and remote endpoints, and the serial interfaces assigned to the multilink bundle.

Example 2-9 Verifying PPP Multilink Configuration

```
R3# show ppp multilink
Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

Configure PPP Authentication (2.3.2)

In this topic, you configure PPP authentication.

PPP Authentication Protocols (2.3.2.1)

PPP defines an LCP that allows negotiation of an authentication protocol for authenticating its peer before allowing network layer protocols to transmit over the link. RFC 1334, *PPP Authentication Protocols*, defines two protocols for authentication, PAP and CHAP, as shown in Figure 2-16.

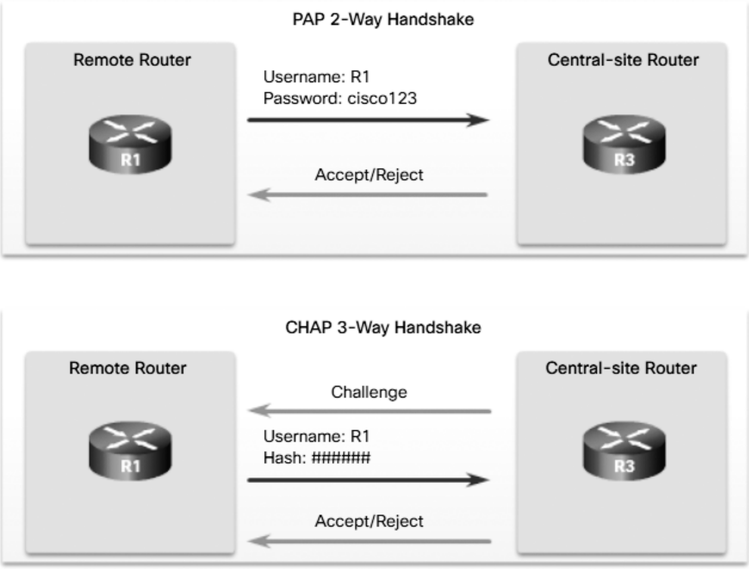


Figure 2-16 PPP Authentication Protocols

PAP is a basic two-way process. There is no encryption. The username and password are sent in plaintext. If it is accepted, the connection is allowed. CHAP is more secure than PAP. It involves a three-way exchange of a shared secret.

The authentication phase of a PPP session is optional. If used, the peer is authenticated after LCP establishes the link and chooses the authentication protocol. Authentication takes place before the network layer protocol configuration phase begins.

The authentication options require that the calling side of the link provide authentication information. This helps ensure that the user has the permission of the network administrator to make the call. Peer routers exchange authentication messages.

Password Authentication Protocol (PAP) (2.3.2.2)

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. PAP is not interactive. When the **ppp authentication pap** interface configuration command is used, the username and password are sent as one LCP data package, as shown in Figure 2-17, rather than one PPP device sending a login prompt and waiting for a response as in some authentication mechanisms.

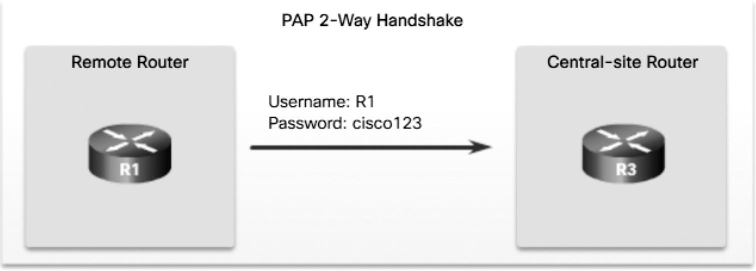
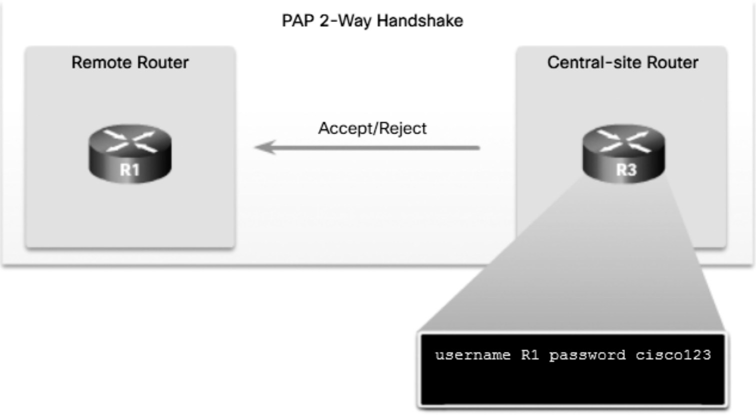


Figure 2-17 Initiating PAP

PAP Process

After PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link until the receiving node acknowledges it or terminates the connection.

At the receiving node, the device running PPP checks the username-password. This device either allows or denies the connection. An accept or reject message is returned to the requester, as shown in Figure 2-18.



```
username R1 password cisco123
```

Figure 2-18 Completing PAP

PAP is not a strong authentication protocol. Using PAP, passwords are sent across the link in plaintext, and there is no protection from playback or repeated trial-and-error attacks. The remote node is in control of the frequency and timing of the login attempts.

Nonetheless, using PAP can be justified sometimes. Despite its shortcomings, PAP may be used in the following environments:

- A large installed base of client applications that do not support CHAP
- Incompatibilities between different vendor implementations of CHAP
- Situations in which a plaintext password must be available to simulate a login at the remote host

Challenge Handshake Authentication Protocol (CHAP) (2.3.2.3)

PAP authenticates only once. After authentication is established with PAP, it does not re-authenticate, thus leaving the network vulnerable to attack.

CHAP is more secure as it conducts periodic challenges to make sure that the remote node still has a valid password value. The password value is variable and changes unpredictably while the link exists.

CHAP is configured using the **ppp authentication chap** interface configuration command.

CHAP Process

After the PPP link establishment phase is complete, the local router sends a challenge message to the remote node, as shown in Figure 2-19.

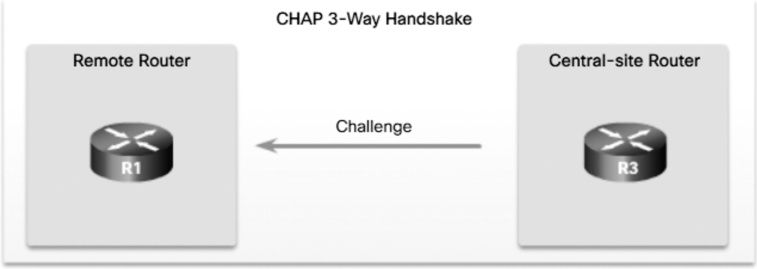


Figure 2-19 Initiating CHAP

The remote node responds with a value that is calculated using a one-way hash function. This is typically *Message Digest 5 (MD5)* based on the password and challenge message, as shown in Figure 2-20.

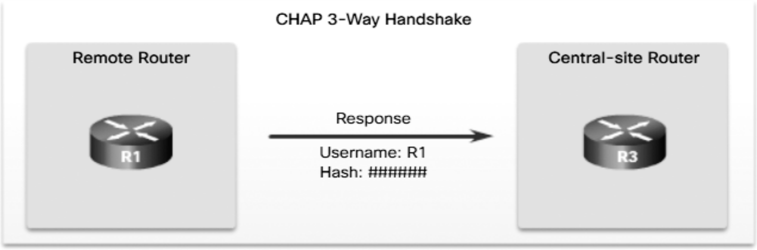
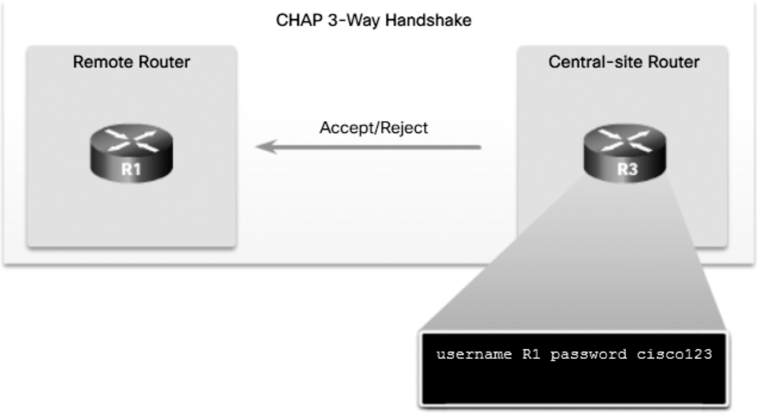


Figure 2-20 Responding CHAP

The local router checks the response against its own calculation of the expected hash value. If the values match, the initiating node acknowledges the authentication, as shown in Figure 2-21. If the values do not match, the initiating node immediately terminates the connection.



```
username R1 password cisco123
```

Figure 2-21 Completing CHAP

CHAP provides protection against a playback attack by using a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value is also unique and random. The use of repeated challenges limits the time of exposure to any single attack. The local router, or a third-party authentication server, is in control of the frequency and timing of the challenges.

PPP Authentication Command (2.3.2.4)

PAP, CHAP, or both can be enabled. If both methods are enabled, the first method specified is requested during link negotiation. If the peer suggests using the second method or simply refuses the first method, the second method should be tried. Some remote devices support CHAP only and some PAP only. The order in which you specify the methods is based on your concerns about the ability of the remote device to correctly negotiate the appropriate method as well as your concern about data line security.

To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** {**chap** | **chap pap** | **pap chap** | **pap**} interface configuration command.

Table 2-7 shows the description for each keyword in the **ppp authentication** command.

Table 2-7 The **ppp authentication** Command

Keyword	Description
chap	Enables CHAP on a serial interface
pap	Enables PAP on a serial interface
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP

Use the **no** form of the command to disable this authentication.

Configuring PPP with Authentication (2.3.2.5)

Figure 2-22 displays the two-router topology used for demonstrating PPP authentication configurations.

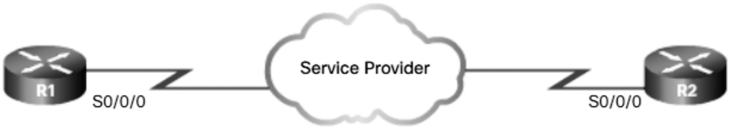


Figure 2-22 PAP and CHAP Configuration Topology

Configuring PAP Authentication

Example 2-10 shows a two-way PAP authentication configuration. Both routers authenticate and are authenticated, so the PAP authentication commands mirror each other. Use the **ppp pap sent-username** *name* **password** *password* interface configuration command to specify the username and password parameters that a router will send. This username and password combination must match those specified with the **username** *name* **password** *password* command of the other receiving router.

Example 2-10 R1 and R2 PAP Configuration

```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password sameone
```

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password sameone
```

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. This is done only on initial link establishment. The hostname on one router must match the username the other router has configured for PPP. The passwords must also match.

Configuring CHAP Authentication

Always configure CHAP instead of PAP because CHAP is more secure than PAP. CHAP periodically verifies the identity of the remote node using a three-way handshake. The hostname on one router must match the username the other router has configured. The passwords must also match. This occurs on initial link establishment and can be repeated any time after the link has been established.

Example 2-11 shows a CHAP configuration.

Example 2-11 R1 and R2 CHAP Configuration

```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```

Notice how the CHAP configuration is also simpler than PAP.

Packet Tracer
□ Activity

Packet Tracer 2.3.2.6: Configuring PAP and CHAP Authentication

Background/Scenario

In this activity, you practice configuring PPP encapsulation on serial links. You also configure PPP PAP authentication and PPP CHAP authentication.

Lab 2.3.2.7: Configuring Basic PPP with Authentication

In this lab, you complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure PPP Encapsulation
- Part 3: Configure PPP CHAP Authentication

Troubleshoot WAN Connectivity (2.4)

In this section, you learn how to troubleshoot PPP.

Troubleshoot PPP (2.4.1)

In this topic, you troubleshoot PPP using **show** and **debug** commands.

Troubleshooting PPP Serial Encapsulation (2.4.1.1)

The privileged EXEC mode **debug** command is very useful for troubleshooting. The command generates real-time output information about various router operations, related traffic generated or received by the router, and any error messages.

However, the **debug** command is a resource-intensive process. It can consume a significant amount of CPU resources as the router is forced to process-switch the packets being debugged. Therefore, the **debug** command is not something we enable to regularly monitor the network. The command is meant to be used for a short period of time when troubleshooting. Therefore, always remember to disable **debug** commands using the **no debug** or **undebug all** privileged EXEC command.

Use the **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **compression**} privileged EXEC mode command to display information about the operation of PPP.

Table 2-8 describes the options for the **debug ppp** command.

Table 2-8 Options for the **debug ppp** Command

Keyword	Description
packet	Displays PPP packets being sent and received.
negotiation	Displays PPP packets transmitted during PPP startup. It is useful to see how PPP options are negotiated.
error	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
authentication	Displays PAP and CHAP authentication protocol messages.
compression	Displays information specific to the exchange of PPP connections using packet compression.

Use the **no** form of this command to disable debugging output.

Use the **debug ppp** command when trying to search the following:

- NCPs that are supported on either end of a PPP connection
- Any loops that might exist in a PPP internetwork
- Nodes that are (or are not) properly negotiating PPP connections
- Errors that have occurred over the PPP connection
- Causes for CHAP session failures
- Causes for PAP session failures

- Information specific to the exchange of PPP connections using the Callback Control Protocol (CBCP), used by Microsoft clients
- Incorrect packet sequence number information where MPPC compression is enabled

Debugging PPP (2.4.1.2)

A useful command to use when troubleshooting serial interface encapsulation is the **debug ppp packet** privileged EXEC mode command, as shown Example 2-12.

Example 2-12 debug ppp packet Command Output

```
R1# debug ppp packet
PPP packet display debugging is on
R1#
*Apr  1 16:15:17.471: Se0/0/0 LQM: O state Open magic 0x1EFC37C3 len 48
*Apr  1 16:15:17.471: Se0/0/0 LQM:    LastOutLQRs 70 LastOutPackets/Octets 194/9735
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerInLQRs 70 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerOutLQRs 71 PeerOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 PPP: I pkt type 0xC025, datagramsize 52 link[ppp]
*Apr  1 16:15:17.487: Se0/0/0 LQM: I state Open magic 0xFE83D624 len 48
*Apr  1 16:15:17.487: Se0/0/0 LQM:    LastOutLQRs 71 LastOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 LQM:    PeerInLQRs 71 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:17.487: Se0/0/0 LQM:    PeerOutLQRs 71 PeerOutPackets/Octets 196/9809
*Apr  1 16:15:17.535: Se0/0/0 LCP: O ECHOREQ [Open] id 36 len 12 magic 0x1EFC37C3
*Apr  1 16:15:17.539: Se0/0/0 LCP-FS: I ECHOREP [Open] id 36 len 12 magic
  0xFE83D624
*Apr  1 16:15:17.539: Se0/0/0 LCP-FS: Received id 36, sent id 36, line up
*Apr  1 16:15:18.191: Se0/0/0 PPP: I pkt type 0xC025, datagramsize 52 link[ppp]
*Apr  1 16:15:18.191: Se0/0/0 LQM: I state Open magic 0xFE83D624 len 48
*Apr  1 16:15:18.191: Se0/0/0 LQM:    LastOutLQRs 71 LastOutPackets/Octets 197/9839
*Apr  1 16:15:18.191: Se0/0/0 LQM:    PeerInLQRs 71 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:18.191: Se0/0/0 LQM:    PeerOutLQRs 72 PeerOutPackets/Octets 198/9883
*Apr  1 16:15:18.191: Se0/0/0 LQM: O state Open magic 0x1EFC37C3 len 48
*Apr  1 16:15:18.191: Se0/0/0 LQM:    LastOutLQRs 72 LastOutPackets/Octets 198/9883
*Apr  1 16:15:18.191: Se0/0/0 LQM:    PeerInLQRs 72 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:18.191: Se0/0/0 LQM:    PeerOutLQRs 72 PeerOutPackets/Octets 199/9913
*Apr  1 16:15:18.219: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 36 len 12 magic
  0xFE83D624
*Apr  1 16:15:18.219: Se0/0/0 LCP-FS: O ECHOREP [Open] id 36 len 12 magic
  0x1EFC37C3
R1# un all
```

The example depicts packet exchanges under normal PPP operation.

The **debug ppp negotiation** privileged EXEC mode command enables the network administrator to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution.

Example 2-13 displays the output of the **debug ppp negotiation** command in a normal negotiation, where both sides agree on NCP parameters.

Example 2-13 Output of **debug ppp negotiation** Command

```
R1# debug ppp negotiation
PPP protocol negotiation debugging is on
R1#
*Apr  1 18:42:29.831: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Apr  1 18:42:29.831: Se0/0/0 PPP: Sending cstate UP notification
*Apr  1 18:42:29.831: Se0/0/0 PPP: Processing CstateUp message
*Apr  1 18:42:29.835: PPP: Alloc Context [66A27824]
*Apr  1 18:42:29.835: ppp2 PPP: Phase is ESTABLISHING
*Apr  1 18:42:29.835: Se0/0/0 PPP: Using default call direction
*Apr  1 18:42:29.835: Se0/0/0 PPP: Treating connection as a dedicated line
*Apr  1 18:42:29.835: Se0/0/0 PPP: Session handle[4000002] Session id[2]
*Apr  1 18:42:29.835: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
*Apr  1 18:42:29.835: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 23
*Apr  1 18:42:29.835: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    QualityType 0xC025 period 1000
  (0x0408C025000003E8)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    MagicNumber 0x1F887DD3 (0x05061F887DD3)
<Output omitted>
*Apr  1 18:42:29.855: Se0/0/0 PPP: Phase is AUTHENTICATING, by both
*Apr  1 18:42:29.855: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from “R1”
<Output omitted>
*Apr  1 18:42:29.871: Se0/0/0 IPCP: Authorizing CP
*Apr  1 18:42:29.871: Se0/0/0 IPCP: CP stalled on event[Authorize CP]
*Apr  1 18:42:29.871: Se0/0/0 IPCP: CP unstall
<Output omitted>
*Apr  1 18:42:29.875: Se0/0/0 CHAP: O SUCCESS id 1 len 4
*Apr  1 18:42:29.879: Se0/0/0 CHAP: I SUCCESS id 1 len 4
*Apr  1 18:42:29.879: Se0/0/0 PPP: Phase is UP
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
*Apr  1 18:42:29.879: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
*Apr  1 18:42:29.879: Se0/0/0 IPCP:    Address 10.0.1.1 (0x03060A000101)
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
*Apr  1 18:42:29.879: Se0/0/0 IPV6CP: Protocol configured, start CP. state[Initial]
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: Event[OPEN] State[Initial to Starting]
```

```
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: Authorizing CP
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: CP stalled on event[Authorize CP]
<Output omitted>
*Apr  1 18:42:29.919: Se0/0/0 IPCP: State is Open
*Apr  1 18:42:29.919: Se0/0/0 IPV6CP: State is Open
*Apr  1 18:42:29.919: Se0/0/0 CDPCP: State is Open
*Apr  1 18:42:29.923: Se0/0/0 CCP: State is Open
*Apr  1 18:42:29.927: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
  10.0.1.2
*Apr  1 18:42:29.927: Se0/0/0 IPCP: Install route to 10.0.1.2
*Apr  1 18:42:39.871: Se0/0/0 LQM: O state Open magic 0x1F887DD3 len 48
*Apr  1 18:42:39.871: Se0/0/0 LQM:    LastOutLQRs 0 LastOutPackets/Octets 0/0
*Apr  1 18:42:39.871: Se0/0/0 LQM:    PeerInLQRs 0 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 18:42:39.871: Se0/0/0 LQM:    PeerOutLQRs 1 PeerOutPackets/Octets
  3907/155488
*Apr  1 18:42:39.879: Se0/0/0 LQM: I state Open magic 0xFF101A5B len 48
*Apr  1 18:42:39.879: Se0/0/0 LQM:    LastOutLQRs 0 LastOutPackets/Octets 0/0
*Apr  1 18:42:39.879: Se0/0/0 LQM:    PeerInLQRs 0 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 18:42:39.879: Se0/0/0 LQM:    PeerOutLQRs 1 PeerOutPackets/Octets
  3909/155225
<Output omitted>
```

In this case, protocol types IPv4 and IPv6 are proposed and acknowledged. The output includes the LCP negotiation, authentication, and NCP negotiation.

The **debug ppp error** privileged EXEC mode command is used to display protocol errors and error statistics associated with PPP connection negotiation and operation, as shown in Example 2-14.

Example 2-14 Output of **debug ppp error** Command

```
R1# debug ppp error
PPP Serial3(i): rlqr receive failure. successes = 15
PPP: myrcvdiffp = 159 peerxmitdiffp = 41091
PPP: myrcvdiffo = 2183 peerxmitdiffo = 1714439
PPP: threshold = 25
PPP Serial2(i): rlqr transmit failure. successes = 15
PPP: myxmitdiffp = 41091 peerrcvdiffp = 159
PPP: myxmitdiffo = 1714439 peerrcvdiffo = 2183
PPP: l->OutLQRs = 1 LastOutLQRs = 1
PPP: threshold = 25
PPP Serial3(i): lqr_protrej() Stop sending LQRs.
PPP Serial3(i): The link appears to be looped back.
```

Troubleshooting a PPP Configuration with Authentication (2.4.1.3)

Authentication is a feature that needs to be implemented correctly; otherwise, the security of your serial connection may be compromised. Always verify your configuration with the **show interfaces serial** command, in the same way as you did without authentication.

Never assume the authentication configuration works without testing it using the previously covered **show** commands. If you discover issues, debugging enables you to verify the issue is with authentication and correct any deficiencies.

For debugging PPP authentication, use the **debug ppp authentication** privileged EXEC mode command as shown in Example 2-15.

Example 2-15 Troubleshooting PPP Authentication Process

```
R2# debug ppp authentication
Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote. Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

The following is an interpretation of the output:

- Line 1 informs us that the router is unable to authenticate on interface Serial0 because the peer did not send a name.
- Line 2 says the router was unable to validate the CHAP response because the username “pioneer” was not found in the local router database.
- Line 3 says no password was found for “pioneer.”
- In the last line, code 4 means that a failure has occurred (other code values include 1 – Challenge, 2 – Response, and 3 – Success). The last line also displays the ID number of the LCP packet (that is, id – 3) and its packet length (that is, len – 48) without the header.

Packet Tracer
□ Activity

Packet Tracer 2.4.1.4: Troubleshooting PPP with Authentication

Background/ Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your boss has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Make sure that all the serial links use PPP CHAP authentication and that all the networks are reachable. The passwords are “cisco” and “class.”

Lab 2.4.1.5: Troubleshooting Basic PPP with Authentication

In this lab, you complete the following objectives:

- Part 1: Build the Network and Load Device Configurations
- Part 2: Troubleshoot the Data Link Layer
- Part 3: Troubleshoot the Network Layer

Summary

Class Activity 2.5.1.1: PPP Validation

Three friends who are enrolled in the Cisco Networking Academy want to check their knowledge of PPP network configuration.

They set up a contest in which each person will be tested on configuring PPP with defined PPP scenario requirements and varying options. Each person devises a different configuration scenario.

The next day they get together and test each other's configuration using their PPP scenario requirements.

Packet Tracer
☐ Activity

Packet Tracer 2.5.1.2: Skills Integration Challenge

Background/Scenario

This activity enables you to practice a variety of skills including configuring VLANs, PPP with CHAP, static and default routing, using IPv4 and IPv6. Due to the sheer number of graded elements, feel free to click Check Results and Assessment Items to see if you correctly entered a graded command. Use the passwords "cisco" and "class" to access EXEC modes of the CLI for routers and switches.

Serial transmissions sequentially send one bit at a time over a single channel. A serial port is bidirectional. Synchronous serial communications require a clocking signal.

Point-to-point links are usually more expensive than shared services; however, the benefits may outweigh the costs. Constant availability is important for some protocols, such as VoIP.

SONET is an optical network standard that uses STDM for efficient use of bandwidth. In the United States, OC transmission rates are standardized specifications for SONET.

The bandwidth hierarchy used by carriers is different in North America (T-carrier) and Europe (E-carrier). In North America, the fundamental line speed is 64 kb/s, or DS0. Multiple DS0s are bundled together to provide higher line speeds.

The demarcation point is the point in the network where the responsibility of the service provider ends and the responsibility of the customer begins. The CPE, usually a router, is the DTE device. The DCE is usually a modem or CSU/DSU.

Cisco HDLC is a bit-oriented synchronous data link layer protocol extension of HDLC; many vendors use it to provide multiprotocol support. This is the default encapsulation method used on Cisco synchronous serial lines.

Synchronous PPP is used to connect to non-Cisco devices, to monitor link quality, provide authentication, or bundle links for shared use. PPP uses HDLC for encapsulating datagrams. LCP is the PPP protocol used to establish, configure, test, and terminate the data link connection. LCP can optionally authenticate a peer using PAP or CHAP. The PPP protocol uses a family of NCPs to simultaneously support multiple network layer protocols. Multilink PPP spreads traffic across bundled links by fragmenting packets and simultaneously sending these fragments over multiple links to same remote address, where they are reassembled.

PPP optionally supports authentication using PAP, CHAP, or both PAP and CHAP protocols. PAP sends authentication data in plaintext. CHAP uses periodic challenge messaging and a one-way hash that helps protect against playback attacks.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Connecting Networks v6 Labs & Study Guide* (ISBN 9781587134296). The Packet Tracer Activity instructions are also in the *Labs & Study Guide*. The PKA files are found in the online course.

Class Activities

Class Activity 2.0.1.2: PPP Persuasion

Class Activity 2.5.1.1: PPP Validation

Labs

Lab 2.3.2.7: Configuring Basic PPP with Authentication

Lab 2.4.1.5: Troubleshooting Basic PPP with Authentication

Packet Tracer
□ **Activity**

Packet Tracer Activities

Packet Tracer 2.1.2.5: Troubleshooting Serial Interfaces

Packet Tracer 2.3.2.6: Configuring PAP and CHAP Authentication

Packet Tracer 2.4.1.4: Troubleshooting PPP with Authentication

Packet Tracer 2.5.1.2: Skills Integration Challenge

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix "Answers to the 'Check Your Understanding' Questions" lists the answers.

1. Which command can be used to view the cable type that is attached to a serial interface?

   A. Router(config)# **show interfaces**

   B. Router(config)# **show controllers**

   C. Router(config)# **show ip interface**

   D. Router(config)# **show ip interface brief**

2. Which serial 0/0/0 interface state will be shown if no serial cable is attached to the router, but everything else has been correctly configured and turned on?

   A. Serial 0/0/0 is administratively down, line protocol is down

   B. Serial 0/0/0 is down, line protocol is down

   C. Serial 0/0/0 is up (disabled)

   D. Serial 0/0/0 is up (looped)

   E. Serial 0/0/0 is up, line protocol is down

   F. Serial 0/0/0 is up, line protocol is up

3. Which is an advantage of using PPP on a serial link instead of HDLC?

   A. Fixed-size frames

   B. Higher speed transmission

   C. Option for authentication

   D. Option for session establishment

4. How does PPP interface with different network layer protocols?

    A. By encoding the information field in the PPP frame

    B. By negotiating with the network layer handler

    C. By specifying the protocol during link establishment through LCP

    D. By using separate NCPs

5. Which three are types of LCP frames used with PPP? (Choose three.)

    A. Link-acknowledgment frames

    C. Link-control frames

    D. Link-establishment frames

    E. Link-maintenance frames

    F. Link-negotiation frames

    G. Link-termination frames

6. Which protocol will terminate the PPP link after the exchange of data is complete?

    A. CDPCP

    B. IPCP

    C. IPV6CP

    D. LCP

    E. NCP

7. Which three statements are true about PPP? (Choose three.)

    A. PPP can be used only between two Cisco devices.

    B. PPP can use synchronous and asynchronous circuits.

    C. PPP carries packets from several network layer protocols in LCPs.

    D. PPP is a default encapsulation of serial interfaces on Cisco routers.

    E. PPP uses LCPs to agree on format options such as authentication, compression, and error detection.

    F PPP uses LCPs to establish, configure, and test the data link connection.

8. What PPP information will be displayed if a network engineer issues the **show ppp multilink** command on a Cisco router?

    A. The IP addresses of the link interfaces

    B. The link LCP and NCP status

    C. The queuing type on the link

    D. The serial interfaces participating in the multilink

9. A network engineer is monitoring an essential but poor-quality PPP WAN link that periodically shuts down. An examination of the interface configurations shows that the **ppp quality 90** command has been issued. What action could the engineer take to reduce the frequency with which the link shuts down?

   A. Issue the command **ppp quality 70**.

   B. Issue the command **ppp quality 100**.

   C. Set the DCE interface to a lower clock rate.

   D. Use the **bandwidth** command to increase the bandwidth of the link.

10. In which situation would the use of PAP be preferable to the use of CHAP?

   A. When a network administrator prefers it because of ease of configuration

   B. When multilink PPP is used

   C. When plaintext passwords are needed to simulate login at the remote host

   D. When router resources are limited

CHAPTER 3

Branch Connections

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are the remote-access broadband connection options for small- to medium-sized businesses?
- What is the appropriate broadband connection for a given network requirement?
- What is PPPOE and how does it operate?
- What is the basic configuration for a PPPoE connection on a client router?
- What are the benefits of VPN technology?
- What are the features of site-to-site and remote-access VPNs?
- What is the purpose and what are the benefits of GRE tunnels?
- How do you troubleshoot a site-to-site GRE tunnel?
- What are the basic BGP features?
- What are the basic BGP design considerations?
- How do you configure an eBGP branch connection?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

PPP over Ethernet (PPPoE) *Page 103*

Internet Protocol Security (IPsec) *Page 103*

Border Gateway Protocol (BGP) *Page 103*

radio frequency (RF) *Page 104*

hybrid fiber-coaxial (HFC) *Page 104*

Data over Cable Service Interface Specification (DOCSIS) *Page 104*

antenna site *Page 105*

transportation network *Page 105*

distribution network *Page 105*

central office (CO) *Page 105*

amplifier *Page 105*

subscriber drop *Page 105*

node *Page 106*

downstream *Page 106*

upstream *Page 106*

asymmetric DSL (ADSL) *Page 107*

symmetric DSL (SDSL) *Page 107*

DSL transceiver *Page 108*

DSL micro filter *Page 108*

Cellular/mobile *Page 109*

dialer interface Page 116

maximum transmission unit (MTU) Page 116

maximum segment size (MSS) Page 118

VPN gateway Page 124

telecommuters Page 126

VPN client software Page 126

Cisco AnyConnect Secure Mobility Client Page 126

Dynamic Multipoint VPN (DMVPN) Page 127

Next Hop Resolution Protocol (NHRP) Page 127

Next Hop Server (NHS) Page 127

Next Hop Clients (NHCs) Page 127

spoke-to-spoke Page 127

Multipoint Generic Routing Encapsulation (mGRE) Page 128

Passenger protocol Page 129

Carrier protocol Page 129

Transport protocol Page 129

Secure Sockets Layer (SSL) Page 134

AS number (ASN) Page 137

path vector routing protocol Page 138

external BGP (eBGP) Page 139

internal BGP (iBGP) Page 139

multihomed Page 139

single-homed Page 140

BGP peers Page 140

Network Address Translation (NAT) Page 143

Introduction (3.0)

Broadband solutions provide teleworkers with high-speed connection options to business locations and to the Internet. Small branch offices can also connect using these same technologies. This chapter covers commonly used broadband solutions, such as cable, DSL, and wireless.

Note

Teleworking is a broad term referring to conducting work by connecting to a workplace from a remote location, with the assistance of telecommunications.

ISPs value the Point-to-Point Protocol (PPP) because of the authentication, accounting, and link management features. Customers appreciate the ease and availability of the Ethernet connection. Ethernet links do not natively support PPP. A solution to this problem was created: *PPP over Ethernet (PPPoE)*. This chapter covers the implementation of PPPoE.

Security is a concern when using the public Internet to conduct business. Virtual private networks (VPNs) are used to improve the security of data across the Internet. A VPN is used to create a private communication channel (also called a tunnel) over a public network. Data can be secured by using encryption in this tunnel through the Internet and by using authentication to protect data from unauthorized access. VPN technology provides security options for data running over these connections. This chapter describes some basic VPN implementations.

Note

VPNs rely on *Internet Protocol Security (IPsec)* to provide security across the Internet. IPsec is beyond the scope of this course.

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels. GRE creates a virtual point-to-point link to Cisco routers at remote points, over an IP internetwork. The chapter covers the basic GRE implementation.

The *Border Gateway Protocol (BGP)* is routing protocol used between autonomous systems. This chapter concludes with a discussion of BGP routing and an implementation of BGP in a single-homed network.

Class Activity 3.0.1.2: Broadband Varieties

Telework employment opportunities are expanding in your local area every day. You have been offered employment as a teleworker for a major corporation. The new employer requires teleworkers to have access to the Internet to fulfill their job responsibilities.

Research the following broadband Internet connection types that are available in your geographic area:

- DSL
- Cable
- Satellite

Consider the advantages and disadvantages of each broadband variation as you notate your research, which may include cost, speed, security, and ease of implementation or installation.

Remote-Access Connections (3.1)

In this section, you learn how to select broadband remote-access technologies to support business requirements.

Broadband Connections (3.1.1)

In this topic, you compare remote-access broadband connection options for small- to medium-sized businesses.

What Is a Cable System? (3.1.1.1)

Accessing the Internet through a cable network is a popular option that teleworkers use to access their enterprise network. The cable system uses a coaxial cable that carries ***radio frequency (RF)*** signals across the network. Coaxial cable is the primary medium used to build cable TV systems.

Visit this website to learn more about the history of cable:

https://www.calcable.org/learn/history-of-cable/

Modern cable systems offer customers advanced telecommunications services, including high-speed Internet access, digital cable television, and residential telephone service. Cable operators typically deploy ***hybrid fiber-coaxial (HFC)*** networks to enable high-speed transmission of data to cable modems located in a small office/home office (SOHO).

The ***Data over Cable Service Interface Specification (DOCSIS)*** is the international standard for adding high-bandwidth data to an existing cable system.

Figure 3-1 shows an example of a cable system.

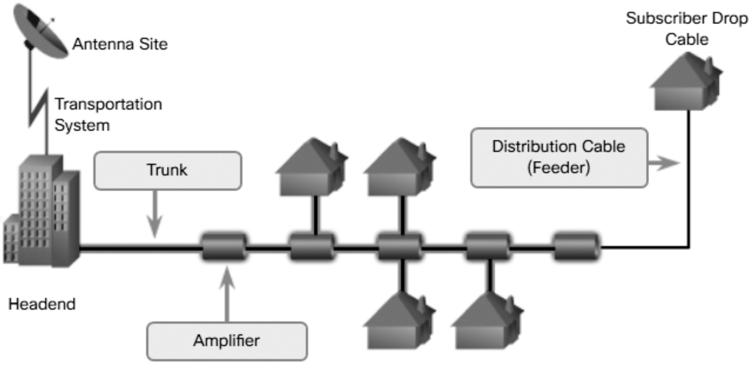


Figure 3-1 Cable System

The following describes the components shown in Figure 3-1:

- *Antenna site*: The location of an antenna site is chosen for optimum reception of over-the-air, satellite, and sometimes point-to-point signals. The main receiving antennas and satellite dishes are located at the antenna site.
- *Transportation network*: A transportation network links a remote antenna site to a headend or a remote headend to the *distribution network*. The transportation network can be microwave, coaxial, or fiber optic.
- **Headend:** This is where signals are first received, processed, formatted, and then distributed downstream to the cable network. The headend facility is usually unmanned, under security fencing, and is similar to a telephone company *central office (CO)*.
- *Amplifier*: This is a device that regenerates an incoming signal to extend further through the network. Cable networks use various types of amplifiers in their transportation and distribution networks.
- *Subscriber drop*: A subscriber drop connects the subscriber to the cable services. The subscriber drop is a connection between the feeder part of a distribution network and the subscriber terminal device (e.g., cable modem). The type of cable commonly used in a subscriber drop consists of radio grade (RG) series 6 (RG6) or series 59 (RG59) coaxial cable.

Cable Components (3.1.1.2)

Figure 3-2 shows an end-to-end cable topology.

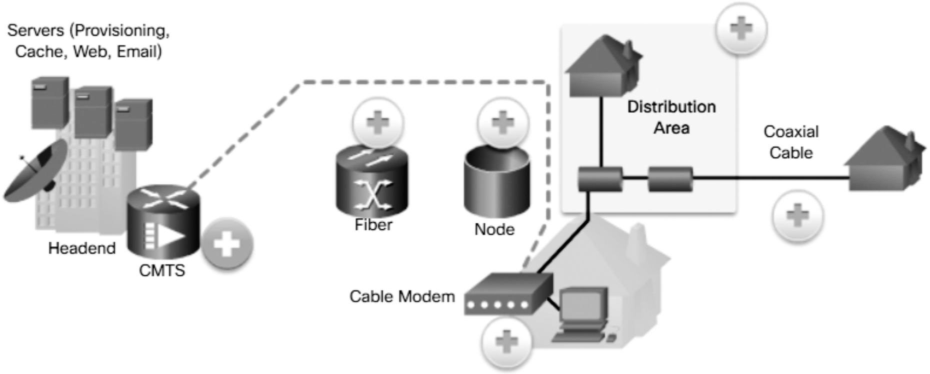


Figure 3-2 End-to-End Data Propagation over Cable

The following describes the components shown in Figure 3-2:

- **Cable modem termination system (CMTS):** A CMTS is a component that exchanges digital signals with cable modem on a cable network. A headend CMTS communicates with CMs that are located in subscriber homes.
- **Fiber:** The trunk portion of the cable network is usually fiber-optic cable.
- ***Node***: Nodes convert optical signals to RF signals.
- **Distribution area:** A distribution network segment (feeder segment) is from 500 to as many as 2000 subscribers.
- **Coaxial cable:** Coaxial feeder cables originate from the node and carry RF signals to the subscribers.
- **Cable modem:** A cable modem enables you to receive data at high speeds. Typically, the cable modem attaches to a standard Ethernet card in the computer.

A headend CMTS communicates with CMs located in subscriber homes. The headend is actually a router with databases for providing Internet services to cable subscribers. The architecture is relatively simple, using an HFC network. The HFC network is a mixed optical-coaxial network in which optical fiber replaces the lower bandwidth coaxial cable. The fiber carries the same broadband content for Internet connections, telephone service, and streaming video as the coaxial cable carries.

In a modern HFC network, typically 500 to 2000 active data subscribers are connected to a cable network segment, all sharing the upstream and downstream bandwidth. DOCSIS standards are used to specify how data is exchanged between cable modem and the headend. For instance, the DOCSIS 3.1 standard supports *downstream* bandwidths (that is, from the headend to the subscriber) up to 10 Gb/s and *upstream* bandwidths (that is, from the subscriber to the headend) of 1 Gb/s.

What Is DSL? (3.1.1.3)

A digital subscriber line (DSL) is a means of providing high-speed connections over installed copper wires. DSL is one of the key teleworker solutions available.

Figure 3-3 shows a representation of bandwidth space allocation on a copper wire for *asymmetric DSL (ADSL)*. The area labeled POTS (Plain Old Telephone System) identifies the frequency range used by the voice-grade telephone service. The area labeled ADSL represents the frequency space used by the upstream and downstream DSL signals. The area that encompasses both the POTS area and the ADSL area represents the entire frequency range supported by the copper wire pair.

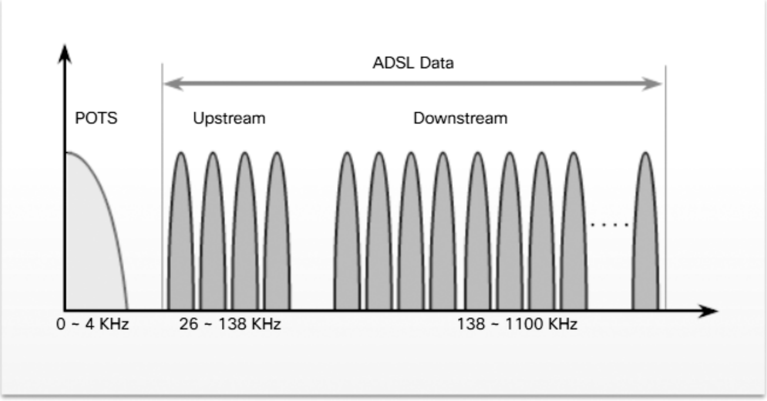


Figure 3-3 Asymmetric DSL in the Electromagnetic Spectrum

Another form of DSL technology is *symmetric DSL (SDSL)*. All forms of DSL service are categorized as ADSL or SDSL, and there are several varieties of each type. ADSL provides higher downstream bandwidth to the user than upload bandwidth. SDSL provides the same capacity in both directions.

The different varieties of DSL provide different bandwidths, some with capabilities exceeding 40 Mb/s. The transfer rates are dependent on the actual length of the local loop, and the type and condition of the cabling. For satisfactory ADSL service, the loop must be less than 3.39 miles (5.46 km).

DSL Connections (3.1.1.4)

Service providers deploy DSL connections in the local loop. The connection is set up between a pair of modems on either end of a copper wire that extends between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM). A DSLAM is the device located at the CO of the provider; it concentrates connections from multiple DSL subscribers. A DSLAM is often built into an aggregation router.

Figure 3-4 shows the equipment needed to provide a DSL connection to a SOHO.

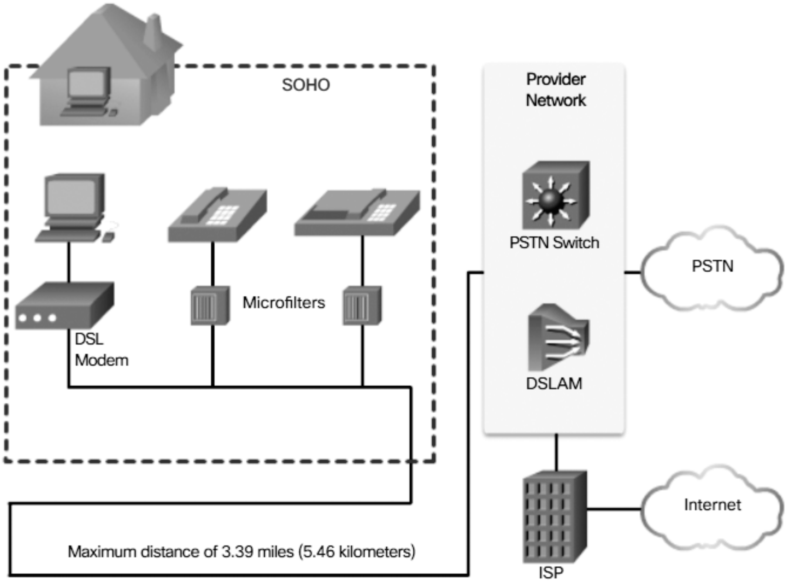


Figure 3-4 DSL Connections

The two important components in this topology are the DSL transceiver and the DSLAM:

- *DSL transceiver*: Connects the computer of the teleworker to the DSL. Usually, the transceiver is a DSL modem connected to the computer using a USB or Ethernet cable. Typically, DSL transceivers are built into small routers with multiple switch ports suitable for home office use.
- **DSLAM:** Located at the CO of the carrier, the DSLAM combines individual DSL connections from users into one high-capacity link to an ISP, and therefore, to the Internet.

A *DSL micro filter* (also known as a DSL filter) is required to connect devices such as phones or fax machines on the DSL network.

Figure 3-5 depicts modern DSL routers and broadband aggregation routers.

The advantage that DSL has over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM. Adding users does not impede performance, unless the DSLAM Internet connection to the ISP, or the Internet, becomes saturated.

Figure 3-5 Example of DSL Routers

Wireless Connection (3.1.1.5)

Developments in broadband wireless technology are increasing wireless availability through three main technologies:

- Municipal Wi-Fi
- *Cellular/mobile*
- Satellite Internet

The sections that follow describe these technologies in more detail.

Municipal Wi-Fi

Many municipal governments, often working with service providers, are deploying wireless networks. Some of these networks provide high-speed Internet access at no cost or for substantially less than the price of other broadband services. Other cities reserve their Wi-Fi networks for official use, providing police, firefighters, and city workers remote access to the Internet and municipal networks.

Most municipal wireless networks use a mesh of interconnected access points, as shown in Figure 3-6. Each access point is in range and can communicate with at least two other access points. The mesh blankets a particular area with radio signals.

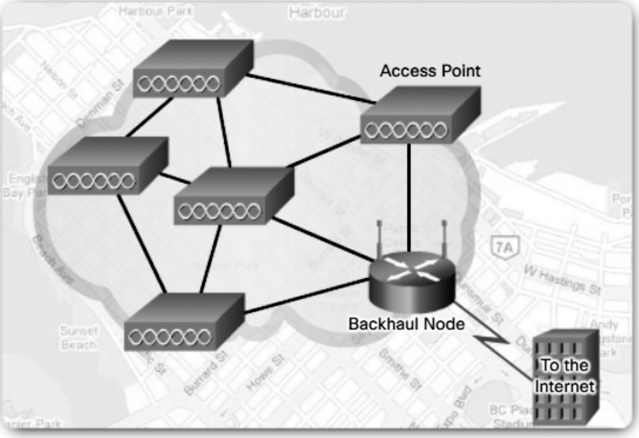


Figure 3-6 Municipal Wireless Network

Cellular/Mobile

Mobile phones use radio waves to communicate through nearby cell towers. The mobile phone has a small radio antenna. The provider has a much larger antenna that sits at the top of a tower, as shown in Figure 3-7.

Figure 3-7 Cellular Tower

Three common terms are used when discussing cellular/mobile networks:

- **Wireless Internet:** A general term for Internet services from a mobile phone or from any device that uses the same technology.

- **2G/3G/4G wireless:** Major changes to the mobile phone companies' wireless networks through the evolution of the second, third, and fourth generations of wireless mobile technologies.
- **Long-Term Evolution (LTE):** A newer and faster technology considered to be part of 4G technology.

Cellular/mobile broadband access consists of various standards such as 4G using LTE. A mobile phone subscription does not necessarily include a mobile broadband subscription. Cellular speeds continue to increase. For example, 4G LTE Category 10 supports up to 450 Mb/s download and 100 Mb/s upload.

Note

Under development is a proposed 5G standard rumored to support higher bandwidth than 4G LTE.

Satellite Internet

Satellite Internet services are used in locations where land-based Internet access is not available or for temporary installations that are mobile. Internet access using satellites is available worldwide, including for providing Internet access to vessels at sea, airplanes in flight, and vehicles moving on land.

Figure 3-8 illustrates a two-way satellite system that provides Internet access to a home subscriber. Upload speeds are about one-tenth of the download speed. Download speeds range from 5 Mb/s to 25 Mb/s.

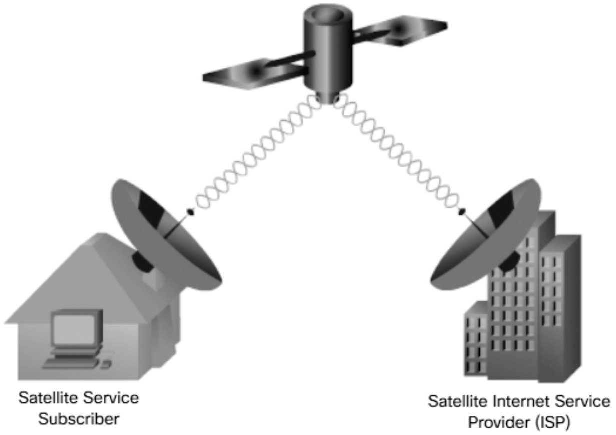


Figure 3-8 Two-Way Satellite Implementation

The primary installation requirement is for the antenna to have a clear view toward the equator, where most orbiting satellites are stationed. Trees and heavy rains can affect reception of the signals.

Note

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology for both fixed and mobile implementations. WiMAX may still be relevant for some areas of the world. However, in most of the world, WiMAX has largely been replaced by LTE for mobile access and cable or DSL for fixed access.

Interactive Graphic

Activity 3.1.1.6: Identify Broadband Connection Terminology

Refer to the online course to complete this activity.

Select a Broadband Connection (3.1.2)

In this topic, you select an appropriate broadband connection for a given network requirement.

Comparing Broadband Solutions (3.1.2.1)

Each broadband solution has advantages and disadvantages. The ideal is to have a fiber-optic cable directly connected to the SOHO network. Some locations have only one option, such as cable or DSL. Some locations have only broadband wireless options for Internet connectivity.

If multiple broadband solutions are available, a cost-versus-benefit analysis should be performed to determine the best solution.

Some factors to consider in making a decision include

- **Cable:** Bandwidth is shared by many users; upstream data rates are often slow during high-usage hours in areas with oversubscription.
- **DSL:** Limited bandwidth is distance sensitive (in relation to the ISP’s central office); the upstream rate is proportionally quite small compared to the downstream rate.
- **Cellular/mobile:** Coverage is often an issue, even within a SOHO where bandwidth is relatively limited.
- **Wi-Fi mesh:** Most municipalities do not have a mesh network deployed; if it is available and the SOHO is in range, it is a viable option.
- **Satellite Internet:** This option is expensive, has limited capacity per subscriber, but often provides access where no other access is possible.

Lab 3.1.2.2: Researching Broadband Internet Access Technologies

In this lab, you complete the following objectives:

- Part 1: Investigate Broadband Distribution
- Part 2: Research Broadband Access Options for Specific Scenarios

PPPoE (3.2)

In this section, you configure a Cisco router with PPPoE.

PPPoE Overview (3.2.1)

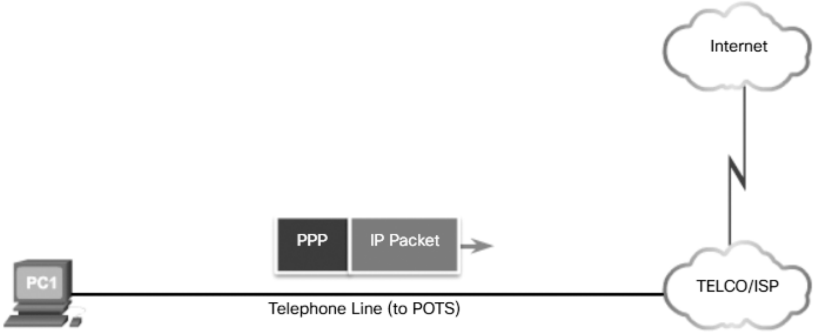
In this topic, you learn how PPPoE operates.

PPPoE Motivation (3.2.1.1)

In addition to understanding the various technologies available for broadband Internet access, it is also important to understand the underlying data link layer protocol that the ISP uses to form a connection.

A data link layer protocol commonly used by ISPs is Point-to-Point Protocol (PPP). PPP can be used on all serial links, including those links created with dialup analog and ISDN modems. To this day, the link from a dialup user to an ISP, using analog modems, likely uses PPP.

Figure 3-9 shows a basic representation of that analog dial connection with PPP.



In a legacy dialup scenario, PC1 reaches the Internet through the TELCO/ISP cloud by using a FAX/MODEM device.

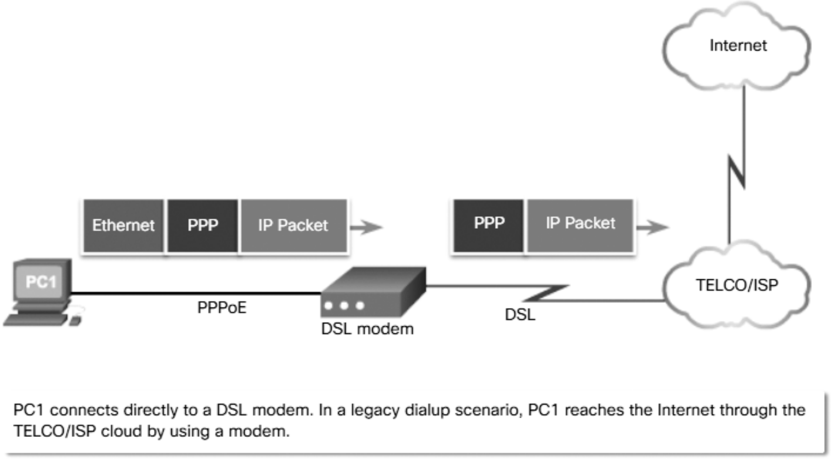
Figure 3-9 PPP Frames over Legacy Dialup Connection

Additionally, ISPs often use PPP as the data link protocol over broadband connections. There are several reasons for this. First, PPP supports the ability to assign IP addresses to remote ends of a PPP link. With PPP enabled, ISPs can use PPP to assign each customer one public IPv4 address. More importantly, PPP supports CHAP authentication. ISPs often want to use CHAP to authenticate customers because during authentication, ISPs can check accounting records to determine whether the customer's bill is paid prior to letting the customer connect to the Internet.

These technologies came to market in the following order, with varying support for PPP:

1. Analog modems for dialup that could use PPP and CHAP
2. ISDN for dialup that could use PPP and CHAP
3. DSL, which did not create a point-to-point link and could not support PPP and CHAP

ISPs value PPP because of the authentication, accounting, and link-management features. Customers appreciate the ease and availability of the Ethernet connection; however, Ethernet links do not natively support PPP. PPP over Ethernet (PPPoE) provides a solution to this problem. As shown in Figure 3-10, PPPoE sends PPP frames encapsulated inside Ethernet frames.



PC1 connects directly to a DSL modem. In a legacy dialup scenario, PC1 reaches the Internet through the TELCO/ISP cloud by using a modem.

Figure 3-10 PPP Frames over an Ethernet Connection (PPPoE)

PPPoE Concepts (3.2.1.2)

As shown in Figure 3-11, the customer's router is usually connected to a DSL modem using an Ethernet cable. PPPoE creates a PPP tunnel over an Ethernet connection.

This allows PPP frames to be sent across the Ethernet cable to the ISP from the customer's router. The modem converts the Ethernet frames to PPP frames by stripping the Ethernet headers. The modem then transmits these PPP frames on the ISP's DSL network.

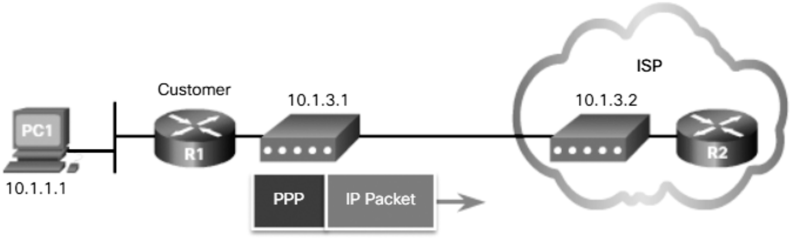


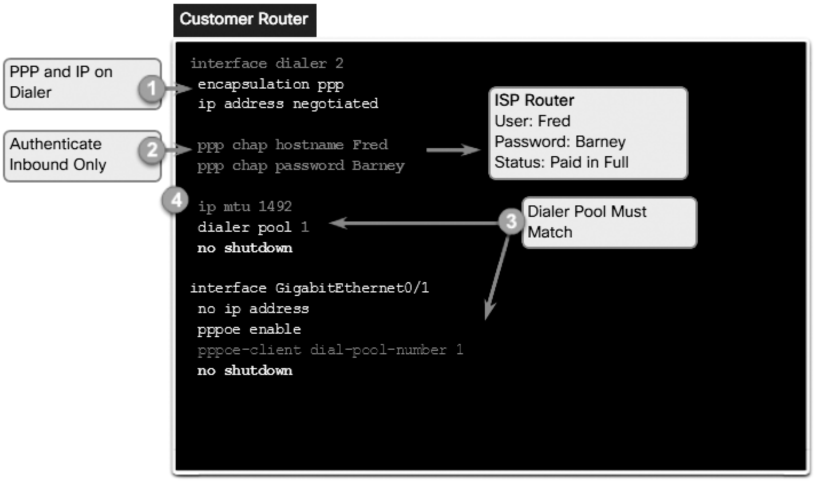
Figure 3-11 Tunneling to Create a PPP Link over Ethernet

Implement PPPoE (3.2.2)

In this topic, you implement a basic PPPoE connection on a client router.

PPPoE Configuration (3.2.2.1)

With the ability to send and receive PPP frames between the routers, the ISP could continue to use the same authentication model as with analog and ISDN. To make it all work, the client and ISP routers need additional configuration, including PPP configuration, as shown in Figure 3-12.



```
interface dialer 2
 encapsulation ppp
 ip address negotiated

 ppp chap hostname Fred
 ppp chap password Barney

 ip mtu 1492
 dialer pool 1
 no shutdown

interface GigabitEthernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
 no shutdown
```

Figure 3-12 Steps for a PPPoE Customer Configuration

To understand the configuration, consider the following:

1. To create a PPP tunnel, the configuration uses a *dialer interface*. A dialer interface is a virtual interface. The PPP configuration is placed on the dialer interface, not the physical interface. The dialer interface is created using the **interface dialer** *number* global configuration command. The client can configure a static IP address but will more likely be automatically assigned a public IP address by the ISP.
2. The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer. The hostname and password configured on the customer router must match the hostname and password configured on the ISP router. Notice in Figure 3-12 that the CHAP username and password match the settings on the ISP router.
3. The physical Ethernet interface that connects to the DSL modem is then enabled with the **pppoe enable** interface configuration command. This command enables PPPoE and links the physical interface to the dialer interface. The dialer interface is linked to the Ethernet interface with the **dialer pool** *number* and **pppoe-client dial-pool-number** *number* interface configuration commands, using the same *number*. The dialer interface number does not have to match the dialer pool number.
4. The *maximum transmission unit (MTU)* should be lowered to 1492, versus the default of 1500, to accommodate the PPPoE headers.

PPPoE Verification (3.2.2.2)

As shown in Figure 3-13, the customer's router is connected to the ISP router using DSL. Both routers have been configured for PPPoE.

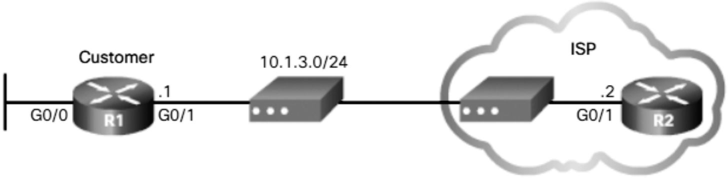


Figure 3-13 Verifying the PPPoE Configuration

In Example 3-1, the **show ip interface brief** command is issued on R1 to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.

Example 3-1 Verifying the Dialer Interface Is Up

```
R1# show ip interface brief
Interface                   IP-Address   OK? Method Status                 Protocol
Embedded-Service-Engine0/0  unassigned   YES unset  administratively down  down
GigabitEthernet0/0          unassigned   YES unset  administratively down  down
GigabitEthernet0/1          unassigned   YES unset  up                     up
Serial0/0/0                 unassigned   YES unset  administratively down  down
Serial0/0/1                 unassigned   YES unset  administratively down  down
Dialer2                     10.1.3.1     YES IPCP   up                     up
Virtual-Access1             unassigned   YES unset  up                     up
Virtual-Access2             unassigned   YES unset  up                     up
R1#
```

As shown in Example 3-2, the **show interface dialer** command on R1 verifies the MTU and PPP encapsulation configured on the dialer interface.

Example 3-2 Verifying the MTU Size and Encapsulation

```
R1# show interface dialer 2
Dialer2 is up, line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.3.1/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
<output omitted>
```

Example 3-3 displays the routing table on R1.

Example 3-3 Verifying the R1 Routing Table

```
R1# show ip route | begin Gateway

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*     0.0.0.0/0 is directly connected, Dialer2
       10.0.0.0/32 is subnetted, 2 subnets
C         10.1.3.1 is directly connected, Dialer2
C         10.1.3.2 is directly connected, Dialer2
R1#
```

Notice that two /32 host routes for 10.0.0.0 have been installed in R1's routing table. The first host route is for the address assigned to the dialer interface. The second host route is the IPv4 address of the ISP. The installation of these two host routes is the default behavior for PPPoE.

As shown in Example 3-4, the **show pppoe session** command enables you to display information about currently active PPPoE sessions.

Example 3-4 Viewing the Current PPPoE Sessions

```
R1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC           Port                  VT   VA          State
           SID  LocMAC                                      VA-st       Type
     N/A     1  30f7.0da3.1641  Gi0/1                  Di2  Vi2         UP
                30f7.0da3.0da1                               UP
R1#
```

The output displays the local and remote Ethernet MAC addresses of both routers. The Ethernet MAC addresses can be verified by using the **show interfaces** command on each router.

PPPoE Troubleshooting (3.2.2.3)

After you ensure that the client router and DSL modem are connected with the proper cables, the cause of a PPPoE connection not functioning properly is usually one or more of the following reasons:

- Failure in the PPP negotiation process
- Failure in the PPP authentication process
- Failure to adjust the TCP ***maximum segment size (MSS)***

PPPoE Negotiation (3.2.2.4)

Verify PPP negotiation using the **debug ppp negotiation** command. Example 3-5 displays part of the debug output after R1's G0/1 interface has been enabled.

Example 3-5 Examining the PPP Negotiation Process

```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
<output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
```

```
*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4
<output omitted>
*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)
*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
*Sep 20 19:05:05.271: Vi2 IPCP: State is Open
*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2
*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address
  10.1.3.2
*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2
R1# undebug all
```

The output is an example of what should be generated when PPP is correctly configured.

The four main points of failure in a PPP negotiation are as follows:

- No response from the remote device (the ISP)
- Link Control Protocol (LCP) not open
- Authentication failure
- IP Control Protocol (IPCP) failure

PPPoE Authentication (3.2.2.5)

After confirming with the ISP that it uses CHAP, verify that the CHAP username and password are correct. Example 3-6 shows the CHAP configuration on the dialer2 interface.

Example 3-6 Verify the CHAP Configuration

```
R1# show running-config | section interface Dialer2
interface Dialer2
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Fred
 ppp chap password 0 Barney
R1#
```

Re-examining the output of the **debug ppp negotiation** command in Example 3-7 verifies that the CHAP username is correct.

Example 3-7 Verify the CHAP Username

```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
<output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4
<output omitted>
*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)
*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
*Sep 20 19:05:05.271: Vi2 IPCP: State is Open
*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2
*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address
  10.1.3.2
*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2
R1# undebug all
```

If the CHAP username or password were incorrect, the output from the **debug ppp negotiation** command would show an authentication failure message such as shown in Example 3-8.

Example 3-8 Authentication Failure Message

```
R1#
*Sep 20 19:05:05.247: Vi2 CHAP: I FAILURE id 1 Len 26 MSG is "Authentication
  failure"
R1#
```

PPPoE MTU Size (3.2.2.6)

Accessing some web pages might be a problem with PPPoE. When the client requests a web page, a TCP three-way handshake occurs between the client and the web server. During the negotiation, the client specifies the value of its TCP maximum segment size (MSS). The TCP MSS is the maximum size of the data portion in the TCP segment.

A host determines the value of its MSS field by subtracting the IP and TCP headers from the Ethernet maximum transmission unit (MTU). On an Ethernet interface, the default MTU is 1500 bytes. Subtracting the IPv4 header of 20 bytes and the TCP header of 20 bytes, the default MSS size will be 1460 bytes, as shown in Figure 3-14.

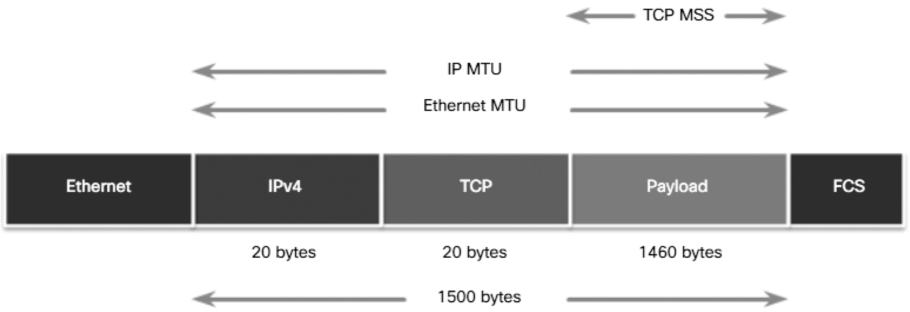


Figure 3-14 MTU and MSS

The default MSS size is 1460 bytes, when the default MTU is 1500 bytes; however, PPPoE supports an MTU of only 1492 bytes to accommodate the additional 8-byte PPPoE header, as shown in Figure 3-15.

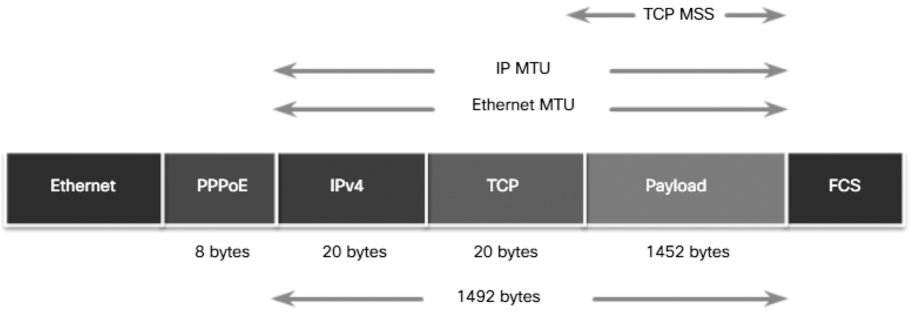


Figure 3-15 Adjusted MSS with PPPoE Header

You can verify the PPPoE MTU size in running configuration, as shown in Example 3-9. This disparity between the host and PPPoE MTU size can cause the router to drop 1500-byte packets and terminate TCP sessions over the PPPoE network.

Example 3-9 Verifying the MTU Size on the Dialer Interface

```
R1# show running-config | section interface Dialer2
interface Dialer2
 mtu 1492
 ip address negotiated
 encapsulation ppp
<output omitted>
```

The **ip tcp adjust-mss** *max-segment-size* interface configuration command helps prevent TCP sessions from being dropped by adjusting the MSS value during the TCP three-way handshake. In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. Example 3-10 shows this configuration on R1's LAN interface.

Example 3-10 Adjusting the TCP MSS

```
R1(config)# interface g0/0
R1(config-if)# ip tcp adjust-mss 1452
```

The TCP MSS value of 1452 plus the 20-byte IPv4 header, the 20-byte TCP header, and the 8-byte PPPoE header adds up to a 1500-byte MTU, as illustrated previously in Figure 3-15.

Lab 3.2.2.7: Configuring a Router as a PPPoE Client for DSL Connectivity

In this lab, you complete the following objectives:

- Part 1: Build the Network
- Part 2: Configure the ISP Router
- Part 3: Configure the Cust1 Router

Lab 3.2.2.8: Troubleshoot PPPoE

In this lab, you compete the following objectives:

- Part 1: Build the Network
- Part 2: Troubleshoot PPPoE on Cust1

VPNs (3.3)

In this section, you learn how VPNs secure site-to-site and remote-access connectivity.

Fundamentals of VPNs (3.3.1)

In this topic, you learn about the benefits of VPN technology.

Introducing VPNs (3.3.1.1)

Organizations need secure, reliable, and cost-effective ways to interconnect multiple networks, such as allowing branch offices and suppliers to connect to a corporation's headquarter network. Additionally, with the growing number of teleworkers, enterprises have an increasing need for secure, reliable, and cost-effective ways to connect employees working in small office/home office (SOHO) and other remote locations, with resources on corporate sites.

As shown in Figure 3-16, organizations use VPNs to create an end-to-end private network connection over third-party networks, such as the Internet. The tunnel eliminates the distance barrier and enables remote users to access central site network resources.

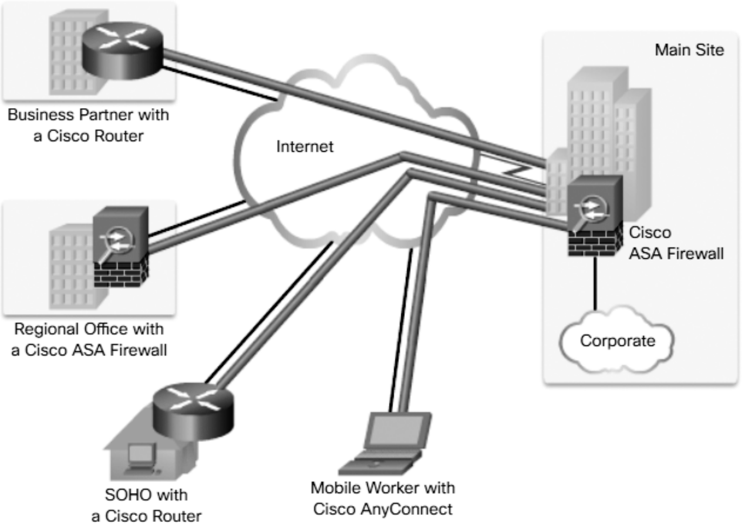


Figure 3-16 VPNs

A VPN is a private network created via tunneling over a public network, usually the Internet. A VPN is a communications environment in which access is strictly controlled to permit peer connections within a defined community of interest.

The first VPNs were strictly IP tunnels that did not include authentication or encryption of the data. For example, Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels. This creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. However, GRE does not support encryption.

Today, a secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.

To implement VPNs, a ***VPN gateway*** is necessary. The VPN gateway could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA). An ASA is a standalone firewall device that combines firewall, VPN concentrator, and intrusion prevention functionality into one software image.

Benefits of VPNs (3.3.1.2)

As shown in Figure 3-17, a VPN uses virtual connections that are routed through the Internet from the private network of an organization to the remote site or employee host. The information from a private network is securely transported over the public network to form a virtual network.

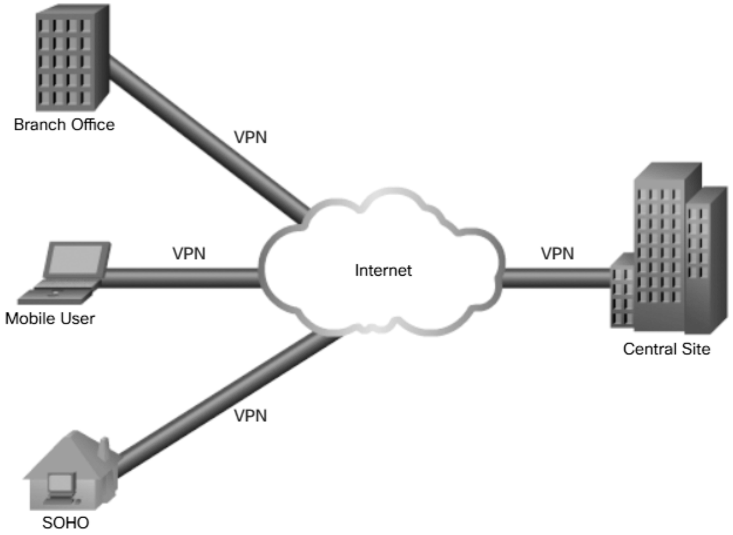


Figure 3-17 VPN Internet Connections

The benefits of a VPN include the following:

- **Cost savings:** VPNs enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main site, thus eliminating expensive, dedicated WAN links and modem banks. Furthermore, with the advent of cost-effective, high-bandwidth technologies, such as DSL, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
- **Scalability:** VPNs enable organizations to use the Internet infrastructure within ISPs and devices, which makes it easy to add new users. Therefore,

organizations are able to add large amounts of capacity without adding significant infrastructure.

- **Compatibility with broadband technology:** VPNs allow mobile workers and teleworkers to take advantage of high-speed, broadband connectivity, such as DSL and cable, to access to their organizations' networks. Broadband connectivity provides flexibility and efficiency. High-speed, broadband connections also provide a cost-effective solution for connecting remote offices.
- **Security:** VPNs can include security mechanisms that provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

Interactive Graphic

Activity 3.3.1.3: Identify the Benefits of VPNs

Refer to the online course to complete this activity.

Types of VPNs (3.3.2)

In this topic, you learn about site-to-site and remote-access VPNs.

Site-to-Site VPNs (3.3.2.1)

A site-to-site VPN is created when devices on both sides of the VPN connection are aware of the VPN configuration in advance, as shown in Figure 3-18.

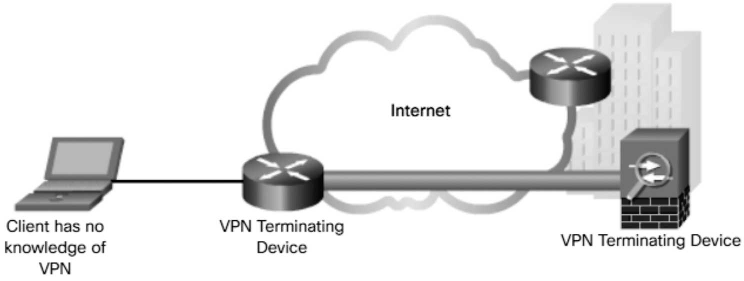


Figure 3-18 Site-to-Site VPNs

The VPN remains static, and internal hosts have no knowledge that a VPN exists. In a site-to-site VPN, end hosts send and receive normal TCP/IP traffic through a VPN "gateway." The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site. The VPN gateway then sends it through a VPN tunnel over the Internet to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

A site-to-site VPN is an extension of a classic WAN network. Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network. In the past, a leased-line or Frame Relay connection was required to connect sites, but because most corporations now have Internet access, these connections are commonly replaced with site-to-site VPNs.

Remote-Access VPNs (3.3.2.2)

Where a site-to-site VPN is used to connect entire networks, a remote-access VPN supports the needs of ***telecommuters***, mobile users, and extranet, consumer-to-business traffic. A remote-access VPN is created when VPN information is not statically set up, but instead allows for dynamically changing information, and can be enabled and disabled. Remote-access VPNs support a client/server architecture, where the VPN client (remote host) gains secure access to the enterprise network via a VPN server device at the network edge, as shown Figure 3-19.

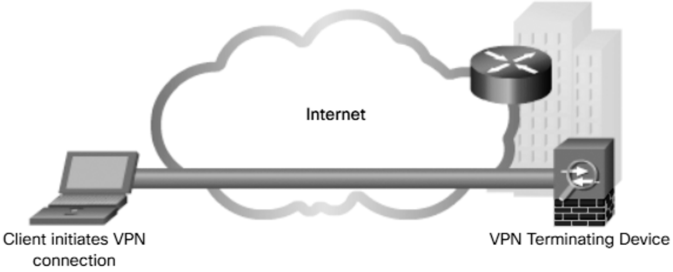


Figure 3-19 Remote-Access VPNs

Remote-access VPNs are used to connect individual hosts that must access their company network securely over the Internet. Internet connectivity used by telecommuters is typically a broadband connection.

VPN client software, such as the ***Cisco AnyConnect Secure Mobility Client*** software, is installed on the teleworker host. When the host sends traffic, the Cisco AnyConnect VPN Client software encapsulates, encrypts, and sends the traffic over the Internet to the destination VPN gateway. Upon receipt, the VPN gateway behaves as it does for site-to-site VPNs.

Note

The Cisco AnyConnect Secure Mobility Client software builds on prior Cisco AnyConnect VPN Client and Cisco VPN Client offerings to improve the always-on VPN experience across more laptop and smartphone-based mobile devices. This client supports IPv6.

DMVPN (3.3.2.3)

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner. The goal is to simplify the configuration while easily and flexibly connecting central office sites with branch sites in a hub-and-spoke (or hub-to-spoke) topology, as shown in Figure 3-20.

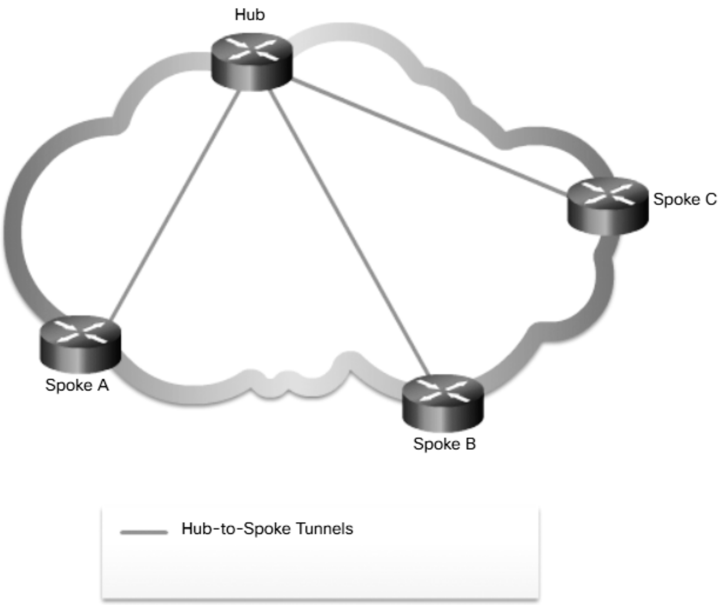


Figure 3-20 DMVPN Hub-to-Spoke Tunnels

With DMVPNs, branch sites can also communicate directly with other branch sites, as shown in Figure 3-21.

DMVPN is built using the following technologies:

- *Next Hop Resolution Protocol (NHRP)*
- Multipoint Generic Routing Encapsulation (mGRE) tunnels
- IP Security (IPsec) encryption

NHRP is a Layer 2 resolution and caching protocol similar to Address Resolution Protocol (ARP). NHRP creates a distributed mapping database of public IP addresses for all tunnel spokes. NHRP is a client/server protocol consisting of the NHRP hub known as the *Next Hop Server (NHS)* and the NHRP spokes known as the *Next Hop Clients (NHCs)*. NHRP supports hub-and-spoke as well as *spoke-to-spoke* configurations.

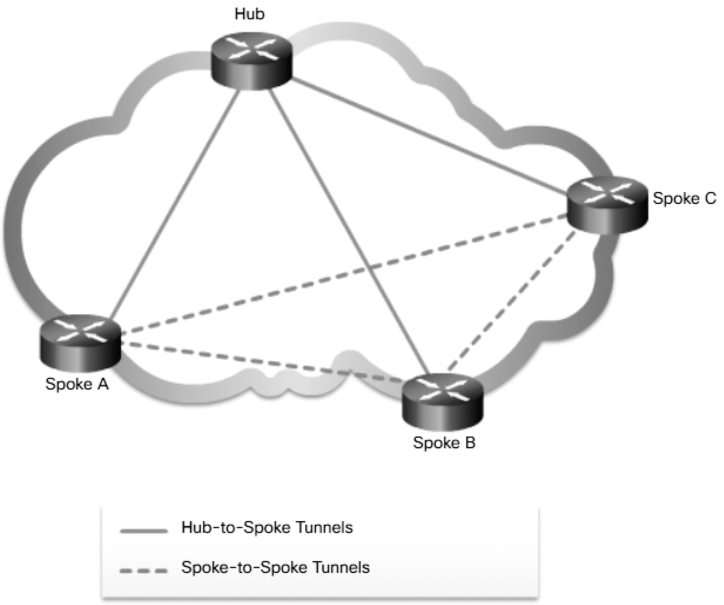


Figure 3-21 DMVPN Hub-to-Spoke and Spoke-to-Spoke Tunnels

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels. DMVPN makes use of ***Multipoint Generic Routing Encapsulation (mGRE)*** tunnel. An mGRE tunnel interface allows a single GRE interface to support multiple IPsec tunnels. With mGRE, dynamically allocated tunnels are created through a permanent tunnel source at the hub and dynamically allocated tunnel destinations, created as necessary, at the spokes. This reduces the size and simplifies the complexity of the configuration.

Like other VPN types, DMVPN relies on IPsec to provide secure transport of private information over public networks, such as the Internet.

Interactive Graphic

Activity 3.3.2.4: Compare Types of VPNs

Refer to the online course to complete this activity.

GRE (3.4)

In this section, you implement a GRE tunnel.

GRE Overview (3.4.1)

In this topic, you learn about the purpose and benefits GRE tunnels.

GRE Introduction (3.4.1.1)

Generic Routing Encapsulation (GRE) is one example of a basic, nonsecure, site-to-site VPN tunneling protocol. GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels. GRE creates a virtual point-to-point link to Cisco routers at remote points, over an IP internetwork.

GRE is designed to manage the transportation of multiprotocol and IP multicast traffic between two or more sites that may have only IP connectivity. It can encapsulate multiple protocol packet types inside an IP tunnel.

As shown in Figure 3-22, a tunnel interface supports a header for each of the following:

- *Passenger protocol*: This is the original IPv4 or IPv6 packet that will be encapsulated by the carrier protocol. It could also be a legacy AppleTalk, DECnet, or IPX packet.
- *Carrier protocol*: This is the encapsulation protocol such as GRE that encapsulates the passenger protocol.
- *Transport protocol*: This is the delivery protocol such as IP that carries the carrier protocol.

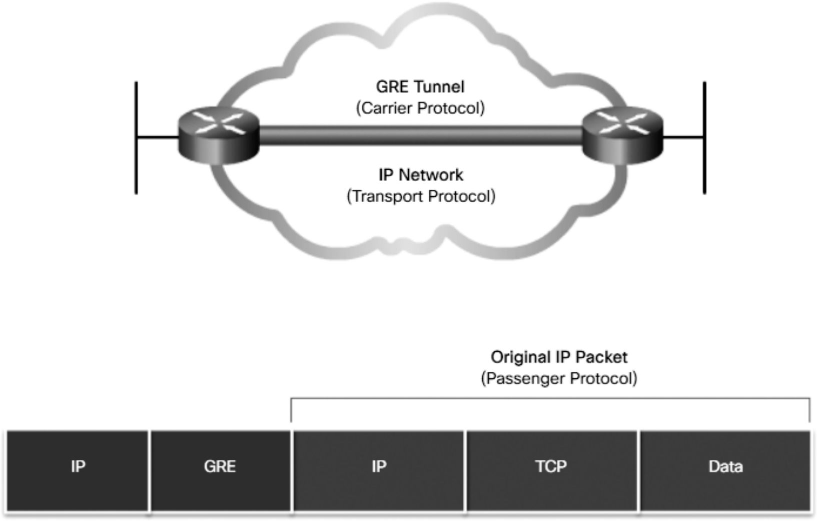


Figure 3-22 Generic Routing Encapsulation

GRE Characteristics (3.4.1.2)

GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. IP tunneling using GRE enables network expansion across a single-protocol backbone environment. It does this by connecting multiprotocol subnetworks in a single-protocol backbone environment.

GRE has these characteristics:

- GRE is defined as an IETF standard (RFC 2784).
- GRE is identified as IP protocol 47 in the Transport protocol IP protocol field.
- GRE encapsulation includes a protocol type field in its header to provide multiprotocol support. Protocol types are defined in RFC 1700 as "EtherTypes."
- GRE is stateless, which means that, by default, it does not include any flow-control mechanisms.
- GRE does not include any strong security mechanisms to protect its payload.
- The GRE header consumes at least 24 bytes of additional overhead for tunneled packets.

Figure 3-23 illustrates the GRE header components.

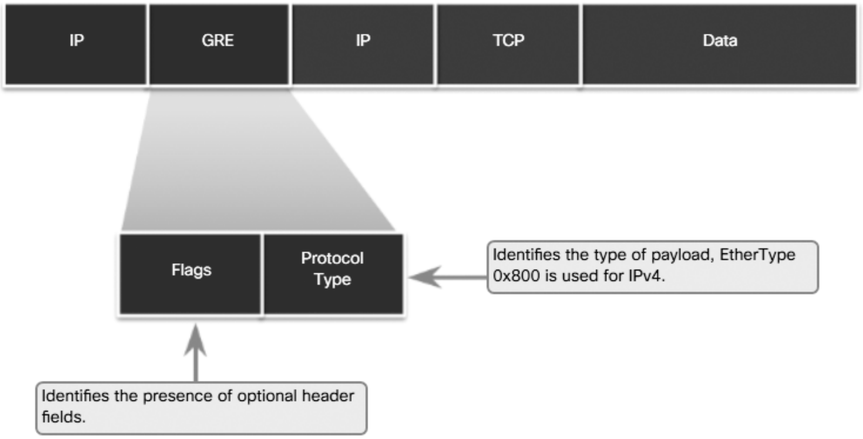

IP
GRE
IP
TCP
Data
Flags
Protocol Type
Identifies the type of payload, EtherType 0x800 is used for IPv4.
Identifies the presence of optional header fields.

Figure 3-23 Header for GRE Encapsulated Packet Header

Interactive Graphic

Activity 3.4.1.3: Identify GRE Characteristics

Refer to the online course to complete this activity.

Implement GRE (3.4.2)

In this topic, you learn how to troubleshoot a site-to-site GRE tunnel.

Configure GRE (3.4.2.1)

The topology displayed in Figure 3-24 will be used to create a GRE VPN tunnel between two sites.

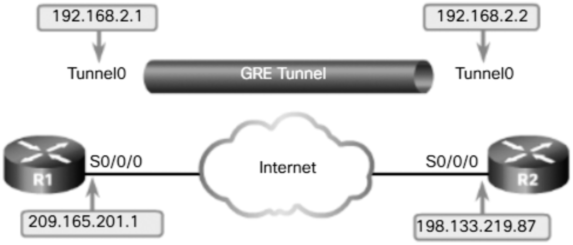


Figure 3-24 GRE Tunnel Configuration Topology

To implement a GRE tunnel, the network administrator must know the reachable IP addresses of the endpoints.

There are five steps to configuring a GRE tunnel:

Step 1. Create a tunnel interface using the **interface tunnel** *number* global configuration command.

Step 2. Configure an IP address for the tunnel interface using the **ip address** *ip-address* interface configuration command. This is normally a private IP address.

Step 3. Specify the tunnel source IP address or source interface using the **tunnel source** {*ip-address* | *interface-name*} interface configuration command.

Step 4. Specify the tunnel destination IP address using the **tunnel destination** *ip-address* interface configuration command.

Step 5. (Optional) Specify GRE tunnel mode as the tunnel interface mode using the **tunnel mode gre** *protocol* interface configuration command. GRE tunnel mode is the default tunnel interface mode for Cisco IOS software.

The sample configuration in Example 3-11 illustrates a basic GRE tunnel configuration for R1 and R2.

Example 3-11 R1 and R2 GRE Tunnel Configuration

```
R1(config)# interface Tunnel0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 209.165.201.2
R1(config-if)# tunnel mode gre ip
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 209.165.201.2
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)# exit
R2(config)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

The minimum configuration requires specification of the tunnel source and destination addresses. The IP subnet must also be configured to provide IP connectivity across the tunnel link. Both tunnel interfaces have the tunnel source set using the IP address of their local serial S0/0/0 interface and the tunnel destination set to the IP address of the peer router serial S0/0/0 interface. The tunnel interface IP address is typically assigned a private IP address. Finally, OSPF is configured to advertise the tunnel network route over the GRE tunnel.

Table 3-1 provides the individual GRE tunnel command descriptions.

Table 3-1 GRE Configuration Command Syntax

Command	Description
ip address *ip_address mask*	Specifies the IP address of the tunnel interface
tunnel source *ip_address*	Specifies the tunnel source IP address, in interface tunnel configuration mode
tunnel destination *ip_address*	Specifies the tunnel destination IP address, in interface tunnel configuration mode
tunnel mode gre ip	Specifies GRE tunnel mode as the tunnel interface mode, in interface tunnel configuration mode

Note

When you are configuring GRE tunnels, it can be difficult to remember which IP networks are associated with the physical interfaces and which IP networks are associated with the tunnel interfaces. Remember that before a GRE tunnel is created, the physical interfaces have already been configured. The **tunnel source** and **tunnel destination** commands reference the IP addresses of the preconfigured physical interfaces. The **ip address** command on the tunnel interfaces refers to an IP network (usually a private IP network) specifically selected for the purposes of the GRE tunnel.

Verify GRE (3.4.2.2)

Several commands can be used to monitor and troubleshoot GRE tunnels. To determine whether the tunnel interface is up or down, use the **show ip interface brief** and **show interface tunnel** *number* privileged EXEC commands, as demonstrated in Example 3-12.

Example 3-12 Verifying GRE

```
R1# show ip interface brief | include Tunnel

Tunnel0                192.168.2.1      YES manual up                up
R1#
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP

<output omitted>
```

The first command verifies that the tunnel 0 interface is up and has an IP address assigned to it. The second command verifies the state of a GRE tunnel, the tunnel source and destination addresses, and the GRE mode supported. The line protocol on a GRE tunnel interface is up as long as there is a route to the tunnel destination. Before a GRE tunnel is implemented, IP connectivity must already be in effect between the IP addresses of the physical interfaces on opposite ends of the potential GRE tunnel.

A routing protocol could also be configured to exchange route information over the tunnel interface. For example if OSPF had also been configured to exchange routes over the GRE tunnel, you could verify that an OSPF adjacency had been established using the **show ip ospf neighbor** command.

In Example 3-13, note that the peering address for the OSPF neighbor is on the IP network created for the GRE tunnel.

Example 3-13 Verifying OSPF Adjacency via GRE Tunnel

```
R1# show ip ospf neighbor

Neighbor ID        Pri  State           Dead Time   Address         Interface
209.165.201.2       0   FULL/  -        00:00:37    192.168.2.2     Tunnel0
```

GRE is considered a VPN because it is a private network that is created by tunneling over a public network. Using encapsulation, a GRE tunnel creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

The advantages of GRE are that it can be used to tunnel non-IP traffic over an IP network, allowing for network expansion by connecting multiprotocol subnetworks across a single-protocol backbone environment. GRE also supports IP multicast tunneling. This means that routing protocols can be used across the tunnel, enabling dynamic exchange of routing information in the virtual network. Finally, it is common practice to create IPv6 over IPv4 GRE tunnels, where IPv6 is the encapsulated protocol and IPv4 is the transport protocol. In the future, these roles will likely be reversed as IPv6 takes over as the standard IP protocol.

However, GRE does not provide encryption or any other security mechanisms. Therefore, data sent across a GRE tunnel is not secure. If secure data communication is needed, IPsec or ***Secure Sockets Layer (SSL)*** VPNs should be configured.

Troubleshoot GRE (3.4.2.3)

Issues with GRE are usually due to one or more of the following misconfigurations:

- The tunnel interface IP addresses are not on the same network or the subnet masks do not match.
- The interfaces for the tunnel source and/or tunnel destination are not configured with the correct IP address or are in the down state.
- Static or dynamic routing is not properly configured.

Figure 3-25 shows the GRE configuration topology.

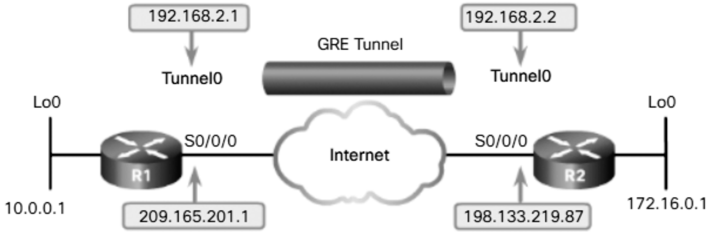


Figure 3-25 GRE Tunnel Configuration Topology

Use the **show ip interface brief** command on both routers to verify that the tunnel interface is up and configured with the correct IP addresses for the physical interface and the tunnel interface. Also, verify that the source interface on each router is up and configured with the correct IP addresses, as shown in Example 3-14.

Example 3-14 Verifying That All Necessary Interfaces Are Up

```
R1# show ip interface brief
<some output omitted>
Interface          IP-Address       OK?  Method    Status    Protocol
Serial0/0/0        209.165.201.1    YES  manual    up        up
Loopback0          10.0.0.1         YES  manual    up        up
Tunnel0            192.168.2.1      YES  manual    up        up
R1#
```

```
R2# show ip interface brief
<some output omitted>
Interface          IP-Address       OK?  Method    Status    Protocol
Serial0/0/0        198.133.219.87   YES  manual    up        up
Loopback0          172.16.0.1       YES  manual    up        up
Tunnel0            192.168.2.2      YES  manual    up        up
R2#
```

Routing can cause an issue. Both routers need a default route pointing to the Internet. Also, both routers need the correct dynamic or static routing configured. You can use the **show ip ospf neighbor** command to verify neighbor adjacency. Regardless of the routing used, you can also use **show ip route** to verify that networks are being passed between the two routers, as shown in Example 3-15.

Example 3-15 Verify That Networks Are Being Routed

```
R1# show ip route ospf
     172.16.0.0/32 is subnetted, 1 subnets
O       172.16.0.0 [110/1001] via 192.168.2.2, 00:19:44, Tunnel0
R1#
```

```
R2# show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.0.0.1 [110/1001] via 192.168.2.1, 00:20:35, Tunnel0
R2#
```

Packet Tracer
□ **Activity**

Packet Tracer 3.4.2.4: Configuring GRE

You are the network administrator for a company that wants to set up a GRE tunnel to a remote office. Both networks are locally configured and need only the tunnel configured.

Packet Tracer
□ **Activity**

Packet Tracer 3.4.2.5: Troubleshooting GRE

A junior network administrator was hired to set up a GRE tunnel between two sites and was unable to complete the task. You have been asked to correct configuration errors in the company network.

Lab 3.4.2.6: Configuring a Point-to-Point GRE VPN Tunnel

In this lab, you complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure a GRE Tunnel
- Part 3: Enable Routing over the GRE Tunnel

eBGP (3.5)

In this section, you implement eBGP in a single-homed remote-access network.

BGP Overview (3.5.1)

In this topic, you learn about the basic BGP features.

IGP and EGP Routing Protocols (3.5.1.1)

RIP, EIGRP, and OSPF are Interior Gateway Protocols (IGPs). ISPs and their customers, such as corporations and other enterprises, usually use an IGP to route traffic within their networks. IGPs are used to exchange routing information within a company network or an autonomous system (AS).

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used for the exchange of routing information between autonomous systems, such as ISPs, companies, and content providers (such as YouTube and Netflix).

In BGP, every AS is assigned a unique 16-bit or 32-bit ***AS number (ASN)***, which uniquely identifies it on the Internet. Figure 3-26 shows an example of how IGPs are interconnected using BGP.

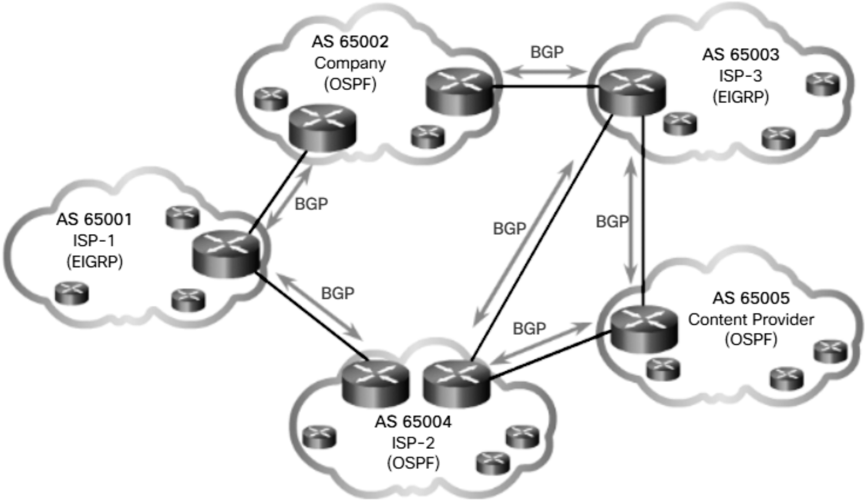


Figure 3-26 IGP and EGP Routing Protocols

Note

Private AS numbers are also available. However, private AS numbers are beyond the scope of this course.

Internal routing protocols use a specific metric, such as OSPF's cost, for determining the best paths to destination networks. BGP does not use a single metric like IGPs. BGP routers exchange several path attributes including a list of AS numbers (hop by hop) necessary to reach a destination network.

For example, in Figure 3-26, AS 65002 may use the AS-path of 65003 and 65005 to reach a network within the content provider AS 65005. BGP is known as a ***path vector routing protocol***.

Note

AS-path is one of several attributes that BGP may use to determine the best path. However, path attributes and BGP best path determination are beyond the scope of this course.

BGP updates are encapsulated over TCP on port 179. Therefore, BGP inherits the connection-oriented properties of TCP, which ensures that BGP updates are transmitted reliably.

IGP routing protocols are used to route traffic within the same organization and administered by a single organization. In contrast, BGP is used to route between networks administered by two different organizations. An AS uses BGP to advertise its networks and, in some cases, networks that it learned about from other autonomous systems, to the rest of the Internet.

eBGP and iBGP (3.5.1.2)

Two routers exchanging BGP routing information are known as BGP peers. As shown in Figure 3-27, there are two types of BGP, as described in the list that follows.

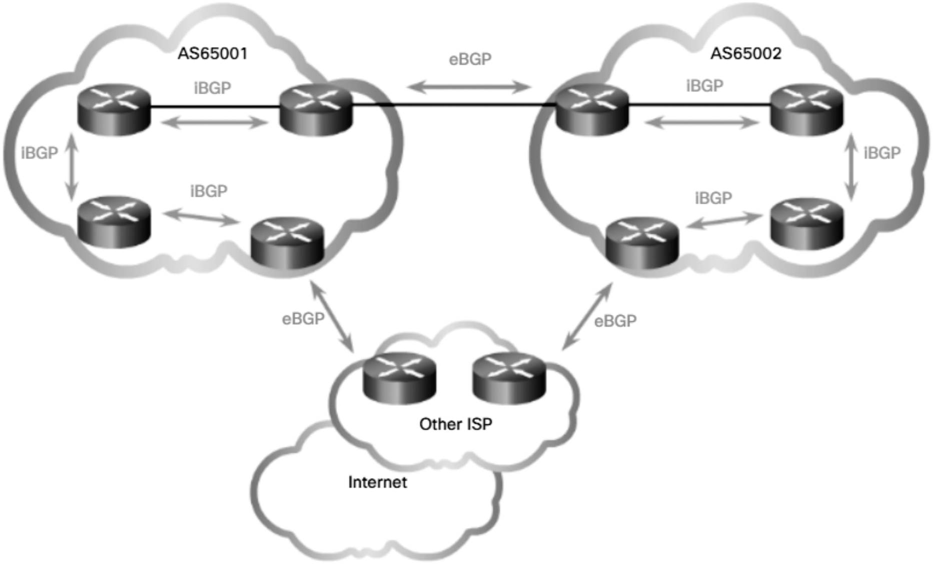


Figure 3-27 eBGP and iBGP Comparison

- ***External BGP (eBGP)***: External BGP is a BGP configuration between two routers in different autonomous systems. For example, eBGP would be used to connect an enterprise AS to a service provider AS.
- ***Internal BGP (iBGP)***: Internal BGP is a BGP configuration between two routers in the same autonomous systems. For example, iBGP would be used between routers in a service provider AS.

This course focuses on eBGP only.

Note

There are differences in how eBGP peers and iBGP peers operate; however, these differences are beyond the scope of this course.

BGP Design Considerations (3.5.2)

In this topic, you learn about BGP design considerations.

When to Use BGP (3.5.2.1)

The use of BGP is most appropriate when an AS has connections to multiple autonomous systems. This is known as ***multihomed***. Each AS in Figure 3-28 is multihomed because each AS has connections to at least two other autonomous systems or BGP peers.

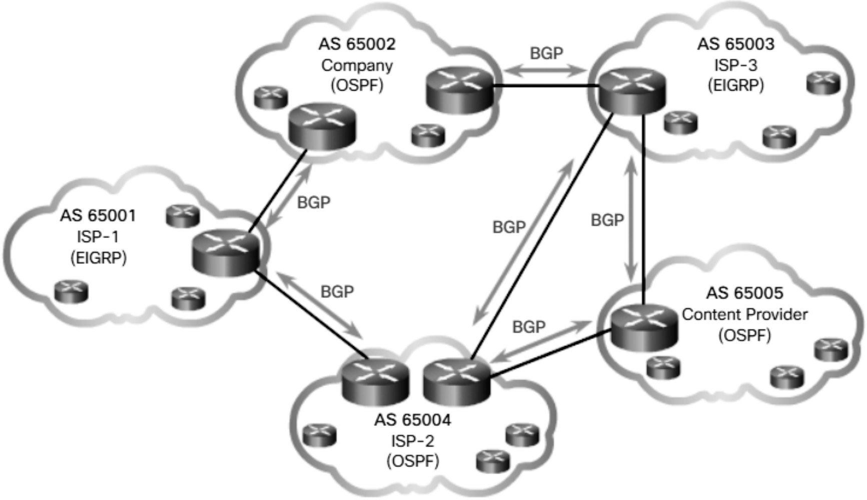


Figure 3-28 Multihomed

When Not to Use BGP (3.5.2.2)

BGP should not be used when at least one of the following conditions exist:

- There is a single connection to the Internet or another AS. This is known as ***single-homed***. In this case, Company-A may run an IGP with the ISP, or Company-A and the ISP each use static routes, as shown in Figure 3-29. Although it is recommended only in unusual situations, for the purposes of this course, you will configure single-homed BGP.
- There is a limited understanding of BGP. A misconfiguration of a BGP router can have far-reaching effects beyond the local AS, negatively impacting routers throughout the Internet.

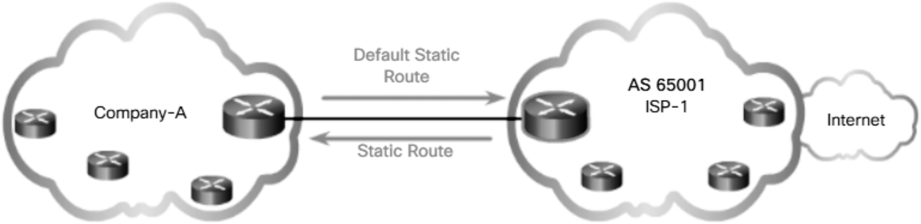


Figure 3-29 Single-Homed

Note

In some single-homed situations, BGP may be appropriate, such as the need for a specific routing policy. However, routing policies are beyond the scope of this course.

BGP Options (3.5.2.3)

BGP is used by autonomous systems to advertise networks that originated within their AS or, in the case of ISPs, the networks that originated from other autonomous systems.

For example, a company connecting to its ISP using BGP would advertise its network addresses to the ISP. The ISP would then advertise these networks to other ISPs (***BGP peers***). Eventually, all other autonomous systems on the Internet would learn about the networks initially originated by the company.

An organization can choose to implement BGP in a multihomed environment in three common ways.

Default Route Only

ISPs advertise a default route to Company-A, as shown in Figure 3-30.

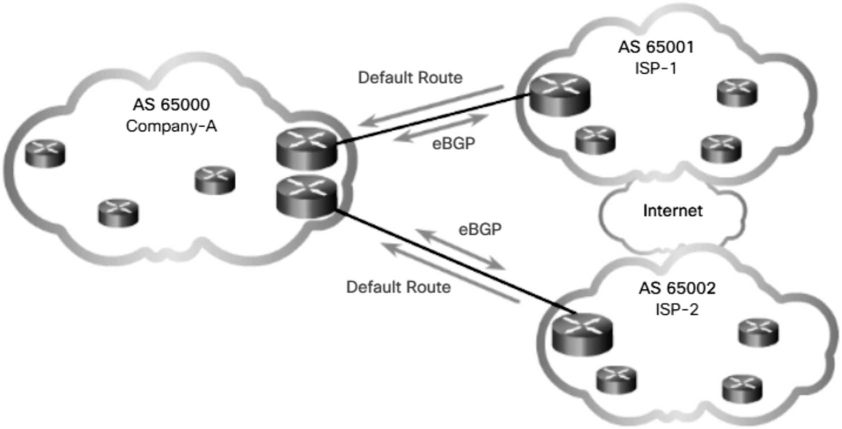


Figure 3-30 Default Route Only

The arrows indicate that the default is configured on the ISPs, not on Company-A. This is the simplest method to implement BGP; however, because the company receives only a default route from both ISPs, suboptimal routing may occur. For example, Company-A may choose to use ISP-1's default route when sending packets to a destination network in ISP-2's AS.

Default Route and ISP Routes

ISPs advertise their default route and their network to Company-A, as shown in Figure 3-31.

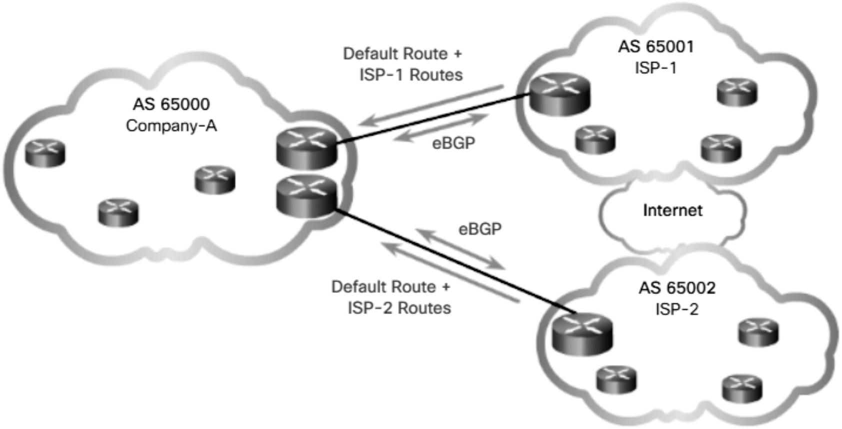


Figure 3-31 Default Route and ISP Routes

This option allows Company-A to forward traffic to the appropriate ISP for networks advertised by that ISP. For example, Company-A would choose ISP-1 for networks advertised by ISP-1. For all other networks, one of the two default routes can be used, which means suboptimal routing may still occur for all other Internet routes.

All Internet Routes

ISPs advertise all Internet routes to Company-A, as shown in Figure 3-32.

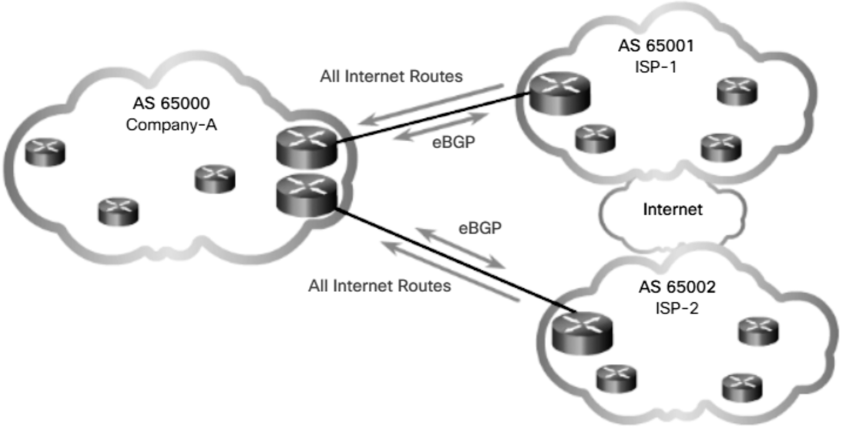


Figure 3-32 All Internet Routes

Because Company-A receives all Internet routes from both ISPs, Company-A can determine which ISP to use as the best path to forward traffic for any network. Although this approach solves the issue of suboptimal routing, the BGP router would require sufficient resources to maintain well over 500,000 Internet networks.

Interactive Graphic

Activity 3.5.2.4: Identify BPG Terminology and Designs

Refer to the online course to complete this activity.

eBGP Branch Configuration (3.5.3)

In this topic, you configure an eBGP branch connection.

Steps to Configure eBGP (3.5.3.1)

To implement eBGP for this course, you need to complete the following tasks:

Step 1. Enable BGP routing.

Step 2. Configure BGP neighbor(s) (peering).

Step 3. Advertise network(s) originating from this AS.

Table 3-2 lists the command syntax and a description for basic eBGP configuration.

Table 3-2 BGP Configuration Commands

Command	Description
Router(config)# **router bgp** *as-number*	Enables a BGP routing process and places the router in router configuration mode.
Router(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	Specifies a BGP neighbor. The *as-number* is the neighbor's AS number.
Router(config-router)# **network** *network-address* [**mask** *network-mask*]	Advertises a network address to an eBGP neighbor as being originated by this AS. The *network-mask* is the subnet mask of the network.

BGP Sample Configuration (3.5.3.2)

In this single-homed BGP topology, Company-A in AS 65000 uses eBGP to advertise its 198.133.219.0/24 network to ISP-1 at AS 65001. ISP-1 advertises a default route in its eBGP updates to Company-A.

Note

BGP is usually not necessary in single-homed AS. It is used here to provide a simple configuration example.

Figure 3-33 shows the BGP configuration topology.

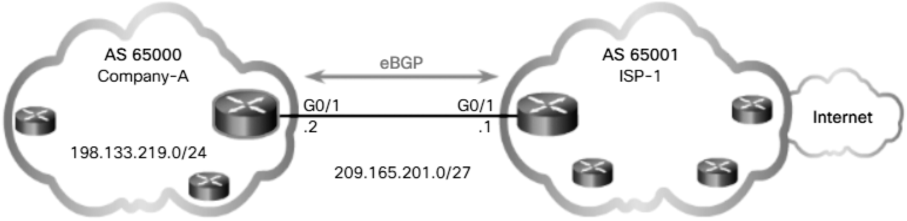


Figure 3-33 BGP Configuration Topology

Example 3-16 shows the BGP configuration for Company-A and ISP-1. Customers typically use private IPv4 address space for internal devices within their own network. Using *Network Address Translation (NAT)*, the Company-A router translates these private IPv4 addresses to one of its public IPv4 addresses, advertised by BGP to the ISP.

Example 3-16 Company-A and ISP BGP Configuration

```
Company-A(config)# router bgp 65000
Company-A(config-router)# neighbor 209.165.201.1 remote-as 65001
Company-A(config-router)# network 198.133.219.0 mask 255.255.255.0
```

```
ISP-1(config)# router bgp 65001
ISP-1(config-router)# neighbor 209.165.201.2 remote-as 65000
ISP-1(config-router)# network 0.0.0.0
```

The **router bgp** global configuration command enables BGP and identifies the AS number for Company-A. A router can belong to only a single AS, so only a single BGP process can run on a router.

The **neighbor** router configuration command identifies the BGP peer IP address and AS number. Notice that the ISP AS number is different than the Company-A AS number. This informs the BGP process that the neighbor is in a different AS and is therefore an external BGP neighbor.

The **network** *network-address* [**mask** *network-mask*] router configuration command enters the *network-address* into the local BGP table. The BGP table contains all routes learned via BGP or advertised using BGP. eBGP will then advertise the *network-address* to its eBGP neighbors.

The **mask** *network-mask* command parameter must be used when the network advertised is different from its classful equivalent. In this example, the 198.133.219.0/24 is equivalent to a class C network. Class C networks have a /24 subnet mask, so in this case the **mask** option is not required. If Customer-A were advertising the 198.133.0.0/16 network, the **mask** option would be required. Otherwise, BGP would advertise the network with a /24 classful mask.

Note

In contrast to an IGP protocol, the *network-address* used in the **network** command does not have to be a directly connected network. The router only needs to have a route to this network in its routing table.

The eBGP commands on the ISP-1 router are similar to the configuration on Company-A. Notice how the **network 0.0.0.0** router configuration command is used to advertise a default network to Company-A.

Note

Although the **network 0.0.0.0** command is a valid BGP configuration option, there are better ways to advertise a default route in eBGP. However, these methods are beyond the scope of this course.

Verify eBGP (3.5.3.3)

You can use three commands to verify eBGP, as described in Table 3-3.

Table 3-3 BGP Verification Commands

Command	Description
Router# **show ip route**	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table
Router# **show ip bgp**	Verify that received and advertised IPv4 networks are in the BGP table
Router# **show ip bgp summary**	Verify IPv4 BGP neighbors and other BGP information

Example 3-17 shows the output for Company-A's IPv4 routing table. Notice how the origin code **B** identifies that the route was learned using BGP. Specifically, in this example, Company-A has received a BGP advertised default route from ISP-1.

Example 3-17 Verifying BGP Routes Are in the Table

```
Company-A# show ip route | include Gateway

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.201.1, 00:36:03
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/24 is directly connected, GigabitEthernet0/0
L        198.133.219.1/32 is directly connected, GigabitEthernet0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.2/32 is directly connected, GigabitEthernet0/1
Company-A#
```

Example 3-18 shows the output of Company-A's BGP table.

Example 3-18 Verifying BGP

```
Company-A# show ip bgp
BGP table version is 3, local router ID is 209.165.201.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf  Weight Path
 *>  0.0.0.0          209.165.201.1            0              0 65001 i
 *>  198.133.219.0/24 0.0.0.0                  0          32768 i
Company-A#
```

The first entry 0.0.0.0 with a next hop of 209.165.201.1 is the default route advertised by ISP-1. The AS path displays the single AS of 65001 because the 0.0.0.0/0 network advertised by ISP-1 originated from the same AS. Most BGP table entries show multiple autonomous system numbers in the path, listing the sequence of AS numbers required to reach the destination network.

The second entry 198.133.219.0/24 is the network advertised by the Company-A router to ISP-1. The next hop address of 0.0.0.0 indicates that the 198.133.219.0/24 network originated from this router.

Example 3-19 displays the status of BGP connection on Company-A. The first line displays the local IPv4 address used to peer with another BGP neighbor and this router's local AS number. The address and AS number of the remote BGP neighbor are shown at the bottom of the output.

Example 3-19 Verify BGP Summary

```
Company-A# show ip bgp summary
BGP router identifier 209.165.201.2, local AS number 65000
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V        AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
209.165.201.1   4     65001      66      66        3    0    0 00:56:11            1
Company-A#
```

Packet Tracer
☐ Activity

Packet Tracer 3.5.3.4: Configure and Verify eBGP

In this activity, you configure and verify the operation of eBGP between autonomous systems 65001 and 65002.

Lab 3.5.3.5: Configure and Verify eBGP

In this lab, you complete the following objectives:

- Build the Network and Configure Basic Device Settings
- Configure eBGP on R1
- Verify eBGP Configuration

Summary (3.6)

Class Activity 3.6.1.1: VPN Planning Design

Your small- to medium-sized business has received quite a few new contracts lately. This circumstance has increased the need for teleworkers and workload outsourcing. The new contract vendors and clients will also need access to your network as the projects progress.

As network administrator for the business, you recognize that VPNs must be incorporated as a part of your network strategy to support secure access by the teleworkers, employees, and vendors or clients.

To prepare for implementation of VPNs on the network, you devise a planning checklist to bring to the next department meeting for discussion.

Packet Tracer
□ **Activity**

Packet Tracer 3.6.1.2: Skills Integration Challenge

In this skills integration challenge, the XYZ Corporation uses a combination of eBGP, PPP, and GRE WAN connections. Other technologies include DHCP, default routing, OSPF for IPv4, and SSH configurations.

Lab 3.6.1.3: Configure a Branch Connection

In this lab, you configure two separate WAN connections: a BGP route over a PPPoE connection and a BGP route over a GRE tunnel. This lab is a test-case scenario and does not represent a realistic BGP implementation.

- Part 1: Build the Network and Load Device Configurations
- Part 2: Configure a PPPoE Client Connection
- Part 3: Configure a GRE Tunnel
- Part 4: Configure BGP over PPPoE and BGP over a GRE Tunnel

Broadband transmission is provided by a wide range of technologies, including DSL, fiber-to-the-home, coaxial cable systems, wireless, and satellite. This transmission requires additional components at the home end and at the corporate end. Broadband wireless solutions include municipal Wi-Fi, cellular/mobile, and satellite Internet. Municipal Wi-Fi mesh networks are not widely deployed. Cellular/mobile coverage can be limited and bandwidth can be an issue. Satellite Internet is relatively expensive and limited, but it may be the only method to provide access.

If multiple broadband connections are available to a particular location, a cost-benefit analysis should be performed to determine the best solution. The best solution may be to connect to multiple service providers to provide redundancy and reliability.

PPPoE is a popular data link protocol for connecting remote networks to their ISPs. PPPoE provides the flexibility of PPP and the convenience of Ethernet.

VPNs are used to create a secure end-to-end private network connection over a third-party network, such as the Internet. GRE is a basic, nonsecure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN. Today it is primarily used to deliver IP multicast traffic or IPv6 traffic over an IPv4 unicast-only connection.

BGP is the routing protocol implemented between autonomous systems. Three basic design options for eBGP are as follows:

- The ISP advertises a default route only to the customer.
- The ISP advertises a default route and all its routes to the customer.
- The ISP advertises all Internet routes to the customer.

Implementing eBGP in a single-homed network requires only a few commands.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Connecting Networks v6 Labs & Study Guide* (ISBN 9781587134296). The Packet Tracer Activity instructions are also in the *Labs & Study Guide*. The PKA files are found in the online course.

Class Activities

Class Activity 3.0.1.2: Broadband Varieties

Class Activity 3.6.1.1: VPN Planning Design

Labs

Lab 3.1.2.2: Researching Broadband Internet Access Technologies

Lab 3.2.2.7: Configuring a Router as a PPPoE Client for DSL Connectivity

Lab 3.2.2.8: Troubleshoot PPPoE

Lab 3.4.2.6: Configuring a Point-to-Point GRE VPN Tunnel

Lab 3.5.3.5: Configure and Verify eBGP

Lab 3.6.1.3: Configure a Branch Connection

Packet Tracer □ Activity

Packet Tracer Activities

Packet Tracer 3.4.2.4: Configuring GRE

Packet Tracer 3.4.2.5: Troubleshooting GRE

Packet Tracer 3.5.3.4: Configure and Verify eBGP

Packet Tracer 3.6.1.2: Skills Integration Challenge

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix "Answers to the 'Check Your Understanding' Questions" lists the answers.

1. Which technology provides a secure connection between a SOHO and the headquarters office?

   A. PPPoE

   B. QoS

   C. VPN

   D. WiMax

2. Which two network components does a teleworker require to connect remotely and securely from home to the corporate network? (Choose two.)

   A. Authentication server

   B. Broadband Internet connection

   C. VPN client software or VPN-enabled router

   D. Multifunction security appliance

   E. VPN server or concentrator

3. What advantage does DSL have compared to cable technology?

   A. DSL has no distance limitations.

   B. DSL is faster.

   C. DSL is not a shared medium.

   D. DSL upload and download speeds are always the same.

4. Which medium is used for delivering data via DSL technology through PSTN?

   A. Copper

   B. Fiber

   C. Radio frequency

   D. Wireless

5. What technology provides service providers the capability to use authentication, accounting, and link management features to customers over Ethernet networks?

   A. DSL

   B. ISDN

   C. PPPoE

   D. QoS

6. Why is the MTU for a PPPoE DSL configuration reduced from 1500 bytes to 1492?

   A. To accommodate the PPPoE headers

   B. To enable CHAP authentication

   C. To establish a secure tunnel with less overhead?

   D. To reduce congestion on the DSL link

7. What are two characteristics of a PPPoE configuration on a Cisco customer router? (Choose two.)

   A. An MTU size of 1492 bytes is configured on the Ethernet interface.

   B. The customer router CHAP username and password are independent of what is configured on the ISP router.

   C. The **dialer pool** command is applied to the Ethernet interface to link it to the dialer interface.

   D. The Ethernet interface does not have an IP address.

   E. The PPP configuration is on the dialer interface.

8. When PPPoE is configured on a customer router, which two commands must have the same value for the configuration to work? (Choose two.)

   A. **dialer pool 2**

   B. **interface dialer 2**

   C. **interface gigabitethernet 0/2**

   D. **ppp chap hostname 2**

   E. **ppp chap password 2**

   F. **pppoe-client dial-pool-number 2**

9. A network design engineer is planning the implementation of a cost-effective method to interconnect multiple networks securely over the Internet. Which type of technology is required?

   A. A dedicated ISP

   B. A GRE IP tunnel

   C. A leased line

   D. A VPN gateway

10. Which statement describes a feature of site-to-site VPNs?

    A. Individual hosts can enable and disable the VPN connection.

    B. Internal hosts send normal, unencapsulated packets.

    C. The VPN connection is not statically defined.

    D. VPN client software is installed on each host.

11. Which remote-access implementation scenario will support the use of Generic Routing Encapsulation tunneling?

    A. A branch office that connects securely to a central site

    B. A central site that connects to a SOHO site without encryption

    C. A mobile user who connects to a router at a central site

    D. A mobile user who connects to a SOHO site

12. Which two statements are key characteristics of BGP? (Choose two.)

    A. It provides interdomain routing between autonomous systems.

    B. It is an advanced distance vector routing protocol.

    C. It uses cost as its metric.

    D. It is a link-state routing protocol.

    E. It uses bandwidth and delay as its metric.

    F. It is a policy-based routing protocol.

13. Which BGP routers will become peers and share routing information?

    A. All BGP routers in the same domain share routing information by default
    B. BGP routers that are configured with the same **network** command
    C. BGP routers that are configured with the same **peer** command
    D. BGP routers that are identified with the **neighbor** command

14. Which of the following BGP statements is true?

    A. BGP is an IGP used to exchange routing information with another AS.
    B. BGP updates are encapsulated using TCP port 179.
    C. Every AS is assigned a unique 160-bit AS number (ASN).
    D. Use BGP when there is a single connection to the Internet or another AS.

15. Assume R1 is in AS 5000 and wants to establish an eBGP peer relationship with another router. Which of the following commands would correctly configure an eBGP relationship?

    A. R1(config-router)# **neighbor 209.165.201.1 remote-as 5000**
    B. R1(config-router)# **neighbor 209.165.201.1 remote-as 10000**
    C. R1(config-router)# **peer 209.165.201.1 remote-as 5000**
    D. R1(config-router)# **peer 209.165.201.1 remote-as 10000**

Index

Symbols

[no] debug ?, 364

Numbers

2G/3G/4G wireless, 111
3G/4G wireless, 38
  Public WAN infrastructure, 37–38
5G, 111
802.1X, secure device access, 233–234

A

AAA (Authentication, Authorization, and Accounting), 217
  secure administrative access, 231–233
abstraction layers, virtualization, 321–322
access control entries (ACEs), 156
access control lists. *See* **ACLs (access control lists)**
access servers, 16
ACEs (access control entries), 156
ACI (Application Centric Infrastructure), 328, 332
  spine-leaf topology, 333–334
ACL Analysis, APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 338
ACL Path Trace, 338
ACLs (access control lists), 156
  APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 337–339
  applying to interfaces, 158–159
  comparing IPv4 and IPv6 ACLs, 185–186
  deleting, 168, 190
  extended IPv4 ACLs
    applying to interfaces, 177–178
    configuring, 175–177
    editing, 182–183
    filtering traffic, 178–180
    structure of, 173–175
    verifying, 181–182
  extended named ACLs, creating, 180–181
  IPv4 ACLs, 162
    troubleshooting, 197–201
  IPv6 ACLs
    applying to interfaces, 189–190
    configuring, 188–189
    deny FTP, 190
    processing packets, 194–197
    restricted access, 190–191
    troubleshooting, 201–207
    types of, 184–185
    verifying, 192–193
  logic operations, 195–196
  named ACLs, 163
  numbered ACLs, 163
  packet filtering, 160–161
  placement of, 163–164
  standard ACLs, configuring, 167–169
  standard IPv4 ACLs, applying, 169–170
  standard named IPv4 ACLs, 170–171
  TCP conversations, 159–160
  transport layer troubleshooting, 394–396
  troubleshooting topology, 421
  verifying, 171–172, 420–422
  wildcard masks, 156–158
Adaptive Security Appliance (ASA), 124
address mapping errors, 391
Address Resolution Protocol (ARP), 127
ADSL (asymmetric DSL), 107
AF (assured forwarding), 293–294
algorithms, queuing. *See* **queuing algorithms**
all Internet routes, BGP (Border Gateway Protocol), 142
amplifiers, 105
analyzing suspicious traffic, SPAN (Switched Port Analyzer), 257
ANP (Application Network Profile), 332
antenna site, 105
APIC (Application Policy Infrastructure Controller), 333
  spine-leaf topology, 333–334

APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 334, 336–337
ACLs (access control lists), 337–339
APIs (application programming interfaces), 329
Application Centric Infrastructure (ACI), 328, 332
spine-leaf topology, 333–334
application enablement platform pillar, Cisco IoT System, 313–314
application layer troubleshooting, 397–398
Application Network Profile (ANP), 332
Application Policy Infrastructure Controller (APIC), 333
Application Policy Infrastructure Controller-Enterprise Module (APIC-EM), 334, 336–337
application programming interfaces (APIs), 329
architecture, 329–330
PPP (Point-to-Point Protocol), 65–66
arp, 406, 407, 409
ARP (Address Resolution Protocol), 127
arp -d, 407
AS number (ASN), 137
ASA (Adaptive Security Appliance), 124
ASN (AS number), 137
AS-path, 138
assured forwarding (AF), 293–294
asymmetric DSL (ADSL), 107
Asynchronous Transfer Mode. *See* ATM (Asynchronous Transfer Mode)
ATM (Asynchronous Transfer Mode), 57
private WAN infrastructure, 29–30
att, brute-force password attack, 221
attacks
CDP reconnaissance attacks, LAN security, 219–220
common attacks, LAN security, 218–219
DHCP attacks, 226–227
mitigating, 230–231
DHCP spoofing attack, 226–227
DHCP starvation attack, 227
DoS attack, 227
MAC address table flooding attack, 222–224
mitigating, 228–229
Telnet attacks, LAN security, 220–222
Telnet DoS attack, 221
VLAN attacks, 225–226
mitigating, 229–230
attenuation, troubleshooting, 389
authentication
PPP (Point-to-Point Protocol), configuration options, 74
PPPoE (Point-to-Point Protocol over Ethernet), 119–120
Authentication, Authorization, and Accounting. *See* AAA (Authentication, Authorization, and Accounting)
authentication servers, 234
authenticators, 234
autonegotiation, 404
avoiding, packet loss, 288–289

B

bandwidth, 96
network transmission quality, 272–273
serial bandwidth, 54–56
baselines, network documentation, 355–357
baselining tools, 379
basic configuration commands, PPP (Point-to-Point Protocol), 76
Basic Rate Interface. *See* BRI (Basic Rate Interface)
BE (best effort), 293
best practices
LAN security
mitigating DHCP attacks, 230–231
mitigating MAC address flooding table attacks, 228–229
mitigating VLAN attacks, 229–230
secure administrative access with AAA, 231–233
secure device access with 802.1X, 233–234
securing the LAN, 227–228
SNMP (Simple Network Management Protocol), 252–253
best-effort model, 284
QoS (quality of service), 284
BGP (Border Gateway Protocol), 103
design considerations, 139–140
eBGP (external BGP), 138–139
configuring, 142–144
verifying configurations, 145–147
iBGP (internal BGP), 138–139
IGP (Interior Gateway Protocols) and EGP (Exterior Gateway Protocols), 137–138
options, 140–142
BOOTP, transport layer troubleshooting, 396

Border Gateway Protocol. ***See*** **BGP (Border Gateway Protocol)**

bottom-up troubleshooting method, 368

branch networks, WANs (wide area networks), 10–11

BRI (Basic Rate Interface), 27

broadband connections

- BGP (Border Gateway Protocol)
  - *design considerations, 139–140*
  - *IGP (Interior Gateway Protocols) and EGP (Exterior Gateway Protocols), 137–138*
  - *options, 140–142*
- cable system, 104–106
- comparing, 112
- DSL (digital subscriber line), 107–108
- GRE (Generic Routing Encapsulation), 129–130
  - *configuring, 131–133*
  - *troubleshooting, 134–136*
- PPPoE (Point-to-Point Protocol over Ethernet), 113–115
  - *configuring, 115–116*
- VPNs (virtual private networks), 123–125
  - *DMVPN (Dynamic Multipoint VPN), 127–128*
  - *remote-access VPNs, 126*
  - *site-to-site VPNs, 125–126*
- wireless, 109–112

broadband modems, 16

brute-force password attack, 221

buffered logging, 386

C

cable, 112

- public WAN infrastructure, 35

cable analyzers, 382–383

cable modem termination system (CMTS), 35, 106

cable modems (CMs), 35, 106

cable system, 104–106

cable testers, 381–383

cabling faults, troubleshooting, 389

CAM table overflow attack, 222

campus networks, WANs (wide area networks), 9–10

carrier protocol, GRE (Generic Routing Encapsulation), 129

CBWFQ (Class-Based Weighted Fair Queuing), 281–282

CDP (Cisco Discovery Protocol), 219–220

CDP reconnaissance attacks, LAN security, 219–220

CEF (Cisco Express Forwarding), 326–327

CEF Forwarding Information Base (FIB), 327

cellular, 110–111, 112

- 3G/4G cellular, 37–38

central office (CO), 15, 105

centralized control plane, 327–328

Challenge Handshake Authentication Protocol. ***See*** **CHAP (Challenge Handshake Authentication Protocol)**

channel service unit/data service unit (CSU/DSU), 17

CHAP (Challenge Handshake Authentication Protocol), 85–86

CHAP authentication, configuring, 88–89

cHDLC (Cisco HDLC), 58, 96

CIR (customer information rate), 297

circuit switching, WANs (wide area networks), 17–18

Cisco 7000 series routers, 63

Cisco AnyConnect Secure Mobility Client Software, 126

Cisco Application Centric Infrastructure (ACI), 328, 332

- spine-leaf topology, 333–334

Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM), 334, 336–337

Cisco Discovery Protocol. ***See*** **CDP reconnaissance attacks**

Cisco Express Forwarding (CEF), 326–327

Cisco FirePOWER 8000 Series Appliance, 312

Cisco HDLC, 58, 96

Cisco Industrial Security Appliance 3000, 311

Cisco IoT System, 307

- application enablement platform pillar, 313–314
- data analytics pillar, 312
- fog computing pillar, 308–310
- management and automation pillar, 313
- network connectivity pillar, 308
- security pillar, 311–312

Cisco IOx, 314

Cisco NAM, 384–385

Cisco Nexus 9000 Series switches, 333

Cisco Switched Port Analyzer. ***See*** **SPAN (Switched Port Analyzer)**

Cisco UCS Manager, 325

Cisco Unified Computing System (UCS), 324–325

Cisco Video Surveillance IP cameras, 312

Cisco Visual Networking Index (VNI), 275–276

class activities
Branching Out, 3
Broadband Varieties, 103–104
Documentation Development, 425
Network Breakdown, 349
Network Maintenance Development, 217
PPP persuasion, 51
PPP Validation, 96
VPN Planning Design, 148
WAN device modules, 43
Class of Service (CoS), Ethernet markings, 291–292
Class-Based Weighted Fair Queuing (CBWFQ), 281–282
classification and marking, QoS (quality of service), 290–291
classification and marking tools, QoS (quality of service), 289
client/server model, 308–309
clock skew, 52–53
cloud computing, 314–315
cloud models, 315–316
cloud services, 315
versus data center, 316–317
virtualization, 317–318
cloud computing model, 308–309
cloud models, 315–316
cloud services, 315
CMs (cable modems), 35
CMTS (cable modem termination system), 35, 106
CO (central office), 15, 105
coaxial cable, 106
code delay, 273
command syntax, extended ACLs, 176
common attacks, LAN security, 218–219
community clouds, 316
community strings, SNMP (Simple Network Management Protocol), 241–243
comparing ACLs (access control lists), IPv4 and IPv6 ACLs, 185–186
compression
IPCP, 73
PPP (Point-to-Point Protocol), configuration options, 74
compression commands, PPP (Point-to-Point Protocol), 76–77
configuration commands, BGP (Border Gateway Protocol), 143
configuration options, PPP (Point-to-Point Protocol), 72
configuring
CHAP authentication, 88–89
eBGP (external BGP), 142–144
verifying, 145–147
extended IPv4 ACLs, 175–177
GRE (Generic Routing Encapsulation), 131–133
HDLC encapsulation, 58
IPv6 ACLs, 188–189
IPv6 topology, 186–188
local SPAN, 260–261
MPPP (multilink PPP), 79
PAP authentication, 87–88
PPP (Point-to-Point Protocol)
basic configuration commands, 76
compression commands, 76–77
configuration options, 74–75
link quality monitoring command, 77–78
multilink PPP commands, 78–80
verifying, 81–82
PPP authentication, 87–89
CHAP (Challenge Handshake Authentication Protocol), 85–86
PAP (Password Authentication Protocol), 83–85
ppp authentication command, 86–87
PPP authentication protocols, 83
PPPoE (Point-to-Point Protocol over Ethernet), 115–116
SNMP (Simple Network Management Protocol), 248–249
verifying configurations, 249–252
SNMPv3, 254
verifying, 254–255
standard ACLs, 167–169
standard named IPv4 ACLs, 170–171
congestion, 388
network transmission quality, 272–273
congestion avoidance, QoS (quality of service), 296–297
congestion avoidance tools, QoS (quality of service), 289
congestion management tools, QoS (quality of service), 289

connectionless systems, 18
connection-oriented systems, 18–19
connectivity issues, 393
console error messages, 388
console logging, 386
console messages, troubleshooting, 391
control plane, 326
controller settings, verifying, 63
controller-based SDN, 335
controllers
  ACI (Application Centric Infrastructure), 332
  APIC (Application Policy Infrastructure Controller), spine-leaf topology, 333–334
  SDN controllers, 331–332
converged networks, 305–306
core routers, 17
correct path, verifying, 415–418
CoS (Class of Service), Ethernet markings, 291–292
CPE (customer premises equipment), 14, 107
CPU overload, 389–390
CSU/DSU (channel service unit/data service unit), 17
customer information rate (CIR), 297
customer premises equipment (CPE), 14, 107

D

DAI (Dynamic ARP Inspection), 228
data, measuring, 358–360
data analytics pillar, Cisco IoT System, 312
data centers, versus cloud computing, 316–317
data communications equipment (DCE), 15
data delay, data traffic, 278
data link layer, OSI model, WANs (wide area networks), 13
data link layer troubleshooting, 390–392
Data Over Cable Service Interface Specification (DOCSIS), 104
data plane, 326
data terminal equipment (DTE), 15
data traffic, 275, 277–278
data-link connection identifier (DLCI), 29
DCE (data communications equipment), 15
debug command, 90, 364, 393
debug ppp authentication command, 94
debug ppp command, 90
debug ppp error command, 93
debug ppp negotiation command, 92–93
debug ppp packet command, 91
debugging, PPP (Point-to-Point Protocol), 88–93
decision process
  extended ACLs, 197
  standard ACLs, 196–197
dedicated servers, virtualization, 318
default gateway, verifying, 411–415
default route, BGP (Border Gateway Protocol), 141–142
default route only, BGP (Border Gateway Protocol), 140–141
de-jitter delay, 273
delays, network transmission quality, 272–273
deleting
  ACLs (access control lists), 168, 190
  extended named ACLs, 180
demarcation point, 15, 96
dense wavelength division multiplexing (DWDM), 22–23
deny FTP, IPv6 ACLs, 190
DENY-ACCESS ACL, 205
description keyword, 169
design considerations, BGP (Border Gateway Protocol), 139–140
destination (SPAN) port, 258
device-based SDN, 334–335
devices, WANs (wide area networks), 16–17
DHCP (Dynamic Host Configuration Protocol), transport layer troubleshooting, 396
DHCP attacks
  LAN security, 226–227
  mitigating, 230–231
DHCP snooping, 230–231
DHCP spoofing attack, 226–227
DHCP starvation attack, 227
diagrams, network topology diagrams, 352–354
dialer interfaces, 116
dialer pool number, 116
dialup, private WAN infrastructure, 25–26
dialup modems, 16
Differentiated Services Code Point (DSCP), 293–294
DiffServ (differentiated services), 284, 286–288
digital multimeters (DMMs), 381–382
digital signal processor (DSP), 274, 326

digital subscriber line (DSL), 9
disabling
  CDP (Cisco Discovery Protocol), 220
  MPPP (multilink PPP), 80
distributed networks, WANs (wide area networks), 11–12
distribution area, 106
divide-and-conquer method, troubleshooting, 369–370
DLCI (data-link connection identifier), 29
DMMs (digital multimeters), 381–382
DMVPN (Dynamic Multipoint VPN), 127–128
DNS
  transport layer troubleshooting, 396–397
  verifying, 422–423
DOCSIS (Data over Cable Service Interface Specification), 104
documentation, network documentation. *See* network documentation
documenting the network. *See also* network documentation
DoS attack, 227
DSCP (Differentiated Services Code), 293–294
DSL (digital subscriber line), 9, 107–108, 112
  public WAN infrastructure, 34
DSL access multiplexer (DSLAM), 34, 107, 108
DSL filter, 108
DSL micro filter, 108
DSL routers, 108–109
DSL transceiver, 108
DSLAM (DSL access multiplexer), 34, 107, 108
DSP (digital signal processor), 274, 326
DTE (data terminal equipment), 15
DTP (Dynamic Trunking Protocol), 225–226
dual-homed topology, WANs (wide area networks), 6–7
duplex auto, 406
duplex mismatches, checking for, 404–406
DWDM (dense wavelength division multiplexing), 22–23
Dynamic ARP Inspection (DAI), 228
Dynamic Multipoint VPN (DMVPN), 127–128
Dynamic Trunking Protocol (DTP), 225–226

E

East-West traffic, 325, 330
eBGP (external BGP), 138–139
  configuring, 142–144
  verifying configurations, 145–147
ECN (Extended Congestion Notification), 293
editing, extended IPv4 ACLs, 182–183
EF (expedited forwarding), 293
EGP (Exterior Gateway Protocols), 137–138
egress traffic, SPAN (Switched Port Analyzer), 258
EIA (Electronic Industries Alliance), 13
encapsulation errors, 391
encryption and tunneling protocols, troubleshooting, 397
end users, questioning, 364–365
end-system configuration files, documentation, 351–352
end-system documentation, 352
end-to-end cable topology, 105–106
end-to-end connectivity, troubleshooting, 398–402
EoMPLS (Ethernet over MPLS), 30–31
error detection, PPP (Point-to-Point Protocol), configuration options, 74
Ethernet, Class of Service (CoS), markings, 291–292
Ethernet links, 404
Ethernet over MPLS (EoMPLS), 30–31
Ethernet WANs, private WAN infrastructure, 30–31
Europe, bandwidth, 54–55
evolving networks, WANs (wide area networks), 8
exceeding design limits, troubleshooting, 389
excessive broadcasts, troubleshooting, 391
expedited forwarding (EF), 293
extended ACLs, decision process, 197
Extended Congestion Notification (ECN), 293
extended IPv4 ACLs, 162
  applying to interfaces, 177–178
  configuring, 175–177
  editing, 182–183
  filtering, traffic, 178–180
  placement of, 163, 166–167
  structure of, 173–175
  verifying, 181–182

extended named ACLs, creating, 180–181
Exterior Gateway Protocols. *See* EGP (Exterior Gateway Protocols)
external BGP. *See* eBGP (external BGP)

F

FCS (Frame Check Sequence), 67
FIB (Forwarding Information Base), 327
fiber, 106
FIFO (First-In First-Out), 279–280
filtering (extended IPv4 ACLs)
  ports, 173–175
  services, 173–175
  traffic, 178–180
First-In First Out (FIFO), 279–280
flow tables, 332
fog computing model, 308–310
fog computing pillar, Cisco IoT System, 308–310
Forwarding Information Base (FIB), 327
forwarding plane, 326
frame fields, PPP (Point-to-Point Protocol), 67
Frame Relay, 18–19, 57
  private WAN infrastructure, 28–29
framing errors, 391
frequency command, 374, 375
full mesh topology, WANs (wide area networks), 6–7

G

gathering symptoms, troubleshooting process, 362–364
Generic Routing Encapsulation (GRE). *See* GRE (Generic Routing Encapsulation)
get-bulk-request, SNMP (Simple Network Management Protocol), 236
get-next-request, SNMP (Simple Network Management Protocol), 236
get-request, SNMP (Simple Network Management Protocol), 236
get-response, SNMP (Simple Network Management Protocol), 236
global enterprise networks, connecting, 13
GRE (Generic Routing Encapsulation), 103, 128, 129–130
  characteristics of, 130
  configuration command syntax, 132
  configuring, 131–133
  troubleshooting, 134–136
  tunnel configuration topology, 131
  verifying configurations, 133–134
group tables, 332

H

hard QoS, 285
hardware troubleshooting tools, 380–385
HDLC, 56
HDLC (High-Level Data Link Control). *See* HDLC
HDLC encapsulation, 57–58
  configuring, 58
  troubleshooting, serial interfaces, 59–63
  WAN encapsulation protocols, 56–57
headend, 105
HFC (hybrid fiber-coaxial) networks, 104
high CPU utilization rates, 388
High-Level Data Link Control. *See* HDLC
hub-and-spoke topology, WANs (wide area networks), 6
hybrid clouds, 316
hybrid fiber-coaxial (HFC) networks, 104
hypervisors, 319
  installing VMs on, 324
  Type 1 hypervisors, 323
  Type 2 hypervisors, 321–323

I

IaaS (infrastructure as a service), 315
iBGP (internal BGP), 138–139
icmp-echo command, 375
ICMPv6 Neighbor Advertisment (NA), 185
ICMPv6 Neighbor Discovery (ND), 185
ICMPv6 Neighbor Solicitation (NS), 185
IEEE (Institute of Electrical and Electronics Engineers), 13
IEEE 802.1X, secure device access, 233–234
IEEE 802.3ab Gigabit Ethernet, 404
IGP (Interior Gateway Protocols), 137–138
inbound ACL logic, ACLs (access control lists), 194
infrastructure as a service (IaaS), 315
ingress traffic, SPAN (Switched Port Analyzer), 258
input errors, 404

input queue drops, 403
installing VMs (virtual machines) on hypervisors, 324
Institute of Electrical and Electronics Engineers (IEEE), 13
Integrated Services Digital Network (ISDN), 18
integrated services (IntServ), 284, 285–286
interface configuration errors, troubleshooting, 389
interfaces, ACLs (access control lists), 158–159
  extended IPv4 ACLs, 177–178
    IPv6 ACLs, 189–190
Interior Gateway Protocols. *See* IGP (Interior Gateway Protocols)
internal BGP (iBGP), 138–139
International Organization for Standardization (ISO), 13
Internet layer, TCP/IP, 367
Internet of Things. *See* IoT (Internet of Things)
Internet Protocol Security. *See* IPsec (Internet Protocol Security)
intrusion prevention system. *See* IPS (intrusion prevention system)
IntServ (integrated services), 284, 285–286
IoT (Internet of Things), 305–306
  pillars of Cisco IoT System, 307
    application enablement platform pillar, 313–314
    data analytics pillar, 312
    fog computing pillar, 308–310
    management and automation pillar, 313
    network connectivity pillar, 308
    security pillar, 311–312
IoT Network security, 311
IoT Physical security, 312
ip access-list [standard | extended] global configuration command, 170
IP connectivity, troubleshooting. *See* troubleshooting IP connectivity
ip host, 422
ip neigh show command, 408
IP Precedence (IPP) field, 293
IP SLA ICMP echo operation, 373
IP SLA operations
  creating, 374
  scheduling, 374
ip sla schedule command, 375
IP SLA (service-level agreement), troubleshooting, 372–373
    configurations, 373–375
    verifying configurations, 376–377
IP Source Guard (IPSG), 228
ip tcp adjust-mss interface configuration command, 122
ipconfig command, 413, 414
IPCP (Internet Protocol Control Protocol), NCPs (Network Control Protocols), PPP (Point-to-Point Protocol), 72–73
IPP (IP Precedence) field, 293
IPS (intrusion prevention system), 217, 257
IPsec (Internet Protocol Security), 103
IPSG (IP Source Guard), 228
IPv4 ACEs, 156
IPv4 ACLs, 162
  troubleshooting, 197–201
IPv4 ARP table, troubleshooting, 406–407
IPv4-Address, IPCP, 73
IPv6 ACLs, 184–185
  applying to interfaces, 189–190
  configuring, 188–189
  deny FTP, 190
  processing packets, 194–197
  restricted access, 190–191
  troubleshooting, 201–207
  verifying, 192–193
  verifying default gateway, 413–415
ipv6 host, 422
IPv6 Neighbor Discovery, 185
IPv6 neighbor table, troubleshooting, 407–408
IPv6 topology, configuring, 186–188
ipv6 unicast-routing, 414
ISDN (Integrated Services Digital Network), 18
  private WAN infrastructure, 26–28
ISDN BRI, 27
ISDN PRI, 28
ISDN tariffs, 28
ISO (International Organization of Standardization), 13
isolating issues using layered models, 365–367
  bottom-up troubleshooting method, 368
  divide-and-conquer method, 369–370
  top-down troubleshooting method, 368–369
ISP routes, BGP (Border Gateway Protocol), 141–142
ITaaS (IT as a service), 315

J

jitter, 19, 274–275
network transmission quality, 272–273

K

keywords
description, 169
log, 396
knowledge bases, 378

L

labs
Configure a Branch Connection, 148
Configure and Verify eBGP, 147
Configure IP SLA ICMP Echo, 377
Configuring a Point-to-Point GRE VPN Tunnel, 136
Configuring a Router as a PPPoE Client for DSL Connectivity, 122
Configuring and Verifying Extended ACLs, 184
Configuring and Verifying IPv6 ACLs, 193
Configuring Basic PPP with Authentication, 89
Configuring SNMP, 255
Implement a Local Span, 262
Researching Broadband Internet Access Technologies, 113
Researching Network Monitoring Software, 248
Troubleshoot PPPoE, 122
Troubleshooting ACL Configuration and Placement, 207
Troubleshooting Basic PPP with Authentication, 95
LAN security
best practices
mitigating DHCP attacks, 230–231
mitigating MAC address flooding table attacks, 228–229
mitigating VLAN attacks, 229–230
secure administrative access with AAA, 231–233
secure device access with 802.1X, 233–234
securing the LAN, 227–228
CDP reconnaissance attacks, 219–220
common attacks, 218–219
DHCP attacks, 226–227
MAC address table flooding attack, 222–224
Telnet attacks, 220–222
VLAN attacks, 225–226
latency, 19
Layer 1 protocols, OSI model, WANs (wide area networks), 13
Layer 2, marking, QoS (quality of service), 291–292
Layer 2 LANs, common attacks, 218–219
Layer 2 protocols, OSI model, WANs (wide area networks), 14
Layer 3, marking, QoS (quality of service), 292–295
layered architecture, PPP (Point-to-Point Protocol), 65–66
layered models
isolating issues, 365–367
troubleshooting methods
bottom-up troubleshooting method, 368
divide-and-conquer method, 369–370
top-down troubleshooting method, 368–369
LCP (Link Control Protocol), 64
PPP (Point-to-Point Protocol), 66
LCP (Link Control Protocol) operations, PPP (Point-to-Point Protocol), 69–71
leaf switches, 334
leased lines, private WAN infrastructure, 23–25
leased-line connections, 52
LEDs (light-emitting diodes), 22
limitations, of WFQ (Weighted Fair Queuing), 281
Link Control Protocol (LCP). ***See*** **LCP (Link Control Protocol)**
link establishment, LCP operation, PPP (Point-to-Point Protocol), 69–70
Link Layer Discovery Protocol. ***See*** **LLDP (Link Layer Discovery Protocol)**
link maintenance, LCP operation, PPP (Point-to-Point Protocol), 70–71
link quality monitoring command, PPP (Point-to-Point Protocol), 77–78
link termination, LCP operation, PPP (Point-to-Point Protocol), 71
LLDP (Link Layer Discovery Protocol), 220
LLQ (Low Latency Queuing), 282–283
local AAA authentication, 232
local loops, 15
local SPAN, 257–259
configuring, 260–261
verifying, 261

log keyword, 396
logging trap, 387
logical topology diagrams, documentation, 353–354
long-term evolution (LTE), 38, 111
LophtCrack, 221
loss of connectivity, 388
Low Latency Queuing (LLQ), 282–283
LTE (long-term evolution), 38, 111

M

M2M (Machine-to-Machine), 306
MAC address table flooding attack, 222–224
  mitigating, 228–229
Machine-to-Machine (M2M), 306
management and automation pillar, Cisco IoT System, 313
management information base. *See* MIB (management information base)
management plane, 326
marking
  Layer 2, QoS (quality of service), 291–292
  Layer 3, QoS (quality of service), 292–295
  QoS (quality of service), 290–291
mask network-mask command, 144
maximum segment size. *See* MSS (maximum segment size)
maximum transmission unit. *See* MTU (maximum transmission unit)
measuring, data, network documentation, 358–360
meter tables, 332
MetroE (Metropolitan Ethernet), 30–31
mGRE (Multipoint Generic Routing Encapsulation), 128
MIB (management information base), OIDs (object IDs), 243–246
MIB (management information base) variables
  community strings, 241
  SNMP (Simple Network Management Protocol), 236–237
mitigating
  DHCP attacks, 230–231
  MAC address table flooding attack, 228–229
  VLAN attacks, 229–230
mobile connections, 110–111, 112
models
  best-effort model, 284
  cloud models, 315–316
  DiffServ (differentiated services), 286–288
  IntServ (integrated services), 285–286
  layered models, isolating issues, 365–367
  OSI reference model, troubleshooting, 365–366
  QoS models, selecting, 283
  TCP/IP model, troubleshooting, 366–367
modems
  broadband modems, 16
  dialup modems, 16
monitor session command, 260
monitor session global configuration command, 260
monitoring, 217
MPLS (Multiprotocol Label Switching), private WAN infrastructure, 32
MPPP (multilink PPP), 78–80
  disabling, 80
MSS (maximum segment size), 120
MTU (maximum transmission unit), 116
  PPPoE (Point-to-Point Protocol over Ethernet), 120–122
multilayer switches, 17
multilink PPP, 74
  commands, 78–80
Multipoint Generic Routing Encapsulation (mGRE), 128
Multiprotocol Label Switching. *See* MPLS (Multiprotocol Label Switching)
municipal Wi-Fi, 36, 109–110

N

NA (Neighbor Advertisement), 185
named ACLs, 170–171
named IPv4 ACLs, 163
name-to-IPv4 mapping, 422
NAT (Network Address Translation) for IPv4, transport layer troubleshooting, 396–397
NBAR (Network Based Application Recognition), 290
NBMA (nonbroadcast multi-access), 28
NCPs (Network Control Protocols), 64
  PPP (Point-to-Point Protocol), 66–67, 72–73
ND (Neighbor Discovery), 185
negotiation, PPPoE (Point-to-Point Protocol over Ethernet), 118–119

Neighbor Advertisement (NA), 185
neighbor command, 144
neighbor issues, troubleshooting, 393
Neighbor Solicitation (NS), 185
netsh interface ipv6 show neighbor, 407
network access layer, TCP/IP, 367
network analysis module, 384–385
Network Based Application Recognition (NBAR), 290
network bottlenecks, 388
network command, 144
network configuration files, documentation, 350–351
network congestion, 272–273
network connectivity pillar, Cisco IoT System, 308
Network Control Protocols. *See* NCPs (Network Control Protocols)
network documentation, 349–350
end-system configuration files, 351–352
establishing a network baseline, 355–357
measuring data, 358–360
network configuration files, 350–351
network topology diagrams, 352–354
network failure, 392
network layer troubleshooting, 392–393
network management system (NMS), 235
network management system (NMS) tools, 377–378
network programming
controllers
ACI (Application Centric Infrastructure), 332
SDN controllers and operations, 331–332
software-defined networking
architecture, 329–330
control plane and data plane, 326–328
network virtualization, 327–329
network topology diagrams, documentation, 352–354
network traffic trends, traffic characteristics, 275–276
network transmission quality
bandwidth, 272–273
congestion, 272–273
delays, 272–273
jitter, 272–273
packet loss, 273–274
prioritizing traffic, 271–272
network troubleshooting
application layer troubleshooting, 397–398
network layer troubleshooting, 392–393
physical layer troubleshooting, 387–390
transport layer troubleshooting
ACLs (access control lists), 394–396
NAT (Network Address Translation) for IPv4, 396–397
network virtualization, 324–325, 327–329
networking models
client/server model, 308–309
cloud computing model, 308–309
fog computing model, 308–310
networks
branch networks, 10–11
campus networks, 9–10
circuit switched networks, 17–18
distributed networks, 11–12
global enterprise networks, 13
PSN (packet-switched network), 18–19
small offices, 8–9
transportation network, 105
WANs (wide area networks). *See* WANs (wide area networks)
Next Hop Clients (NHCs), 127
Next Hop Resolution Protocol (NHRP), 127
Next Hop Server (NHS), 127
NHCs (Next Hop Clients), 127
NHRP (Next Hop Resolution Protocol), 127
NHS (Next Hop Server), 127
NMS (network management system), 235, 237
NMS (network management system) tools, 377–378
no cdp enable interface configuration command, 220
no cdp run global configuration mode command, 220
no ip access-group command, 170
no ip sla schedule, 375
no lldp receive, 220
no lldp run, 220
no lldp transmit, 220
no ppp multilink command, 80
NO_ACCESS statements, ACLs (access control lists), 172
nodes, 106
noise, troubleshooting, 389
nonbroadcast multi-access (NBMA), 28
North America, bandwidth, 54–55
North-South traffic, 330
NS (Neighbor Solicitation), 185
nslookup, 422, 423
numbered IPv4 ACL, 163

O

object IDs (OIDs), MIB (management information base), 243–246
OC transmission rates, 55
OIDs (object IDs), MIB (management information base), 243–246
OpenFlow, 328
OpenFlow switches, 331
OpenStack, 328
operational technology (OT), 311
operations
- SNMP (Simple Network Management Protocol), 236–237
- WANs (wide area networks), OSI model, 13–14

optical time-domain reflectometers (OTDRs), 381–382
OptiView XG Network Analysis Tablet, 384
OSI model
- PPP (Point-to-Point Protocol), 65
- WANs (wide area networks), 13–14

OSI reference model, troubleshooting, 365–366
OT (operational technology), 311
OTDRs (optical time-domain reflectometers), 381–382
outbound ACL logic, ACLs (access control lists), 195
output errors, 404
output queue drops, 403

P

PaaS (platform as a service), 315
packet analyzers, 256, 257
packet filtering, 208
- ACLs (access control lists), 160–161

packet loss
- avoiding, 288–289
- network transmission quality, 273–274

packet switching, WANs (wide area networks), 18–19
packet tracers
- CCNA Skills Integration Challenge, 425
- Configure and Verify eBGP, 147
- Configure Standard IPv4 ACLs, 172
- Configuring Extended ACLs - Scenario 1, 184
- Configuring Extended ACLs - Scenario 2, 184
- Configuring Extended ACLs - Scenario 3, 184
- Configuring GRE, 136
- Configuring IPv6 ACLs, 193
- Configuring PAP and CHAP Authentication, 89
- Skills Integration Challenge, 96, 148
- Troubleshooting Challenge: Documenting the Network, 360
- Troubleshooting Challenge: Using Documentation to Solve Issues, 424
- Troubleshooting Enterprise Networks 1, 423
- Troubleshooting Enterprise Networks 2, 423
- Troubleshooting Enterprise Networks 3, 423–424
- Troubleshooting GRE, 136
- Troubleshooting IPv4 ACLs, 206
- Troubleshooting IPv6 ACLs, 206
- Troubleshooting PPP with Authentication, 94–95
- troubleshooting serial interfaces, 63

packetization delay, 273
packet-switched network (PSN), 18–19
PAP (Password Authentication Protocol), 83–85
PAP authentication, configuring, 87–88
parallel ports, 52–53
passenger protocol, GRE (Generic Routing Encapsulation), 129
Password Authentication Protocol. *See* PAP (Password Authentication Protocol)
passwords, plaintext passwords, 243
performance lower than baseline, 388
permanent virtual circuits (PVCs), 28
permit and deny command syntax, IPv6 ACLs, 188–189
physical layer
- OSI model, WANs (wide area networks), 13
- verifying, IP connectivity, 402–404

physical topology diagrams, documentation, 352–353
pillars of Cisco IoT System, 307
- application enablement platform pillar, 313–314
- data analytics pillar, 312
- fog computing pillar, 308–310
- management and automation pillar, 313
- network connectivity pillar, 308
- security pillar, 311–312

ping, 363, 400, 401
placement of, ACLs (access control lists), 163–164
Plain Old Telephone System (POTS), 107
plaintext passwords, 243

platform as a service (PaaS), 315
point of presence (POP), 34
point-to-point communication links, 53–54
point-to-point connections, 52
Point-to-Point Protocol. *See* PPP
point-to-point serial communication, 52–53
point-to-point topology, WANs (wide area networks), 5
policing traffic, 297–298
policy-based SDN, 335–336
POP (point of presence), 34
port mirroring, SPAN (Switched Port Analyzer), 256
port numbers, TCP, 160
portable network analyzers, 384
ports
- filtering, extended IPv4 ACLs, 173–175
- trusted DHCP ports, 230
- untrusted ports, 230

POTS (Plain Old Telephone System), 107
power-related issues, troubleshooting, 389
PPP (Point-to-Point Protocol), 57, 64–65
- advantages of, 65
- configuration options, 72
- configuring
  - *basic configuration commands, 76*
  - *compression commands, 76–77*
  - *configuration options, 74–75*
  - *link quality monitoring command, 77–78*
  - *multilink PPP commands, 78–80*
- debugging, 88–93
- frame fields, 67
- layered architecture, 65–66
- LCP (Link Control Protocol), 66
- NCPs (Network Control Protocols), 66–67
- sessions
  - *establishing, 68–69*
  - *LCP operation, 69–71*
  - *NCPs (Network Control Protocols), 72–73*
- synchronous PPP, 97
- verification commands, 82
- verifying configurations, 81–82, 116–118

PPP authentication
- configuring, 87–89
  - *CHAP (Challenge Handshake Authentication Protocol), 85–86*
  - *PAP (Password Authentication Protocol), 83–85*
  - *ppp authentication command, 86–87*
  - *PPP authentication protocols, 83*
- troubleshooting, 94–95

ppp authentication command, 86–87
PPP authentication protocols, 83
PPP callback, 74
PPP multilink, verifying configurations, 82
PPP multilink commands, 78–80
PPP over Ethernet. *See* PPPoE (Point-to-Point Protocol over Ethernet)
ppp quality percentage command, 77
PPP serial encapsulation, troubleshooting, 90–91
PPP tunnels, creating, 116
PPPoE (Point-to-Point Protocol over Ethernet), 103, 113–115
- authentication, 119–120
- configuring, 115–116
- MTU (maximum transmission unit) size, 120–122
- negotiation, 118–119
- troubleshooting, 118

pppoe enable interface configuration command, 116
PQ (priority queuing), 282
PRI (Primary Rate Interface), 27
Primary Rate Interface. *See* PRI (Primary Rate Interface)
prioritizing, traffic, network transmission quality, 271–272
Priority (PRI) field, 291
priority queuing (PQ), 282
private clouds, 316
private communication channel, 103
private WAN infrastructure, 21
- ATM (Asynchronous Transfer Mode), 29–30
- dialup, 25–26
- Ethernet WANs, 30–31
- Frame Relay, 28–29
- ISDN (Integrated Services Digital Network), 26–28
- leased lines, 23–25
- MPLS (Multiprotocol Label Switching), 32
- VSAT (very small aperture terminal), 32–33

processing packets, IPv6 ACLs, 194–197
propagation delay, 273
protocol analyzers, 379–380
protocol field names, NCPs (Network Control Protocols), PPP (Point-to-Point Protocol), 66–67

protocols
- ARP (Address Resolution Protocol), 127
- BGP (Border Gateway Protocol). *See* BGP (Border Gateway Protocol)
- CDP (Cisco Discovery Protocol), 219–220
- CHAP (Challenge Handshake Authentication Protocol), 85–86
- DHCP (Dynamic Host Configuration Protocol), 396
- eBGP (external BGP), 138–139
- EGP (Exterior Gateway Protocols), 137–138
- external BGP. *See* eBGP (external BGP)
- Interior Gateway Protocols. *See* IGP (Interior Gateway Protocols)
- internal BGP (iBGP), 138–139
- IPCP (Internet Protocol Control Protocol), 72–73
- LCP (Link Control Protocol), 64
- LLDP (Link Layer Discovery Protocol), 220
- NCPs (Network Control Protocols), 64
- NHRP (Next Hop Resolution Protocol), 127
- PAP (Password Authentication Protocol), 83–85
- PPP. *See* PPP (Point-to-Point Protocol)
- PPPoE. *See* PPPoE (Point-to-Point Protocol over Ethernet)
- RSTP (Real-Time Streaming Protocol), 277
- RSVP (Resource Reservation Protocol), 285–286
- RTP (Real-Time Protocol), 274
- SNMP. *See* SNMP (Simple Network Management Protocol)
- WAN encapsulation protocols, 56–57

PSN (packet-switched network), 18–19

PSTN (public switched telephone network), 18

public clouds, 315

public switched telephone network (PSTN), 18

public WAN infrastructure, 21
- 3G/4G cellular, 37–38
- cable, 35
- DSL (digital subscriber line), 34
- VPNs (virtual private networks), 38–40
- wireless, 36–37

PVCs (permanent virtual circuits), 28

Q

QoS (quality of service)
- avoiding packet loss, 288–289
- classification and marking, 290–291
- congestion avoidance, 296–297
- DiffServ (differentiated services), 286–288
- marking at Layer 2, 291–292
- marking at Layer 3, 292–295
- network transmission quality
  - *bandwidth, 272–273*
  - *congestion, 272–273*
  - *delays, 272–273*
  - *jitter, 272–273*
  - *packet loss, 273–274*
  - *prioritizing traffic, 271–272*
- QoS models
  - *best-effort model, 284*
  - *DiffServ (differentiated services), 286–288*
  - *integrated services (IntServ), 285–286*
  - *selecting QoS policy models, 283*
- queuing algorithms, 278–279
  - *CBWFQ (Class-Based Weighted Fair Queuing), 281–282*
  - *FIFO (First-In First-Out), 279–280*
  - *LLQ (Low Latency Queuing), 282–283*
  - *WFQ (Weighted Fair Queuing), 280–281*
- shaping and policing traffic, 297–298
- tools, 289–290
- traffic characteristics
  - *data traffic, 277–278*
  - *network traffic trends, 275–276*
  - *video traffic, 276–277*
  - *voice traffic, 276*
- trust boundaries, 295–296

QoS models
- best-effort model, 284
- DiffServ (differentiated services), 286–288
- integrated services (IntServ), 285–286
- selecting QoS policy models, 283

QoS policy models, selecting, 283

questioning end users, 364–365

queuing algorithms, 278–279
- CBWFQ (Class-Based Weighted Fair Queuing), 281–282
- FIFO (First-In First-Out), 279–280
- LLQ (Low Latency Queuing), 282–283
- WFQ (Weighted Fair Queuing), 280–281

queuing delay, 273

queuing packets, 271–272

R

radio frequency (RF), 104
read-only (ro), community strings, 241
read-write (rw), SNMP (Simple Network Management Protocol), 241
Real-Time Protocol (RTP), 274
Real-Time Streaming Protocol (RSTP), 277
remote SPAN (RSPAN), 259–260
remote-access connections, broadband connections
  cable system, 104–106
  DSL (digital subscriber line), 107–108
  wireless, 109–112
remote-access VPNs, 39–40, 126
removing. *See* deleting
Resource Reservation Protocol (RSVP), 285–286
restricted access, IPv6 ACLs, 190–191
RF (radio frequency), 104
ro (read-only), community strings, 241
route print, 412
router bgp command, 144
router documentation, 350
routers, 17
routing tables, troubleshooting, 393
RSPAN (remote SPAN), 259–260
RSPAN destination session, 259
RSPAN source session, 259
RSPAN VLAN, 259
RSTP (Real-Time Streaming Protocol), 277
RSVP (Resource Reservation Protocol), 285–286
RTP (Real-Time Protocol), 274
rw (read-write), SNMP (Simple Network Management Protocol), 241

S

SaaS (software as a service), 315
satellite Internet, 36, 111–112
scheduling, IP SLA operations, 374
SDH (Synchronous Digital Hierarchy), 22
SDLC (Synchronous Data Link Control), 57
SDN (software-defined networking), 328
  APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 336–337
  architecture, 329–330
  control plane and data plane, 326–328
  controller-based SDN, 335
  device-based SDN, 334–335
  network virtualization, 327–329
  policy-based SDN, 335–336
  SDN types, 334–336
SDN controllers, 329–330, 331–332
SDN operations, 331–332
SDSL (symmetric DSL), 107
secure administrative access with AAA, 231–233
secure device access, 802.1X, 233–234
securing the LAN, 227–228
security, 217
  LAN security. *See* LAN security
  SNMP. *See* SNMP (Simple Network Management Protocol)
  SPAN. *See* SPAN (Switched Port Analyzer)
  VPNs (virtual private networks), 103
security models, SNMP (Simple Network Management Protocol), 240
security pillar, Cisco IoT System, 311–312
sequence numbers, editing, extended ACLs, 182
serial bandwidth, 54–56
serial communications
  point-to-point communication links, 53–54
  serial and parallel ports, 52–53
  serial bandwidth, 54–56
serial connections, 52
serial interfaces
  troubleshooting, HDLC encapsulation, 59–63
  verifying, 59
Serial Line Internet Protocol (SLIP), 57
serial point-to-point, serial communications
  point-to-point communication links, 53–54
  serial and parallel ports, 52–53
  serial bandwidth, 54–56
serial ports, 52–53
serial PPP encapsulation configuration, verifying, 81
serialization delay, 273
server virtualization, 319–320
server-based AAA authentication, 232
servers, access servers, 16
service provider network infrastructure, WANs (wide area networks), 21–23
services
  filtering, extended IPv4 ACLs, 173–175
  WANs (wide area networks)
    choosing WAN link connections, 40–42

service provider network infrastructure, 21–23
WAN link connection options, 20–21
sessions, PPP (Point-to-Point Protocol)
establishing, 68–69
LCP operation, 69–71
NCPs (Network Control Protocols), 72–73
set-request, SNMP (Simple Network Management Protocol), 236
shaping, traffic, 297–298
show access-list privileged EXEC command, 168
show access-lists command, 172, 181–182, 183
show arp, 359
show cdp neighbors detail, 359
show controllers cbus command, 63
show controllers command, 62
show interface, 359
show interface dialer command, 117
show interface tunnel, 133
show interfaces, 402
show interfaces command, 82
show interfaces fa 0/20, 405
show interfaces serial command, 60, 82
show ip access-lists, 420
show ip cache flow, 359
show ip interface [brief]359
show ip interface brief, 133, 358, 363
show ip interface go/o command, 182
show ip interfaces, 420
show ip interfaces serial 0/0/1, 421
show ip ospf neighbor command, 135
show ip route, 135, 359, 364, 412, 415
show ip route command, 418
show ip sla application privileged EXEC mode command, 373
show ip sla configuration, 376
show ip sla statistics, 376
show ipv6 access-list, 420
show ipv6 interface [brief]359
show ipv6 interface brief, 358, 363
show ipv6 interface GigabitEthernet o/o, 413–414
show ipv6 interfaces, 420
show ipv6 neighbors, 408
show ipv6 route, 359, 364, 416
show mac address-table command, 408
show memory, 402
show monitor command, 261
show neighbors, 359
show port, 359
show ppp multilink command, 82
show pppoe session command, 118
show processes cpu, 402
show protocols, 364
show running-config, 359, 364, 422
show snmp command, 250, 252
show snmp community command, 252
show snmp output command, 250
show snmp privileged EXEC mode command, 250
show tech-support, 359
show version, 359
show vlan, 359, 409
Simple Network Management Protocol. *See* SNMP (Simple Network Management Protocol)
single-homed, BGP (Border Gateway Protocol), 140
site-to-site VPNs, 38–39, 125–126
SLIP (Serial Line Internet Protocol), 57
small office/home office. *See* SOHO (small office/home office)
small offices, WANs (wide area networks), 8–9
SNMP (Simple Network Management Protocol), 235–236
agent traps, 237–238
best practices, 252–253
community strings, 241–243
configuring, 248–249
SNMPv3, 254
SNMPv3, verifying configuration, 254–255
MIB (management information base), OIDs (object IDs), 243–246
operations, 236–237
transport layer troubleshooting, 397
verifying, configurations, 249–252
versions of, 238–240
SNMP agents, 235–236
SNMP Graphing tool, 245
SNMP manager, 235
SNMP polling, 237
SNMP traps, 386
snmp_server enable traps ? command, 249–250
snmpget utility, 244–245
snmp-server enable traps command, 249
SNMPv1, 238
SNMPv2, 239

SNMPv3, 239, 246–247, 253
configuring, 254
verifying configurations, 254–255
soft QoS, 287
software as a service (SaaS), 315
software troubleshooting tools, 377
baselining tools, 379
knowledge bases, 378
NMS (network management system) tools, 377–378
software-defined networking (SDN), 328
APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 336–337
architecture, 329–330
control plane and data plane, 326–328
controller-based SDN, 335
device-based SDN, 334–335
network virtualization, 327–329
policy-based SDN, 335–336
SDN types, 334–336
SOHO (small office/home office), 104
SONET (Synchronous Optical Networking), 22, 96
Source (SPAN) port, 258
source VLAN, SPAN (Switched Port Analyzer), 258
SPAN (Switched Port Analyzer), 217
analyzing suspicious traffic, 257
local SPAN, 257–259
configuring, 260–261
verifying, 261
port mirroring, 256
remote SPAN (RSPAN), 259–260
troubleshooting, 262–263
SPAN Engineering, 8
branch networks, 10–11
campus networks, 9–10
distributed networks, 11–12
small offices, 8–9
SPAN session, 258
Spanning Tree Protocol (STP), 391–392
spine-leaf topology, 333–334
standard ACLs, decision process, 196–197
standard IPv4 ACLs, 162
applying, 169–170
configuring, 167–169
placement of, 163–165
standard named IPv4 ACLs, 170–171
STP (Spanning Tree Protocol), 391–392
STP failures or loops, 391–392
suboptimal performance, 393
subscriber drop, 105
supplicant, 234
switch documentation, 351
switch MAC address table, troubleshooting, 408–409
switch spoofing attack, 225
Switched Port Analyzer. *See* SPAN (Switched Port Analyzer)
switches, Cisco Nexus 9000 Series switches, 333
symmetric DSL (SDSL), 107
Synchronous Data Link Control (SDLC), 57
Synchronous Digital Hierarchy (SDH), 22
Synchronous Optical Networking (SONET), 22
synchronous PPP, 97
syslog server, 386
troubleshooting, 385–387

T

Tag Control Information (TCI), 291
tail drop, 282
TCI (Tag Control Information), 291
TCP conversations, ACLs (access control lists), 159–160
TCP MSS, PPPoE (Point-to-Point Protocol over Ethernet), 122
TCP/IP application layer protocols, 397
TCP/IP model, troubleshooting, 366–367
TDM (time-division multiplexed, 26
TDRs (time-domain reflectometers), 381–382
Telecommunications Industry Association (TIA), 13
teleworking, 12, 103
Telnet, verifying transport layer, 418–420
telnet, 363
Telnet attacks, LAN security, 220–222
Telnet DoS attack, 221
terminal lines, 386
terminology, WANs (wide area networks), 14–16
text editor, editing, extended ACLs, 182
TIA (Telecommunications Industry Association), 13
time-division multiplexed (TDM), 26
time-domain reflectometers (TDRs), 381–382
TLS (Transport Layer Security), 331
toll network, 16

tools
QoS (quality of service), 289–290
troubleshooting tools. *See* troubleshooting tools,
software troubleshooting tools, 377–379
top-down troubleshooting method, 368–369
topologies, WANs (wide area networks), 5
dual-homed topology, 6–7
full mesh topology, 6–7
hub-and-spoke topology, 6
point-to-point topology, 5
topology database, troubleshooting, 393
ToS (Type of Service), 292
traceroute, 363, 401–402
traffic
filtering with extended ACLs, 178–180
policing, 297–298
prioritizing, network transmission quality, 271–272
shaping, 297–298
UDP-based traffic, 296–297
traffic characteristics
data traffic, 277–278
network traffic trends, 275–276
video traffic, 276–277
voice traffic, 276
traffic marking, QoS (quality of service), 290
transport layer, verifying, 418–420
Transport Layer Security (TLS), 331
transport layer troubleshooting
ACLs (access control lists), 394–396
NAT (Network Address Translation) for IPv4, 396–397
transport layers, TCP/IP, 367
transport protocol, GRE (Generic Routing Encapsulation), 129
transportation network, 105
troubleshooting
ACLs (access control lists), processing packets, 194–197
application layer troubleshooting, 397–398
data link layer troubleshooting, 390–392
GRE (Generic Routing Encapsulation), 134–136
IP SLA (service-level agreement)
configurations, 373–375
verifying configurations, 376–377
IPv4 ACLs, 197–201
IPv6 ACLs, 201–207
isolating issues using layered models, 365–367
bottom-up troubleshooting method, 368
divide-and-conquer method, 369–370
top-down troubleshooting method, 368–369
troubleshooting methods, 371–372
network documentation
documenting the network, 349–352
establishing a network baseline, 355–357
measuring data, 358–360
network topology diagrams, 352–354
network layer troubleshooting, 392–393
physical layer troubleshooting, 387–390
PPP authentication, 94–95
PPP serial encapsulation, 90–91
PPPoE (Point-to-Point Protocol over Ethernet), 118
serial interfaces, HDLC encapsulation, 59–63
SPAN (Switched Port Analyzer), 262–263
transport layer troubleshooting
ACLs (access control lists), 394–396
NAT (Network Address Translation) for IPv4, 396–397
troubleshooting decision tree, 418
troubleshooting IP connectivity
checking for duplex mismatches, 404–406
end-to-end connectivity, 398–402
verifying ACLs, 420–422
verifying correct path, 415–418
verifying default gateway, 411–415
verifying DNS, 422–423
verifying Layer 2 and Layer 3 addressing on local network, 406–411
verifying physical layer, 402–404
verifying transport layer, 418–420
troubleshooting methods, 368–371
guidelines for, 371–372
troubleshooting policies, 362
troubleshooting process
gathering symptoms, 362–364
general procedures, 360–362
questioning end users, 364–365
troubleshooting scenarios, IP SLA (service-level agreement), 372–373
troubleshooting tools
hardware troubleshooting tools, 380–385
protocol analyzers, 379–380
software troubleshooting tools, 377

baselining tools, 379
knowledge bases, 378
NMS (network management system) tools, 377–378
syslog server, 385–387
trust boundaries, QoS (quality of service), 295–296
trusted DHCP ports, 230
tunneling and encryption protocols, troubleshooting, 397
tunnels, 103
Type 1 hypervisors, 323
Type 2 hypervisors, 321–323
Type of Service (ToS), 292

U

UCS (Unified Computing System), 324–325
UDP-based traffic, 296–297
untrusted ports, 230

V

variables, MIB variables
community strings, 241
SNMP (Simple Network Management Protocol), 236–237
verification commands
BGP (Border Gateway Protocol), 145
PPP (Point-to-Point Protocol), 82
verifying
ACLs (access control lists), 171–172, 420–422
controller settings, 63
correct path, troubleshooting, 415–418
default gateway, troubleshooting, 411–415
DNS, 422–423
extended IPv4 ACLs, 181–182
GRE (Generic Routing Encapsulation) configurations, 133–134
IP SLA (service-level agreement) configurations, 376–377
IPv6 ACLs, 192–193
local SPAN, 261
physical layer, IP connectivity, 402–404
PPP (Point-to-Point Protocol) configuration, 81–82
PPPoE (Point-to-Point Protocol over Ethernet) configurations, 116–118
serial interfaces, 59
SNMP (Simple Network Management Protocol) configurations, 249–252
SNMPv3, configurations, 254–255
transport layer, 418–420
versions of SNMP (Simple Network Management Protocol), 238–240
very small aperture terminal. ***See*** **VSAT (very small aperture terminal)**
video traffic, 276–277
virtual LANs (VLANs), 325
virtual network infrastructure
installing VMs on hypervisors, 324
network virtualization, 324–325
Type 1 hypervisors, 323
Virtual Private LAN Service (VPLS), 30–31
virtual private networks. ***See*** **VPNs (virtual private networks)**
virtualization
abstraction layers, 321–322
advantages of, 320
cloud computing, 317–318
dedicated servers, 318
server virtualization, 319–320
Type 2 hypervisors, 321–323
Visual Networking Index (VNI), 275–276
VLAN assignments, troubleshooting, end-to-end connectivity, 409
VLAN attacks
LAN security, 225–226
mitigating, 229–230
VLANs (virtual LANs), 325
VMs (virtual machines), installing, on hypervisors, 324
VNI (Visual Networking Index), 275–276
voice traffic, 275, 276
VPLS (Virtual Private LAN Service), 30–31
VPN gateway, 125
VPNs (virtual private networks), 12, 103, 123–125
DMVPN (Dynamic Multipoint VPN), 127–128
public WAN infrastructure, 38–40
remote-access VPNs, 126
site-to-site VPNs, 125–126
VSAT (very small aperture terminal), private WAN infrastructure, 32–33

W

WAN access technologies, 21
WAN encapsulation protocols, 56–57
WAN link connection options, 20–21
WAN link connections, choosing, 40–42
WAN switches, 17
WANs (wide area networks), 3
- branch networks, 10–11
- campus networks, 9–10
- circuit switching, 17–18
- devices, 16–17
- distributed networks, 11–12
- evolving networks, 8
- operations, OSI model, 13–14
- packet switching, 18–19
- private WAN infrastructure
  - *ATM (Asynchronous Transfer Mode), 29–30*
  - *dialup, 25–26*
  - *Ethernet WANs, 30–31*
  - *Frame Relay, 28–29*
  - *ISDN (Integrated Services Digital Network), 26–28*
  - *leased lines, 23–25*
  - *MPLS (Multiprotocol Label Switching), 32*
  - *VSAT (very small aperture terminal), 32–33*
- public WAN infrastructure
  - *3G/4G cellular, 37–38*
  - *cable, 35*
  - *DSL (digital subscriber line), 34*
  - *VPNs (virtual private networks), 38–40*
  - *wireless, 36–37*
- purpose of, 3–5
- services
  - *choosing WAN link connections, 40–42*
  - *service provider network infrastructure, 21–23*
  - *WAN link connection options, 20–21*
- small offices, 8–9
- terminology, 14–16
- topologies, 5
  - *dual-homed topology, 6–7*
  - *full mesh topology, 6–7*
  - *hub-and-spoke topology, 6*
  - *point-to-point topology, 5*

Weighted Fair Queuing (WFQ), 280–281
Weighted Random Early Detection (WRED), 289, 296–297
WFQ (Weighted Fair Queuing), 280–281
wide-area networks. *See* WANs (wide area networks)
Wi-Fi, municipal Wi-Fi, 109–110
Wi-Fi mesh, 112
wildcard masks, ACLs (access control lists), 156–158
WiMAX (Worldwide Interoperability for Microwave Access), 36, 112
wireless, public WAN infrastructure, 36–37
wireless connections, 109
- cellular/mobile, 110–111
- municipal Wi-Fi, 109–110
- satellite Internet, 111–112

wireless Internet, 110
Wireshark Protocol Analyzer, 381
Worldwide Interoperability for Microwave Access (WiMAX), 36
WRED (Weighted Random Early Detection), 289, 296–297

X-Y-Z

X.25, 57