Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)

Copyright © 2020 Cisco Systems, Inc.

Published by:
Cisco Press
Hoboken, New Jersey

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

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020936826

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Switching, Routing, and Wireless Essentials 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.
Trademark Acknowledgments

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

Feedback Information

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

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

We greatly appreciate your assistance.
About the Contributing Authors

Bob Vachon is a professor at Cambrian College (Sudbury, Ontario, Canada) and Algonquin College (Ottawa, Ontario, Canada). He has more than 30 years of teaching experience in computer networking and information technology. He has also collaborated on many Cisco Networking Academy courses, including CCNA, CCNA Security, CCNP, and Cybersecurity as team lead, lead author, and subject matter expert. Bob enjoys family, friends, and being outdoors playing guitar by a campfire.

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 M.Ed. 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 xxvii

Chapter 1 Basic Device Configuration 1
Chapter 2 Switching Concepts 45
Chapter 3 VLANs 59
Chapter 4 Inter-VLAN Routing 97
Chapter 5 STP Concepts 137
Chapter 6 EtherChannel 175
Chapter 7 DHCPv4 199
Chapter 8 SLAAC and DHCPv6 223
Chapter 9 FHRP Concepts 261
Chapter 10 LAN Security Concepts 275
Chapter 11 Switch Security Configuration 313
Chapter 12 WLAN Concepts 347
Chapter 13 WLAN Configuration 397
Chapter 14 Routing Concepts 445
Chapter 15 IP Static Routing 495
Chapter 16 Troubleshoot Static and Default Routes 531

Appendix A Answers to the “Check Your Understanding” Questions 545
Glossary 561
Index 587
Reader Services
Contents

Introduction  xxvii

Chapter 1  Basic Device Configuration  1

Objectives  1

Key Terms  1

Introduction (1.0)  2

Configure a Switch with Initial Settings (1.1)  2

Switch Boot Sequence (1.1.1)  2
The boot system Command (1.1.2)  3
Switch LED Indicators (1.1.3)  3
Recovering from a System Crash (1.1.4)  6
Switch Management Access (1.1.5)  8
Switch SVI Configuration Example (1.1.6)  8

Configure Switch Ports (1.2)  11

Duplex Communication (1.2.1)  11
Configure Switch Ports at the Physical Layer (1.2.2)  12
Auto-MDIX (1.2.3)  13
Switch Verification Commands (1.2.4)  14
Verify Switch Port Configuration (1.2.5)  14
Network Access Layer Issues (1.2.6)  15
Interface Input and Output Errors (1.2.7)  17
Troubleshooting Network Access Layer Issues (1.2.8)  18

Secure Remote Access (1.3)  20

Telnet Operation (1.3.1)  20
SSH Operation (1.3.2)  20
Verify the Switch Supports SSH (1.3.3)  22
Configure SSH (1.3.4)  22
Verify SSH Is Operational (1.3.5)  24

Basic Router Configuration (1.4)  25

Configure Basic Router Settings (1.4.1)  26
Dual Stack Topology (1.4.3)  27
Configure Router Interfaces (1.4.4)  27
IPv4 Loopback Interfaces (1.4.6)  28
Verify Directly Connected Networks (1.5)  29
  Interface Verification Commands (1.5.1)  30
  Verify Interface Status (1.5.2)  30
  Verify IPv6 Link Local and Multicast Addresses (1.5.3)  31
  Verify Interface Configuration (1.5.4)  32
  Verify Routes (1.5.5)  32
  Filter Show Command Output (1.5.6)  34
    The section Filter  34
    The include Filter  34
    The exclude Filter  35
    The begin Filter  35
  Command History Feature (1.5.8)  36

Summary (1.6)  38
  Configure a Switch with Initial Settings  38
  Configure Switch Ports  38
  Secure Remote Access  38
  Basic Router Configuration  39
  Verify Directly Connected Networks  39

Practice  40
Check Your Understanding Questions  41

Chapter 2  Switching Concepts  45
Objectives  45
Key Terms  45

Frame Forwarding (2.1)  46
  Switching in Networking (2.1.1)  46
  The Switch MAC Address Table (2.1.2)  47
  The Switch Learn and Forward Method (2.1.3)  48
  Switching Forwarding Methods (2.1.5)  48
  Store-and-Forward Switching (2.1.6)  49
  Cut-Through Switching (2.1.7)  49

Collision and Broadcast Domains (2.2)  51
  Collision Domains (2.2.1)  51
  Broadcast Domains (2.2.2)  52
  Alleviate Network Congestion (2.2.3)  53
Chapter 3 VLANs 59
Objectives 59
Key Terms 59
Introduction (3.0) 60
Overview of VLANs (3.1) 60
VLAN Definitions (3.1.1) 60
Benefits of a VLAN Design (3.1.2) 61
Types of VLANs (3.1.3) 63
Default VLAN 63
Data VLAN 64
Native VLAN 64
Management VLAN 64
Voice VLAN 65
VLANs in a Multi-Switched Environment (3.2) 66
Defining VLAN Trunks (3.2.1) 66
Network Without VLANs (3.2.2) 67
Network with VLANs (3.2.3) 68
VLAN Identification with a Tag (3.2.4) 69
VLAN Tag Field Details 69
Native VLANs and 802.1Q Tagging (3.2.5) 70
Tagged Frames on the Native VLAN 70
Untagged Frames on the Native VLAN 70
Voice VLAN Tagging (3.2.6) 71
Voice VLAN Verification Example (3.2.7) 72
VLAN Configuration (3.3) 73
VLAN Ranges on Catalyst Switches (3.3.1) 73
Normal Range VLANs 74
Extended Range VLANs 74
VLAN Creation Commands (3.3.2) 75
VLAN Creation Example (3.3.3) 75
VLAN Port Assignment Commands (3.3.4) 76
VLAN Port Assignment Example (3.3.5) 77
Data and Voice VLANs (3.3.6) 78
Data and Voice VLAN Example (3.3.7) 78
Verify VLAN Information (3.3.8) 79
Change VLAN Port Membership (3.3.9) 81
Delete VLANs (3.3.10) 82

VLAN Trunks (3.4) 83
Trunk Configuration Commands (3.4.1) 83
Trunk Configuration Example (3.4.2) 83
Verify Trunk Configuration (3.4.3) 85
Reset the Trunk to the Default State (3.4.4) 86

Dynamic Trunking Protocol (3.5) 87
Introduction to DTP (3.5.1) 88
Negotiated Interface Modes (3.5.2) 89
Results of a DTP Configuration (3.5.3) 89
Verify DTP Mode (3.5.4) 90

Summary (3.6) 92
Overview of VLANs 92
VLANs in a Multi-Switched Environment 92
VLAN Configuration 92
VLAN Trunks 93
Dynamic Trunking Protocol 93

Practice 93
Check Your Understanding Questions 94

Chapter 4  Inter-VLAN Routing 97
Objectives 97
Key Terms 97
Introduction (4.0) 98

Inter-VLAN Routing Operation (4.1) 98
What Is Inter-VLAN Routing? (4.1.1) 98
Legacy Inter-VLAN Routing (4.1.2) 98
Router-on-a-Stick Inter-VLAN Routing (4.1.3) 100
Inter-VLAN Routing on a Layer 3 Switch (4.1.4) 102
Introduction (5.0)  139

Purpose of STP (5.1)  139
  Redundancy in Layer 2 Switched Networks (5.1.1)  139
  Spanning Tree Protocol (5.1.2)  140
  STP Recalculation (5.1.3)  141
  Issues with Redundant Switch Links (5.1.4)  141
  Layer 2 Loops (5.1.5)  142
  Broadcast Storm (5.1.6)  143
  The Spanning Tree Algorithm (5.1.7)  145

STP Operations (5.2)  148
  Steps to a Loop-Free Topology (5.2.1)  148
    Bridge Priority  149
    Extended System ID  149
    MAC address  150
  1. Elect the Root Bridge (5.2.2)  150
  Impact of Default BIDs (5.2.3)  151
  Determine the Root Path Cost (5.2.4)  152
  2. Elect the Root Ports (5.2.5)  152
  3. Elect Designated Ports (5.2.6)  153
  4. Elect Alternate (Blocked) Ports (5.2.7)  156
  Elect a Root Port from Multiple Equal-Cost Paths (5.2.8)  156
    1. Lowest Sender BID  157
    2. Lowest Sender Port Priority  157
    3. Lowest Sender Port ID  158
  STP Timers and Port States (5.2.9)  158
  Operational Details of Each Port State (5.2.10)  160
  Per-VLAN Spanning Tree (5.2.11)  160

Evolution of STP (5.3)  161
  Different Versions of STP (5.3.1)  161
  RSTP Concepts (5.3.2)  162
  RSTP Port States and Port Roles (5.3.3)  163
    STP and RSTP Port States  163
  PortFast and BPDU Guard (5.3.4)  165
  Alternatives to STP (5.3.5)  166
Chapter 8  SLAAC and DHCPv6  223
Objectives  223
Key Terms  223
Introduction (8.0)  224
IPv6 GUA Assignment (8.1)  224
IPv6 Host Configuration (8.1.1)  224
IPv6 Host Link-Local Address (8.1.2)  224
IPv6 GUA Assignment (8.1.3)  226
Three RA Message Flags (8.1.4)  226
SLAAC (8.2)  228
SLAAC Overview (8.2.1)  228
Enabling SLAAC (8.2.2)  229
Verify IPv6 Addresses  229
Enable IPv6 Routing  230
Verify SLAAC Is Enabled  230
SLAAC Only Method (8.2.3)  231
ICMPv6 RS Messages (8.2.4)  232
Host Process to Generate Interface ID (8.2.5)  233
Duplicate Address Detection (8.2.6)  234
DHCPv6 (8.3)  234
DHCPv6 Operation Steps (8.3.1)  234
Stateless DHCPv6 Operation (8.3.2)  236
Enable Stateless DHCPv6 on an Interface (8.3.3)  237
Stateful DHCPv6 Operation (8.3.4)  238
Enable Stateful DHCPv6 on an Interface (8.3.5)  239
Configure DHCPv6 Server (8.4)  240
DHCPv6 Router Roles (8.4.1)  240
Configure a Stateless DHCPv6 Server (8.4.2)  240
Configure a Stateless DHCPv6 Client (8.4.3)  243
Configure a Stateful DHCPv6 Server (8.4.4)  245
Configure a Stateful DHCPv6 Client (8.4.5)  248
DHCPv6 Server Verification Commands (8.4.6)  250
Configure a DHCPv6 Relay Agent (8.4.7)  252
Verify the DHCPv6 Relay Agent (8.4.8)  252
Summary  255
IPv6 GUA Assignment  255
SLAAC  255
Chapter 9  FHRP Concepts  261
Objectives  261
Key Terms  261

Introduction (9.0)  262
First Hop Redundancy Protocols (9.1)  262
  Default Gateway Limitations (9.1.1)  262
  Router Redundancy (9.1.2)  264
  Steps for Router Failover (9.1.3)  265
  FHRP Options (9.1.4)  266

HSRP (9.2)  267
  HSRP Overview (9.2.1)  267
  HSRP Priority and Preemption (9.2.2)  268
    HSRP Priority  268
    HSRP Preemption  268
  HSRP States and Timers (9.2.3)  269

Summary (9.3)  271
  First Hop Redundancy Protocols  271
    HSRP  271

Practice  272

Check Your Understanding Questions  272

Chapter 10  LAN Security Concepts  275
Objectives  275
Key Terms  275

Introduction (10.0)  277
Endpoint Security (10.1)  277
  Network Attacks Today (10.1.1)  277
  Network Security Devices (10.1.2)  278
  Endpoint Protection (10.1.3)  278
  Cisco Email Security Appliance (10.1.4)  279
  Cisco Web Security Appliance (10.1.5)  280
Access Control (10.2) 281
  Authentication with a Local Password (10.2.1) 281
  AAA Components (10.2.2) 283
  Authentication (10.2.3) 283
    Local AAA Authentication 284
    Server-Based AAA Authentication 284
  Authorization (10.2.4) 285
  Accounting (10.2.5) 285
  802.1X (10.2.6) 286

Layer 2 Security Threats (10.3) 287
  Layer 2 Vulnerabilities (10.3.1) 287
  Switch Attack Categories (10.3.2) 288
  Switch Attack Mitigation Techniques (10.3.3) 289

MAC Address Table Attack (10.4) 290
  Switch Operation Review (10.4.1) 290
  MAC Address Table Flooding (10.4.2) 290
  MAC Address Table Attack Mitigation (10.4.3) 291

LAN Attacks (10.5) 292
  VLAN Hopping Attacks (10.5.2) 293
  VLAN Double-Tagging Attack (10.5.3) 293
    VLAN Attack Mitigation 295
  DHCP Messages (10.5.4) 296
  DHCP Attacks (10.5.5) 296
    DHCP Starvation Attack 296
    DHCP Spoofing Attack 297
  ARP Attacks (10.5.7) 300
  Address Spoofing Attack (10.5.8) 303
  STP Attack (10.5.9) 303
  CDP Reconnaissance (10.5.10) 305

Summary (10.6) 307
Practice 308
Check Your Understanding Questions 309

Chapter 11  Switch Security Configuration 313
Objectives 313
Key Terms 313
Introduction (11.0) 314
Implement Port Security (11.1) 314
   Secure Unused Ports (11.1.1) 314
   Mitigate MAC Address Table Attacks (11.1.2) 315
   Enable Port Security (11.1.3) 316
   Limit and Learn MAC Addresses (11.1.4) 317
   Port Security Aging (11.1.5) 319
   Port Security Violation Modes (11.1.6) 321
   Ports in error-disabled State (11.1.7) 322
   Verify Port Security (11.1.8) 324
      Port Security for All Interfaces 325
      Port Security for a Specific Interface 325
   Verify Learned MAC Addresses 326
   Verify Secure MAC Addresses 326

Mitigate VLAN Attacks (11.2) 327
   VLAN Attacks Review (11.2.1) 327
   Steps to Mitigate VLAN Hopping Attacks (11.2.2) 327

Mitigate DHCP Attacks (11.3) 329
   DHCP Attack Review (11.3.1) 329
   DHCP Snooping (11.3.2) 329
   Steps to Implement DHCP Snooping (11.3.3) 330
   DHCP Snooping Configuration Example (11.3.4) 331

Mitigate ARP Attacks (11.4) 332
   Dynamic ARP Inspection (11.4.1) 333
   DAI Implementation Guidelines (11.4.2) 333
   DAI Configuration Example (11.4.3) 333

Mitigate STP Attacks (11.5) 335
   PortFast and BPDU Guard (11.5.1) 335
   Configure PortFast (11.5.2) 336
   Configure BPDU Guard (11.5.3) 338

Summary (11.6) 340
Practice 342
Check Your Understanding Questions 343

Chapter 12 WLAN Concepts 347
Objectives 347
Key Terms 347
Introduction (12.0) 349

Introduction to Wireless (12.1) 349
  Benefits of Wireless (12.1.1) 349
  Types of Wireless Networks (12.1.2) 349
  Wireless Technologies (12.1.3) 350
  802.11 Standards (12.1.4) 353
  Radio Frequencies (12.1.5) 354
  Wireless Standards Organizations (12.1.6) 355

WLAN Components (12.2) 356
  Wireless NICs (12.2.2) 356
  Wireless Home Router (12.2.3) 357
  Wireless Access Points (12.2.4) 358
  AP Categories (12.2.5) 358
    Autonomous APs 359
    Controller-Based APs 359
  Wireless Antennas (12.2.6) 360

WLAN Operation (12.3) 362
  802.11 Wireless Topology Modes (12.3.2) 362
  BSS and ESS (12.3.3) 364
    Basic Service Set 364
    Extended Service Set 365
  802.11 Frame Structure (12.3.4) 365
  CSMA/CA (12.3.5) 367
  Wireless Client and AP Association (12.3.6) 367
  Passive and Active Discover Mode (12.3.7) 368
    Passive Mode 368
    Active Mode 369

CAPWAP Operation (12.4) 370
  Introduction to CAPWAP (12.4.2) 370
  Split MAC Architecture (12.4.3) 371
    DTLS Encryption (12.4.4) 372
    FlexConnect APs (12.4.5) 372

Channel Management (12.5) 373
  Frequency Channel Saturation (12.5.1) 373
  Channel Selection (12.5.2) 375
  Plan a WLAN Deployment (12.5.3) 377
WLAN Threats (12.6) 379
  Wireless Security Overview (12.6.2) 379
  DoS Attacks (12.6.3) 380
  Rogue Access Points (12.6.4) 381
  Man-in-the-Middle Attack (12.6.5) 381

Secure WLANs (12.7) 383
  SSID Cloaking and MAC Address Filtering (12.7.2) 383
    SSID Cloaking 383
    MAC Addresses Filtering 384
  802.11 Original Authentication Methods (12.7.3) 385
  Shared Key Authentication Methods (12.7.4) 385
  Authenticating a Home User (12.7.5) 386
  Encryption Methods (12.7.6) 387
  Authentication in the Enterprise (12.7.7) 388
  WPA3 (12.7.8) 389
    WPA3-Personal 389
    WPA3-Enterprise 390
    Open Networks 390
    IoT Onboarding 390

Summary (12.8) 391

Practice 392

Check Your Understanding Questions 392

Chapter 13 WLAN Configuration 397

Objectives 397

Key Terms 397

Introduction (13.0) 398

Remote Site WLAN Configuration (13.1) 398
  The Wireless Router (13.1.2) 398
  Log in to the Wireless Router (13.1.3) 399
  Basic Network Setup (13.1.4) 401
  Basic Wireless Setup (13.1.5) 404
  Configure a Wireless Mesh Network (13.1.6) 408
  NAT for IPv4 (13.1.7) 408
  Quality of Service (13.1.8) 410
  Port Forwarding (13.1.9) 410
Configure a Basic WLAN on the WLC (13.2)  412
  WLC Topology (13.2.2)  412
  Log in to the WLC (13.2.3)  414
  View AP Information (13.2.4)  415
  Advanced Settings (13.2.5)  416
  Configure a WLAN (13.2.6)  416

Configure a WPA2 Enterprise WLAN on the WLC (13.3)  421
  SNMP and RADIUS (13.3.2)  421
  Configure SNMP Server Information (13.3.3)  421
  Configure RADIUS Server Information (13.3.4)  423
  Topology with VLAN 5 Addressing (13.3.6)  424
  Configure a New Interface (13.3.7)  425
  Configure a DHCP Scope (13.3.9)  428
  Configure a WPA2 Enterprise WLAN (13.3.11)  430

Troubleshoot WLAN Issues (13.4)  433
  Troubleshooting Approaches (13.4.1)  433
  Wireless Client Not Connecting (13.4.2)  435
  Troubleshooting When the Network Is Slow (13.4.3)  436
  Updating Firmware (13.4.4)  438

Summary (13.5)  440
Practice  441
Check Your Understanding Questions  441

Chapter 14  Routing Concepts  445
Objectives  445
Key Terms  445
Introduction (14.0)  447
Path Determination (14.1)  447
  Two Functions of Router (14.1.1)  447
  Router Functions Example (14.1.2)  447
  Best Path Equals Longest Match (14.1.3)  448
  IPv4 Address Longest Match Example (14.1.4)  449
  IPv6 Address Longest Match Example (14.1.5)  449
  Build the Routing Table (14.1.6)  450
    Directly Connected Networks  450
    Remote Networks  450
    Default Route  451
Packet Forwarding (14.2)  451
Packet Forwarding Decision Process (14.2.1)  451
Forwards the Packet to a Device on a Directly Connected Network  452
Forwards the Packet to a Next-Hop Router  453
Drops the Packet—No Match in Routing Table  453
End-to-End Packet Forwarding (14.2.2)  453
PC1 Sends Packet to PC2  453
R1 Forwards the Packet to PC2  454
R2 Forwards the Packet to R3  455
R3 Forwards the Packet to PC2  455
Packet Forwarding Mechanisms (14.2.3)  455
Process Switching  456
Fast Switching  456
Cisco Express Forwarding (CEF)  458

Basic Router Configuration Review (14.3)  459
Topology (14.3.1)  459
Configuration Commands (14.3.2)  459
Verification Commands (14.3.3)  461
Filter Command Output (14.3.4)  466

IP Routing Table (14.4)  467
Route Sources (14.4.1)  467
Routing Table Principles (14.4.2)  469
Routing Table Entries (14.4.3)  469
Directly Connected Networks (14.4.4)  470
Static Routes (14.4.5)  471
Static Routes in the IP Routing Table (14.4.6)  472
Dynamic Routing Protocols (14.4.7)  474
Default Route (14.4.9)  475
Structure of an IPv4 Routing Table (14.4.10)  477
Structure of an IPv6 Routing Table (14.4.11)  478
Administrative Distance (14.4.12)  479

Static and Dynamic Routing (14.5)  480
Static or Dynamic? (14.5.1)  480
Static Routes  481
Dynamic Routing Protocols  481
Dynamic Routing Evolution (14.5.2)  482
Dynamic Routing Protocol Concepts (14.5.3)  483
Chapter 15  IP Static Routing  495

Objectives  495

Key Terms  495

Introduction (15.0)  496

Static Routes (15.1)  496
  Types of Static Routes (15.1.1)  496
  Next-Hop Options (15.1.2)  497
  IPv4 Static Route Command (15.1.3)  497
  IPv6 Static Route Command (15.1.4)  498
  Dual-Stack Topology (15.1.5)  499
  IPv4 Starting Routing Tables (15.1.6)  499
  IPv6 Starting Routing Tables (15.1.7)  501

Configure IP Static Routes (15.2)  503
  IPv4 Next-Hop Static Route (15.2.1)  503
  IPv6 Next-Hop Static Route (15.2.2)  504
  IPv4 Directly Connected Static Route (15.2.3)  505
  IPv6 Directly Connected Static Route (15.2.4)  506
  IPv4 Fully Specified Static Route (15.2.5)  507
  IPv6 Fully Specified Static Route (15.2.6)  509
  Verify a Static Route (15.2.7)  510
    Display Only IPv4 Static Routes  511
    Display a Specific IPv4 Network  511
    Display the IPv4 Static Route Configuration  511
    Display Only IPv6 Static Routes  512
    Display a Specific IPv6 Network  512
    Display the IPv6 Static Route Configuration  512
Configure IP Default Static Routes (15.3) 513
  Default Static Route (15.3.1) 513
    IPv4 Default Static Route 513
    IPv6 Default Static Route 514
  Configure a Default Static Route (15.3.2) 514
  Verify a Default Static Route (15.3.3) 515

Configure Floating Static Routes (15.4) 517
  Floating Static Routes (15.4.1) 517
  Configure IPv4 and IPv6 Floating Static Routes (15.4.2) 518
  Test the Floating Static Route (15.4.3) 520

Configure Static Host Routes (15.5) 521
  Host Routes (15.5.1) 521
    Automatically Installed Host Routes (15.5.2) 522
  Static Host Routes (15.5.3) 523
  Configure Static Host Routes (15.5.4) 523
  Verify Static Host Routes (15.5.5) 523
  Configure IPv6 Static Host Route with Link-Local Next-Hop (15.5.6) 524

Summary (15.6) 525
  Static Routes 525
    Configure IP Static Routes 525
    Configure IP Default Static Routes 525
    Configure Floating Static Routes 526
    Configure Static Host Routes 526

Practice 527

Check Your Understanding Questions 527

Chapter 16 Troubleshoot Static and Default Routes 531

Objectives 531

Introduction (16.0) 532

Packet Processing with Static Routes (16.1) 532
  Static Routes and Packet Forwarding (16.1.1) 532

Troubleshoot IPv4 Static and Default Route Configuration (16.2) 533
  Network Changes (16.2.1) 534
  Common Troubleshooting Commands (16.2.2) 534
Solve a Connectivity Problem (16.2.3)  536
  Ping the Remote LAN  536
  Ping the Next-Hop Router  537
  Ping R3 LAN from S0/1/0  537
  Verify the R2 Routing Table  538
  Correct the R2 Static Route Configuration  538
  Verify New Static Route Is Installed  538
  Ping the Remote LAN Again  539

Summary (16.3)  540
  Packet Processing with Static Routes  540
  Troubleshoot IPv4 Static and Default Route Configuration  540

Practice  541
Check Your Understanding Questions  542

Appendix A  Answers to the “Check Your Understanding” Questions  545

Glossary  561

Index  587
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

*Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)* is the official supplemental textbook for the Cisco Network Academy CCNA Switching, Routing, and Wireless Essentials version 7 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.

As a textbook, this book 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 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 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 each chapter 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 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 more than 300 terms.

### Practice

Practice makes perfect. This 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:** 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.

- **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 is a practice section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter.

- **Page references to online course:** After headings, you will see, for example, (1.1.2). 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.
About Packet Tracer Software and Activities

Interspersed throughout the chapters you'll find a few Cisco Packet Tracer activities. 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 Networking Academy Switching, Routing, and Wireless Essentials course and is divided into 16 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, “Basic Device Configuration”:** This chapter explains how to configure devices using security best practices. Included are initial switch and router configuration, switch port configuration, remote access configuration, and how to verify connectivity between two networks.

- **Chapter 2, “Switching Concepts”:** This chapter explains how switches forward data. Included are frame forwarding methods and collision and broadcast domain comparison.

- **Chapter 3, “VLANs”:** This chapter explains how to implement VLANs and trunking in a switched network. Included are explanations of the purpose of VLANs, how VLANs forward frames in a multiswitched environment, VLAN port assignments, trunk configuration, and DTP configuration.

- **Chapter 4, “Inter-VLAN Routing”:** This chapter explains how to implement inter-VLAN routing. Included are descriptions of inter-VLAN routing options, router-on-a-stick configuration, Layer 3 switch inter-VLAN routing, and troubleshooting common inter-VLAN routing configuration issues.

- **Chapter 5, “STP Concepts”:** This chapter explains how STP enables redundancy in a Layer 3 network. Included are explanations of common problems in redundant Layer 2 networks, STP operation, and Rapid PVST+ operation.

- **Chapter 6, “EtherChannel”:** This chapter explains how to implement EtherChannel on switched links. Included are descriptions of EtherChannel technology, EtherChannel configuration, and troubleshooting EtherChannel.

- **Chapter 7, “DHCPv4”:** This chapter explains how to implement DHCPv4 for multiple LANs. Included is an explanation of DHCPv4 operation, as well as configuring a router as a DHCPv4 server or DHCPv4 client.
Chapter 8, “SLAAC and DHCPv6”: This chapter explains how to implement dynamic address allocation in an IPv6 network. Included are explanations of how an IPv6 host acquires its addressing, SLAAC operation, DHCPv6 operation, and configuring a router as a stateful or stateless DHCPv6 server.

Chapter 9, “FHRP Concepts”: This chapter explains how FHRPs provide default gateway services in a redundant network. Included are explanations of the purpose of FHRPs and HSRP operation.

Chapter 10, “LAN Security Concepts”: This chapter explains how vulnerabilities compromise LAN security. Included are explanations of how to use endpoint security, how AAA and 802.1X are used to authenticate, Layer 2 vulnerabilities, MAC address table attacks, and LAN attacks.

Chapter 11, “Switch Security Configuration”: This chapter explains how to configure switch security to mitigate LAN attacks. Included is port security implementation as well as mitigating VLAN, DHCP, ARP, and STP attacks.

Chapter 12, “WLAN Concepts”: This chapter explains how WLANs enable network connectivity for wireless devices. Included are explanations of WLAN technology, WLAN components, and WLAN operation. In addition, the chapter discusses how CAPWAP is used to manage multiple APs for a WLC. WLAN channel management is discussed. The chapter concludes with a discussion of threats to WLANs and how to secure WLANs.

Chapter 13, “WLAN Configuration”: This chapter explains how to implement a WLAN using a wireless router and a WLC. Included are explanations of wireless router configuration and WLC WLAN configuration for both WPA2 PSK and WPA2 Enterprise authentication. The chapter concludes with a discussion of how to troubleshoot common wireless configuration issues.

Chapter 14, “Routing Concepts”: This chapter explains how routers use information in packets to make forwarding decisions. Included are explanations of path determination, packet forwarding, basic router configuration, routing table structure, and static and dynamic routing concepts.

Chapter 15, “IP Static Routing”: This chapter explains how to implement IPv4 and IPv6 static routes. Included are static route syntax, static and default routing configuration, floating static routing configuration, and static host route configuration.

Chapter 16, “Troubleshoot Static and Default Routes”: This chapter explains how to troubleshoot static and default route implementations. Included are explanations of how a router processes packets when a static route is configured, and how to troubleshoot command static and default route configuration issues.
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.

Figure Credits

Figure 1-6, screenshot of Telnet Session Capture © Wireshark
Figure 1-7, screenshot of SSH Session Capture © Wireshark
Figure 7-8, screenshot of Configuring a Home Router as a DHCPv4 Client © 2020 Belkin International, Inc.
Figure 8-1, screenshot of Manual Configuration of an IPv6 Windows Host © Microsoft 2020
Figure 8-2, screenshot of Automatic Configuration of an IPv6 Windows Host © Microsoft 2020
Figure 10-1, screenshot of WannaCry Ransomware © Lazarus Group
Figure 10-29, screenshot of Wireshark Capture of a CDP Frame © Wireshark
Figure 12-38, screenshot of Disabling SSID Broadcast (SSID Cloaking) on a Wireless Router © 2020 Belkin International, Inc.
Figure 12-39, screenshot of Configuring MAC Address Filtering on a Wireless Router © 2020 Belkin International, Inc.
Figure 12-41, screenshot of Selecting the Authentication Method on a Wireless Router © 2020 Belkin International, Inc.
Figure 12-42, screenshot of Setting the Encryption Method on a Wireless Router © 2020 Belkin International, Inc.
Figure 12-43, screenshot of Configuring WPA2 Enterprise Authentication on a Wireless Router © 2020 Belkin International, Inc.
Figure 13-3, screenshot of Connecting to a Wireless Router Using a Browser © 2020 Belkin International, Inc.
Figure 13-4, screenshot of Basic Network Setup - Step 1 © 2020 Belkin International, Inc.
Figure 13-5, screenshot of Basic Network Setup - Step 2 © 2020 Belkin International, Inc.
Figure 13-6, screenshot of Basic Network Setup - Step 3 © 2020 Belkin International, Inc.

Figure 13-7, screenshot of Basic Network Setup - Step 4 © 2020 Belkin International, Inc.

Figure 13-8, screenshot of Basic Network Setup - Step 6 © 2020 Belkin International, Inc.

Figure 13-9, screenshot of Basic Wireless Setup - Step 1 © 2020 Belkin International, Inc.

Figure 13-10, screenshot of Basic Wireless Setup - Step 2 © 2020 Belkin International, Inc.

Figure 13-11, screenshot of Basic Wireless Setup - Step 3 © 2020 Belkin International, Inc.

Figure 13-12, screenshot of Basic Wireless Setup - Step 4 © 2020 Belkin International, Inc.

Figure 13-13, screenshot of Basic Wireless Setup - Step 5 © 2020 Belkin International, Inc.

Figure 13-14, screenshot of Basic Wireless Setup - Step 6 © 2020 Belkin International, Inc.

Figure 13-16, screenshot of Verifying the Status of a Wireless Router © 2020 Belkin International, Inc.

Figure 13-18, screenshot of Configuring Port Forwarding on a Wireless Router © 2020 Belkin International, Inc.
CHAPTER 4

Inter-VLAN Routing

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

■ What are the options for configuring inter-VLAN routing?
■ How do you configure router-on-a-stick inter-VLAN routing?
■ How do you configure inter-VLAN routing using Layer 3 switching?
■ How do you troubleshoot common inter-VLAN configuration issues?

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

inter-VLAN routing  Page 98
legacy inter-VLAN routing  Page 98
router-on-a-stick  Page 98
subinterfaces  Page 100
switched virtual interface (SVI)  Page 112
routed port  Page 112
Introduction (4.0)

Now you know how to segment and organize your network into VLANs. Hosts can communicate with other hosts in the same VLAN, and you no longer have hosts sending out broadcast messages to every other device in your network, eating up needed bandwidth. But what if a host in one VLAN needs to communicate with a host in a different VLAN? If you are a network administrator, you know that people will want to communicate with other people outside of your network. This is where inter-VLAN routing can help you. Inter-VLAN routing uses a Layer 3 device, such as a router or a Layer 3 switch. Let’s take your VLAN expertise and combine it with your network layer skills and put them to the test!

Inter-VLAN Routing Operation (4.1)

In this section, you learn about two options for configuring for inter-VLAN routing.

What Is Inter-VLAN Routing? (4.1.1)

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

- **Legacy Inter-VLAN routing**: This is a legacy solution. It does not scale well.
- **Router-on-a-Stick**: This is an acceptable solution for a small- to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs)**: This is the most scalable solution for medium to large organizations.

Legacy Inter-VLAN Routing (4.1.2)

The first inter-VLAN routing solution relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.
For example, refer to the topology in Figure 4-1 where R1 has two interfaces connected to switch S1.

**Note**

The IPv4 addresses of PC1, PC2, and R1 all have a /24 subnet mask.

![Figure 4-1](image.png)

**Figure 4-1** Legacy Inter-VLAN Routing Example

As shown in Table 4-1, the example MAC address table of S1 is populated as follows:

- Fa0/1 port is assigned to VLAN 10 and is connected to the R1 G0/0/0 interface.
- Fa0/11 port is assigned to VLAN 10 and is connected to PC1.
- Fa0/12 port is assigned to VLAN 20 and is connected to the R1 G0/0/1 interface.
- Fa0/11 port is assigned to VLAN 20 and is connected to PC2.

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>F0/1</td>
<td>R1 G0/0/0 MAC</td>
<td>10</td>
</tr>
<tr>
<td>F0/11</td>
<td>PC1 MAC</td>
<td>10</td>
</tr>
<tr>
<td>F0/12</td>
<td>R1 G0/0/1 MAC</td>
<td>20</td>
</tr>
<tr>
<td>F0/24</td>
<td>PC2 MAC</td>
<td>20</td>
</tr>
</tbody>
</table>
When PC1 sends a packet to PC2 on another network, it forwards it to its default gateway 192.168.10.1. R1 receives the packet on its G0/0/0 interface and examines the destination address of the packet. R1 then routes the packet out its G0/0/1 interface to the F0/12 port in VLAN 20 on S1. Finally, S1 forwards the frame to PC2.

Legacy inter-VLAN routing using physical interfaces works, but it has a significant limitation. It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.

In our example, R1 required two separate Ethernet interfaces to route between VLAN 10 and VLAN 20. What if there were six (or more) VLANs to interconnect? A separate interface would be required for each VLAN. Obviously, this solution is not scalable.

**Note**

This method of inter-VLAN routing is no longer implemented in switched networks and is included for explanation purposes only.

### Router-on-a-Stick Inter-VLAN Routing (4.1.3)

The “router-on-a-stick” inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It requires only one physical Ethernet interface to route traffic between multiple VLANs on a network.

A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using *subinterfaces* to identify routable VLANs.

The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.

When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.1Q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface.

Figure 4-2 shows an example of router-on-a-stick inter-VLAN routing. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1 using a single, physical router interface.
Figure 4-2   Unicast from VLAN 10 Is Route to VLAN 30

Figure 4-2 illustrates the following steps:

Step 1.   PC1 sends its unicast traffic to switch S2.
Step 2.   Switch S2 tags the unicast traffic as originating on VLAN 10 and forwards the unicast traffic out its trunk link to switch S1.
Step 3.   Switch S1 forwards the tagged traffic out the other trunk interface on port F0/3 to the interface on router R1.
Step 4.   Router R1 accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 30 using its configured subinterfaces.

In Figure 4-3, R1 routes the traffic to the correct VLAN.

Figure 4-3 illustrates the following steps:

Step 5.   The unicast traffic is tagged with VLAN 30 as it is sent out the router interface to switch S1.
Step 6.   Switch S1 forwards the tagged unicast traffic out the other trunk link to switch S2.
Step 7.   Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.
Inter-VLAN Routing on a Layer 3 Switch (4.1.4)

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch, as shown in Figure 4-4.

Note

The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.
A Layer 3 switch is also called a multilayer switch because it operates at Layer 2 and Layer 3. However, in this course we use the term Layer 3 switch.

Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.
- They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
- Latency is much lower because data does not need to leave the switch to be routed to a different network.
- They are more commonly deployed in a campus LAN than routers.

The only disadvantage is that Layer 3 switches are more expensive than Layer 2 switches, but they can be less expensive than a separate Layer 2 switch and router.

Check Your Understanding—Inter-VLAN Routing Operation (4.1.5)
Refer to the online course to complete this activity.

Router-on-a-Stick Inter-VLAN Routing (4.2)
In this section, you configure router-on-a-stick inter-VLAN routing.

Router-on-a-Stick Scenario (4.2.1)
In the previous section, three ways to create inter-VLAN routing were listed, and legacy inter-VLAN routing was detailed. This section details how to configure router-on-a-stick inter-VLAN routing. You can see in the figure that the router is not in the center of the topology but instead appears to be on a stick near the border, hence the name.
In Figure 4-5, the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.

<table>
<thead>
<tr>
<th>Subinterface</th>
<th>VLAN</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/0/1.10</td>
<td>10</td>
<td>192.168.10.1/24</td>
</tr>
<tr>
<td>G0/0/1.20</td>
<td>20</td>
<td>192.168.20.1/24</td>
</tr>
<tr>
<td>G0/0/1.30</td>
<td>99</td>
<td>192.168.99.1/24</td>
</tr>
</tbody>
</table>
Assume that R1, S1, and S2 have initial basic configurations. Currently, PC1 and PC2 cannot ping each other because they are on separate networks. Only S1 and S2 can ping each other, but they but are unreachable by PC1 or PC2 because they are also on different networks.

To enable devices to ping each other, the switches must be configured with VLANs and trunking, and the router must be configured for inter-VLAN routing.

**S1 VLAN and Trunking Configuration (4.2.2)**

Complete the following steps to configure S1 with VLANs and trunking:

**Step 1.** Create and name the VLANs. First, the VLANs are created and named, as shown in Example 4-1. VLANs are created only after you exit out of VLAN subconfiguration mode.

**Example 4-1  Create and Name VLANs**

```
S1(config)# vlan 10
S1(config-vlan)# name LAN10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name LAN20
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

**Step 2.** Create the management interface. Next, the management interface is created on VLAN 99 along with the default gateway of R1, as shown in Example 4-2.

**Example 4-2  Create the Management Interface**

```
S1(config)# interface vlan 99
S1(config-if)# ip add 192.168.99.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#
```

**Step 3.** Configure access ports. Next, port Fa0/6 connecting to PC1 is configured as an access port in VLAN 10, as shown in Example 4-3. Assume PC1 has been configured with the correct IP address and default gateway.
Example 4-3  Configure Access Ports

```
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

Step 4. Configure trunking ports. Finally, ports Fa0/1 connecting to S2 and Fa05 connecting to R1 are configured as trunk ports, as shown in Example 4-4.

Example 4-4  Configure Trunking Ports

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# end
```

*S 00:22:43.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

*S 00:22:44.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

S2 VLAN and Trunking Configuration (4.2.3)
The configuration for S2 is similar to S1, as shown in Example 4-5.

Example 4-5  S2 Configuration

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
```
R1 Subinterface Configuration (4.2.4)

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed.

A subinterface is created using the `interface interface_id.subinterface_id` global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

- **encapsulation dot1q vlan_id [native]**: This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified `vlan-id`. The `native` keyword option is only appended to set the native VLAN to something other than VLAN 1.

- **ip address ip-address subnet-mask**: This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur.

When all subinterfaces have been created, enable the physical interface using the `no shutdown` interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

In the configuration in Example 4-6, the R1 G0/0/1 subinterfaces are configured for VLANs 10, 20, and 99.
Example 4-6  R1 Subinterface Configuration

```
R1(config)# interface G0/0/1.10  
R1(config-subif)# description Default Gateway for VLAN 10  
R1(config-subif)# encapsulation dot1q 10  
R1(config-subif)# ip add 192.168.10.1 255.255.255.0  
R1(config-subif)# exit  
R1(config)#  
R1(config)# interface G0/0/1.20  
R1(config-subif)# description Default Gateway for VLAN 20  
R1(config-subif)# encapsulation dot1q 20  
R1(config-subif)# ip add 192.168.20.1 255.255.255.0  
R1(config-subif)# exit  
R1(config)#  
R1(config)# interface G0/0/1.99  
R1(config-subif)# description Default Gateway for VLAN 99  
R1(config-subif)# encapsulation dot1q 99  
R1(config-subif)# ip add 192.168.99.1 255.255.255.0  
R1(config-subif)# exit  
R1(config)#  
R1(config)# interface G0/0/1  
R1(config-if)# description Trunk link to S1  
R1(config-if)# no shut  
R1(config-if)# end  
R1#  
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down  
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up  
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up  
R1#  
```

Verify Connectivity Between PC1 and PC2 (4.2.5)

The router-on-a-stick configuration is complete after the switch trunk and the router subinterfaces have been configured. The configuration can be verified from the hosts, router, and switch.

From a host, verify connectivity to a host in another VLAN using the `ping` command. It is a good idea to first verify the current host IP configuration using the `ipconfig` Windows host command, as shown in Example 4-7.
Example 4-7  Verify Windows Host Configuration

```
C:\Users\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . :  
    Link-local IPv6 Address : fe80::5c43:ee7c:2959:da68%6
    IPv4 Address : 192.168.10.10
    Subnet Mask : 255.255.255.0
    Default Gateway : 192.168.10.1
C:\Users\PC1>
```

The output confirms the IPv4 address and default gateway of PC1. Next, use `ping` to verify connectivity with PC2 and S1, as shown in Figure 4-5. The `ping` output successfully confirms that inter-VLAN routing is operating, as shown in Example 4-8.

Example 4-8  Verify Inter-VLAN Routing by Pinging from PC1

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
    Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
    Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
    Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
    Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
    Request timed out.
    Request timed out.
    Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
    Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
    Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```
Router-on-a-Stick Inter-VLAN Routing Verification  (4.2.6)

In addition to using ping between devices, the following show commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- show ip route
- show ip interface brief
- show interfaces
- show interfaces trunk

As shown in Example 4-9, verify that the subinterfaces are appearing in the routing table of R1 by using the `show ip route` command. Notice that there are three connected routes (C) and their respective exit interfaces for each routable VLAN. The output confirms that the correct subnets, VLANs, and subinterfaces are active.

Example 4-9  Verify Subinterfaces Are in Routing Table

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
   192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
     C   192.168.10.0/24 is directly connected, GigabitEthernet0/0/1.10
     L   192.168.10.1/32 is directly connected, GigabitEthernet0/0/1.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
     C   192.168.20.0/24 is directly connected, GigabitEthernet0/0/1.20
     L   192.168.20.1/32 is directly connected, GigabitEthernet0/0/1.20
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
     C   192.168.99.0/24 is directly connected, GigabitEthernet0/0/1.99
     L   192.168.99.1/32 is directly connected, GigabitEthernet0/0/1.99
R1#
```

Another useful router command is `show ip interface brief`, as shown in Example 4-10. The output confirms that the subinterfaces have the correct IPv4 address configured, and that they are operational.

Example 4-10  Verify Subinterface IP Addresses and Status

```
R1# show ip interface brief | include up
GigabitEthernet0/0/1       unassigned  YES unset  up  up
G10/0/1.10                  192.168.10.1  YES manual  up  up
G10/0/1.20                  192.168.20.1  YES manual  up  up
G10/0/1.99                  192.168.99.1  YES manual  up  up
R1#
```
Subinterfaces can be verified using the `show interfaces subinterface-id` command, as shown in Example 4-11.

**Example 4-11  Verify Details of the Subinterface**

```plaintext
R1# show interfaces g0/0/1.10
GigabitEthernet0/0/1.10 is up, line protocol is up
    Hardware is ISR4221-2x1GE, address is 10b3.d605.0301 (bia 10b3.d605.0301)
    Description: Default Gateway for VLAN 10
    Internet address is 192.168.10.1/24
    MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
    ARP type: ARPA, ARP Timeout 04:00:00
    Keepalive not supported
    Last clearing of "show interface" counters never
R1#
```

The misconfiguration could also be on the trunking port of the switch. Therefore, it is also useful to verify the active trunk links on a Layer 2 switch by using the `show interfaces trunk` command, as shown in Example 4-12. The output confirms that the link to R1 is trunking for the required VLANs.

**Note**

Although VLAN 1 was not explicitly configured, it was automatically included because control traffic on trunk links will always be forwarded on VLAN 1.

**Example 4-12  Verify Trunk Link Status**

```plaintext
S1# show interfaces trunk
Port    Mode     Encapsulation Status  Native vlan
Fa0/1   on       802.1q      trunking  1
Fa0/5   on       802.1q      trunking  1
Port    Vlans allowed on trunk
Fa0/1   1-4094
Fa0/5   1-4094
Port    Vlans allowed and active in management domain
Fa0/1   1,10,20,99
Fa0/5   1,10,20,99
Port    Vlans in spanning tree forwarding state and not pruned
Fa0/1   1,10,20,99
Fa0/5   1,10,20,99
S1#
```
Packet Tracer—Configure Router-on-a-Stick Inter-VLAN Routing (4.2.7)
In this Packet Tracer activity, you check for connectivity prior to implementing inter-VLAN routing. Then you configure VLANs and inter-VLAN routing. Finally, you enable trunking and verify connectivity between VLANs.

Lab—Configure Router-on-a-Stick Inter-VLAN Routing (4.2.8)
In this lab, you complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure Switches with VLANs and Trunking
- Part 3: Configure Trunk-Based Inter-VLAN Routing

Inter-VLAN Routing using Layer 3 Switches (4.3)
In this section, you configure inter-VLAN routing using Layer 3 switches.

Layer 3 Switch Inter-VLAN Routing (4.3.1)
Modern enterprise networks rarely use router-on-a-stick because it does not scale easily to meet requirements. In these very large networks, network administrators use Layer 3 switches to configure inter-VLAN routing.

Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small- to medium-sized organization. However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

- Route from one VLAN to another using multiple switched virtual interfaces (SVIs).
- Convert a Layer 2 switchport to a Layer 3 interface (that is, a routed port). A routed port is similar to a physical interface on a Cisco IOS router.
To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same `interface vlan vlan-id` command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.

**Layer 3 Switch Scenario (4.3.2)**

In Figure 4-6, the Layer 3 switch, D1, is connected to two hosts on different VLANs. PC1 is in VLAN 10, and PC2 is in VLAN 20, as shown. The Layer 3 switch will provide inter-VLAN routing services to the two hosts.

![Layer 3 Switch Inter-VLAN Routing Topology](image)

**Figure 4-6** Layer 3 Switch Inter-VLAN Routing Topology

Table 4-3 shows the IP addresses for each VLAN.

**Table 4-3** D1 VLAN IP Addresses

<table>
<thead>
<tr>
<th>VLAN Interface</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>192.168.10.1/24</td>
</tr>
<tr>
<td>20</td>
<td>192.168.20.1/24</td>
</tr>
</tbody>
</table>
Layer 3 Switch Configuration (4.3.3)

Complete the following steps to configure S1 with VLANs and trunking:

**Step 1.** Create the VLANs. First, create the two VLANs as shown in Example 4-13.

**Example 4-13  Create the VLANs**

```bash
D1(config)# vlan 10
D1(config-vlan)# name LAN10
D1(config-vlan)# vlan 20
D1(config-vlan)# name LAN20
D1(config-vlan)# exit
D1(config)#
```

**Step 2.** Create the SVI VLAN interfaces. Configure the SVI for VLANs 10 and 20, as shown in Example 4-14. The IP addresses that are configured will serve as the default gateways to the hosts in the respective VLANs. Notice the informational messages showing the line protocol on both SVIs changed to up.

**Example 4-14  Create the SVI VLAN Interfaces**

```bash
D1(config)# interface vlan 10
D1(config-if)# description Default Gateway SVI for 192.168.10.0/24
D1(config-if)# ip add 192.168.10.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
D1(config)# int vlan 20
D1(config-if)# description Default Gateway SVI for 192.168.20.0/24
D1(config-if)# ip add 192.168.20.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
*Sep 17 13:52:16.053: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
*Sep 17 13:52:16.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
```

**Step 3.** Configure access ports. Next, configure the access ports connecting to the hosts and assign them to their respective VLANs, as shown in Example 4-15.
Step 4. **Enable IP routing.** Finally, enable IPv4 routing with the `ip routing` global configuration command to allow traffic to be exchanged between VLANs 10 and 20, as shown in Example 4-16. This command must be configured to enable inter-VLAN routing on a Layer 3 switch for IPv4.

**Example 4-16  Enable IP Routing**

```
D1(config)# ip routing
D1(config)#
```

**Layer 3 Switch Inter-VLAN Routing Verification (4.3.4)**

Inter-VLAN routing using a Layer 3 switch is simpler to configure than the router-on-a-stick method. After the configuration is complete, the configuration can be verified by testing connectivity between the hosts.

From a host, verify connectivity to a host in another VLAN using the `ping` command. It is a good idea to first verify the current host IP configuration using the `ipconfig` Windows host command. The output in Example 4-17 confirms the IPv4 address and default gateway of PC1.

**Example 4-17  Verify Windows Host Configuration**

```
C:\Users\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address : fe80::5c43:ee7c:2959:da68%6
    IPv4 Address : 192.168.10.10
    Subnet Mask : 255.255.255.0
    Default Gateway : 192.168.10.1
C:\Users\PC1>
```
Next, verify connectivity with PC2 using the **ping** Windows host command, as shown in Example 4-18. The **ping** output successfully confirms that inter-VLAN routing is operating.

**Example 4-18**  Verify Inter-VLAN Routing by Pinging from PC1

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
```

**Routing on a Layer 3 Switch (4.3.5)**

If VLANs are to be reachable by other Layer 3 devices, they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the `no switchport` interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.

**Routing Scenario on a Layer 3 Switch (4.3.6)**

In Figure 4-7, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.

**Note**

OSPF routing configuration is covered in another course. In this module, OSPF configuration commands will be given to you in all activities and assessments. It is not required that you understand the configuration in order to enable OSPF routing on the Layer 3 switch.
Routing Configuration on a Layer 3 Switch (4.3.7)

Complete the following steps to configure D1 to route with R1:

**Step 1.** Configure the routed port. Configure G1/0/1 to be a routed port, assign it an IPv4 address, and enable it, as shown in Example 4-19.

**Example 4-19** Configure the Routed Port

```
D1(config)# interface GigabitEthernet1/0/1
D1(config-if)# description routed Port Link to R1
D1(config-if)# no switchport
D1(config-if)# ip address 10.10.10.2 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
```

**Step 2.** Enable routing, as shown in Example 4-20. Ensure IPv4 routing is enabled with the `ip routing` global configuration command.

**Example 4-20** Enable Routing

```
D1(config)# ip routing
D1(config)#
```
Step 3. Configure routing. Configure the OSPF routing protocol to advertise the VLAN 10 and VLAN 20 networks, along with the network that is connected to R1, as shown in Example 4-21. Notice the message informing you that an adjacency has been established with R1.

**Example 4-21  Configure Routing**

```bash
D1(config)# router ospf 10
D1(config-router)# network 192.168.10.0 0.0.0.255 area 0
D1(config-router)# network 192.168.20.0 0.0.0.255 area 0
D1(config-router)# network 10.10.10.0 0.0.0.3 area 0
D1(config-router)# ^Z
D1#
```

*Sep 17 13:52:51.163: %OSPF-5-ADJCHG: Process 10, Nbr 10.20.20.1 on
  GigabitEthernet1/0/1 from LOADING to FULL, Loading Done
D1#

Step 4. Verify routing. Verify the routing table on D1, as shown in Example 4-22. Notice that D1 now has a route to the 10.20.20.0/24 network.

**Example 4-22  Verify Routing**

```bash
D1# show ip route | begin Gateway
Gateway of last resort is not set
    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
      C         10.10.10.0/30 is directly connected, GigabitEthernet1/0/1
      L         10.10.2.32 is directly connected, GigabitEthernet1/0/1
    0     10.20.20.0/24 [110/2] via 10.10.10.1, 00:00:06, GigabitEthernet1/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
      C         192.168.10.0/24 is directly connected, Vlan10
      L         192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
      C         192.168.20.0/24 is directly connected, Vlan20
      L         192.168.20.1/32 is directly connected, Vlan20
D1#
```

Step 5. Verify connectivity. At this time, PC1 and PC2 are able to ping the server connected to R1, as shown in Example 4-23.

**Example 4-23  Verify Connectivity**

```bash
C:\Users\PC1> ping 10.20.20.254
Ping request echo request timed out.
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
```
Chapter 4: Inter-VLAN Routing

Packet Tracer—Configure Layer 3 Switching and Inter-VLAN Routing (4.3.8)
In this Packet Tracer activity, you configure Layer 3 switching and Inter-VLAN routing on a Cisco 3560 switch.

Troubleshoot Inter-VLAN Routing (4.4)
In this section, you learn how to troubleshoot issues in an inter-VLAN routing environment.

Common Inter-VLAN Issues (4.4.1)
By now, you know that when you configure and verify, you must also be able to troubleshoot. This section discusses some common network problems associated with inter-VLAN routing.

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, use the list in Table 4-4 for other common reasons why inter-VLAN connectivity may fail.
### Table 4-4  Common Inter-VLAN Issues

<table>
<thead>
<tr>
<th>Issue Type</th>
<th>How to Fix</th>
<th>How to Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing VLANs</td>
<td>■ Create (or re-create) the VLAN if it does not exist. ■ Ensure host port is assigned to the correct VLAN.</td>
<td>show vlan [brief]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show interfaces switchport ping</td>
</tr>
<tr>
<td>Switch Trunk Port Issues</td>
<td>■ Ensure trunks are configured correctly. ■ Ensure port is a trunk port and enabled.</td>
<td>show interfaces trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show running-config</td>
</tr>
<tr>
<td>Switch Access Port Issues</td>
<td>■ Assign correct VLAN to access port. ■ Ensure port is an access port and enabled. ■ Host is incorrectly configured in the wrong subnet.</td>
<td>show interfaces switchport</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show running-config interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ipconfig</td>
</tr>
<tr>
<td>Router Configuration Issues</td>
<td>■ Router subinterface IPv4 address is incorrectly configured. ■ Router subinterface is assigned to the VLAN ID.</td>
<td>show ip interface brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show interfaces</td>
</tr>
</tbody>
</table>

### Troubleshoot Inter-VLAN Routing Scenario (4.4.2)

Next, examples of some of these inter-VLAN routing problems are covered in more detail. The topology in Figure 4-8 will be used for all of these issues.

![Figure 4-8  Inter-VLAN Routing Troubleshooting Topology](image-url)
The VLAN and IPv4 addressing information for R1 is shown in Table 4-5.

Table 4-5  Router R1 Subinterfaces

<table>
<thead>
<tr>
<th>Subinterface</th>
<th>VLAN</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/0/0.10</td>
<td>10</td>
<td>192.168.10.1/24</td>
</tr>
<tr>
<td>G0/0/0.20</td>
<td>20</td>
<td>192.168.20.1/24</td>
</tr>
<tr>
<td>G0/0/0.30</td>
<td>99</td>
<td>192.168.99.1/24</td>
</tr>
</tbody>
</table>

Missing VLANs (4.4.3)

An inter-VLAN connectivity issue could be caused by a missing VLAN. The VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link.

For example, PC1 is currently connected to VLAN 10, as shown in the show vlan brief command output in Example 4-24.

Example 4-24  Verify VLAN for PC1

```
S1# show vlan brief
VLAN  Name               Status          Ports
----  -------------------  ---------------------
  1    default             active        Fa0/2, Fa0/3, Fa0/4, Fa0/7
               Fa0/8, Fa0/9, Fa0/10, Fa0/11
               Fa0/12, Fa0/13, Fa0/14, Fa0/15
               Fa0/16, Fa0/17, Fa0/18, Fa0/19
               Fa0/20, Fa0/21, Fa0/22, Fa0/23
               Fa0/24, Gi0/1, Gi0/2
 10    LAN10               active        Fa0/6
 20    LAN20               active        
 99    Management         active        
 1002  fddi-default       act/unsup     
 1003  token-ring-default act/unsup     
 1004  fddinet-default    act/unsup     
 1005  trnet-default      act/unsup     
S1#  
```

Now assume that VLAN 10 is accidently deleted, as shown in Example 4-25.
Example 4-25  VLAN 10 Is Deleted

S1(config)# no vlan 10
S1(config)# do show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  default</td>
<td>active</td>
<td>Fa0/2, Fa0/3, Fa0/4, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>20  LAN20</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>99  Management</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

Notice that VLAN 10 is now missing from the output in Example 4-25. Also notice that port Fa0/6 has not been reassigned to the default VLAN. The reason is because when you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN or re-create the missing VLAN.

Use the `show interface interface-id switchport` command to verify the VLAN membership, as shown in Example 4-26.

Example 4-26  Verify an Interface's VLAN Membership

S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)

Re-creating the missing VLAN would automatically reassign the hosts to it, as shown in Example 4-27.
Example 4-27  Attempt to Re-create and Verify VLAN 10

```
S1(config)# vlan 10
S1(config-vlan)# do show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>active</td>
<td>Fa0/2, Fa0/3, Fa0/4, Fa0/7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/8, Fa0/9, Fa0/10, Fa0/11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/12, Fa0/13, Fa0/14, Fa0/15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/16, Fa0/17, Fa0/18, Fa0/19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/20, Fa0/21, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/24, Gi0/1, Gi0/2</td>
</tr>
</tbody>
</table>

20  LAN20        active  Fa0/6
99  Management   active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
```

Notice that the VLAN has not been created as expected. The reason is because you must exit from VLAN sub-configuration mode to create the VLAN, as shown in Example 4-28.

Example 4-28  Exit VLAN Configuration Mode and Then Re-create and Verify VLAN

```
S1(config-vlan)# exit
S1(config)# vlan 10
S1(config)# do show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>active</td>
<td>Fa0/2, Fa0/3, Fa0/4, Fa0/7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/8, Fa0/9, Fa0/10, Fa0/11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/12, Fa0/13, Fa0/14, Fa0/15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/16, Fa0/17, Fa0/18, Fa0/19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/20, Fa0/21, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/24, Gi0/1, Gi0/2</td>
</tr>
</tbody>
</table>

10  VLAN0010     active  Fa0/6
20  LAN20        active
99  Management   active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
S1(config)#
```
Now notice that the VLAN is included in the list and that the host connected to Fa0/6 is on VLAN 10.

**Switch Trunk Port Issues (4.4.4)**

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

For example, assume PC1 was able to connect to hosts in other VLANs until recently. A quick look at maintenance logs revealed that the S1 Layer 2 switch was recently accessed for routine maintenance. Therefore, you suspect the problem may be related to that switch.

On S1, verify that the port connecting to R1 (i.e., F0/5) is correctly configured as a trunk link using the `show interfaces trunk` command, as shown in Example 4-29.

**Example 4-29  Verify Trunking**

```
S1# show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q trunking 1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```

The Fa0/5 port connecting to R1 is mysteriously missing from the output. Verify the interface configuration using the `show running-config interface fa0/5` command, as shown in Example 4-30.

**Example 4-30  Verify Interface Configuration**

```
S1# show running-config interface fa0/5
Building configuration...
Current configuration : 96 bytes
!
interface FastEthernet0/5
description Trunk link to R1
switchport mode trunk
shutdown
end
S1#
```
As you can see, the port was accidently shut down. To correct the problem, reenable the port and verify the trunking status, as shown in Example 4-31.

**Example 4-31  Reenable and Verify the Port**

```
S1(config)# interface fa0/5
S1(config-if)# no shut
S1(config-if)#
*Mar  1 04:46:44.153: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
S1(config-if)#
*Mar  1 04:46:47.962: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
S1(config-if)#
S1(config-if)# do show interface trunk
Port        Mode             Encapsulation     Status     Native vlan
Fa0/1       on               802.1q             trunking    1
Fa0/5       on               802.1q             trunking    1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/5       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
S1(config-if)#
```

To reduce the risk of a failed inter-switch link disrupting inter-VLAN routing, redundant links and alternate paths should be part of the network design.

**Switch Access Port Issues (4.4.5)**

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

Assume PC1 has the correct IPv4 address and default gateway but is not able to ping its own default gateway. PC1 is supposed to be connected to a VLAN 10 port.

Verify the port configuration on S1 using the `show interfaces interface-id switchport` command, as shown in Example 4-32.
Example 4-32  Verify the Port Configuration

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

The Fa0/6 port has been configured as an access port, as indicated by “static access”. However, it appears that it has not been configured to be in VLAN 10. Verify the configuration of the interface, as shown in Example 4-33.

Example 4-33  Verify the Port Configuration in the Running-Config

```
S1# show running-config interface fa0/6
Building configuration...
Current configuration : 87 bytes
!
interface FastEthernet0/6
description PC-A access port
switchport mode access
end
S1#
```

Assign port Fa0/6 to VLAN 10 and verify the port assignment, as shown in Example 4-34.

Example 4-34  Assign the VLAN to the Port and Verify the Configuration

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport access vlan 10
S1(config-if)#
S1(config-if)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)

PC1 is now able to communicate with hosts on other VLANs.

**Router Configuration Issues (4.4.6)**

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations. For instance, an incorrect IP address was configured or the wrong VLAN ID was assigned to the subinterface.

For example, R1 should be providing inter-VLAN routing for users in VLANs 10, 20, and 99. However, users in VLAN 10 cannot reach any other VLAN.

You verified the switch trunk link and all appears to be in order. Verify the subinterface status using the `show ip interface brief` command, as shown in Example 4-35.

**Example 4-35  Verify the Status of the Subinterfaces**

```
R1# show ip interface brief
Interface           IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down  down
GigabitEthernet0/0/1   unassigned      YES unset  up                       up
Gi0/0/1.10            192.168.10.1    YES manual up                   up
Gi0/0/1.20            192.168.20.1    YES manual up                   up
Gi0/0/1.99            192.168.99.1    YES manual up                   up
Serial0/1/0           unassigned      YES unset  administratively down  down
Serial0/1/1           unassigned      YES unset  administratively down  down
R1#
```

The subinterfaces have been assigned the correct IPv4 addresses, and they are operational.

Verify which VLANs each of the subinterfaces is on. To do so, the `show interfaces` command is useful, but it generates a great deal of additional unrequired output.
The command output can be reduced using IOS command filters as shown in Example 4-36.

**Example 4-36  Verify the VLANs Configured on Each Subinterface**

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

The pipe symbol (|) along with some select keywords is a useful method to help filter command output. In this example, the keyword **include** was used to identify that only lines containing the letters “Gig” or “802.1Q” will be displayed. Because of the way the **show interface** output is naturally listed, using these filters produces a condensed list of interfaces and their assigned VLANs.

Notice that the G0/0/1.10 interface has been incorrectly assigned to VLAN 100 instead of VLAN 10. This is confirmed by looking at the configuration of the R1 GigabitEthernet 0/0/1.10 subinterface, as shown in Example 4-37.

**Example 4-37  Verify the Configuration of the Subinterface in the Running-Config**

```
R1# show running-config interface g0/0/1.10
Building configuration...
Current configuration : 146 bytes
!
interface GigabitEthernet0/0/1.10
    description Default Gateway for VLAN 10
    encapsulation dot1Q 100
    ip address 192.168.10.1 255.255.255.0
end
R1#
```

To correct this problem, configure subinterface G0/0/1.10 to be on the correct VLAN using the **encapsulation dot1q** 10 subinterface configuration mode command, as shown in Example 4-38.
Example 4-38  Correct and Verify the Subinterface Configuration

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# end
R1#
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
GigabitEthernet0/0/1.20 is up, line protocol is up
    Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
R1#
```

When the subinterface has been assigned to the correct VLAN, it is accessible by devices on that VLAN, and the router can perform inter-VLAN routing.

With verification, router configuration problems are quickly addressed, allowing inter-VLAN routing to function properly.

Check Your Understanding—Troubleshoot Inter-VLAN Routing (4.4.7)
Refer to the online course to complete this activity.

Packet Tracer—Troubleshoot Inter-VLAN Routing (4.4.8)
In this Packet Tracer activity, you complete the following objectives:

- Part 1: Locate Network Problems
- Part 2: Implement the Solution
- Part 3: Verify Network Connectivity

Lab—Troubleshoot Inter-VLAN Routing (4.4.9)
In this lab, you complete the following objectives:

- Part 1: Build the Network and Load Device Configurations
- Part 2: Troubleshoot the Inter-VLAN Routing Configuration
- Part 3: Verify VLAN Configuration, Port Assignment, and Trunking
- Part 4: Test Layer 3 Connectivity
Summary (4.5)

The following is a summary of each section in the chapter:

**Inter-VLAN Routing Operation**

Hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services. Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN. Three options include legacy, router-on-a-stick, and a Layer 3 switch using SVIs. Legacy used a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router. The router-on-a-stick inter-VLAN routing method requires only one physical Ethernet interface to route traffic between multiple VLANs on a network. A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. The router interface is configured using subinterfaces to identify routable VLANs. The configured subinterfaces are software-based virtual interfaces associated with a single physical Ethernet interface. The modern method is Inter-VLAN routing on a Layer 3 switch using SVIs. The SVI is created for a VLAN that exists on the switch. The SVI performs the same functions for the VLAN as a router interface. It provides Layer 3 processing for packets being sent to or from all switch ports associated with that VLAN.

**Router-on-a-Stick Inter-VLAN Routing**

To configure a switch with VLANs and trunking, complete the following steps: create and name the VLANs, create the management interface, configure access ports, and configure trunking ports. The router-on-a-stick method requires a subinterface to be created for each VLAN to be routed. A subinterface is created using the `interface interface_id.subinterface_id` global configuration mode command. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, the physical interface must be enabled using the `no shutdown` interface configuration command. From a host, verify connectivity to a host in another VLAN using the `ping` command. Use `ping` to verify connectivity with the host and the switch. To verify and troubleshoot, use the `show ip route`, `show ip interface brief`, `show interfaces`, and `show interfaces trunk` commands.

**Inter-VLAN Routing Using Layer 3 Switches**

Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Capabilities of a Layer 3 switch include routing from one VLAN
Chapter 4: Inter-VLAN Routing

131

to another using multiple switched virtual interfaces (SVIs) and converting a Layer 2 switch port to a Layer 3 interface (that is, a routed port). To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same `interface vlan vlan-id` command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs. To configure a switch with VLANS and trunking, complete the following steps: create the VLANS, create the SVI VLAN interfaces, configure access ports, and enable IP routing. From a host, verify connectivity to a host in another VLAN using the `ping` command. Next, verify connectivity with the host using the `ping` Windows host command. VLANs must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured. A routed port is created on a Layer 3 switch by disabling the switch port feature on a Layer 2 port that is connected to another Layer 3 device. The interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch. To configure a Layer 3 switch to route with a router, follow these steps: configure the routed port, enable routing, configure routing, verify routing, and verify connectivity.

Troubleshoot Inter-VLAN Routing

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues such as missing VLANs, switch trunk port issues, switch access port issues, and router configuration issues. A VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link. Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, a misconfigured switch port could be caused when the connecting router port is not assigned to the correct VLAN. With a router-on-a-stick solution, the most common cause is a misconfigured trunk port. When a problem is suspected with a switch access port configuration, use `ping` and `show interfaces interface-id switch-port` commands to identify the problem. Router configuration problems with router-on-a-stick configurations are usually related to subinterface misconfigurations. Verify the subinterface status using the `show ip interface brief` command.

Packet Tracer—Inter-VLAN Routing Challenge (4.5.1)

In this activity, you demonstrate and reinforce your ability to implement inter-VLAN routing, including configuring IP addresses, VLANs, trunking, and subinterfaces.

Lab—Implement Inter-VLAN Routing (4.5.2)

In this lab, you complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
Practice

The following activities provide practice with the topics introduced in this chapter. The Labs are available in the companion *Switching, Routing, and Wireless Essentials Labs and Study Guide (CCNAv7)* (ISBN 9780136634386). The Packet Tracer Activity instructions are also in the Labs & Study Guide. The PKA files are found in the online course.

**Labs**
- Lab 4.2.8: Configure Router-on-a-Stick Inter-VLAN Routing
- Lab 4.4.9: Troubleshoot Inter-VLAN Routing
- Lab 4.5.2: Implement Inter-VLAN Routing

**Packet Tracer Activities**
- Packet Tracer 4.2.7: Configure Router-on-a-Stick Inter-VLAN Routing
- Packet Tracer 4.3.8: Configure Layer 3 Switching and Inter-VLAN Routing
- Packet Tracer 4.4.8: Troubleshoot Inter-VLAN Routing
- Packet Tracer 4.5.1: Inter-VLAN Routing Challenge

**Check Your Understanding Questions**

Complete all the review questions listed here to test your understanding of the sections and concepts in this chapter. The appendix “Answers to the ‘Check Your Understanding’ Questions” lists the answers.
1. A router has two FastEthernet interfaces and needs to connect to four VLANs in the local network. How can this be accomplished using the fewest number of physical interfaces without unnecessarily decreasing network performance?
   A. Add a second router to handle the inter-VLAN traffic.
   B. Implement a router-on-a-stick configuration.
   C. Interconnect the VLANs via the two additional FastEthernet interfaces.
   D. Use a hub to connect the four VLANs with a FastEthernet interface on the router.

2. What distinguishes traditional legacy inter-VLAN routing from router-on-a-stick?
   A. Traditional routing is able to use only a single switch interface, whereas a router-on-a-stick can use multiple switch interfaces.
   B. Traditional routing requires a routing protocol, whereas a router-on-a-stick only needs to route directly connected networks.
   C. Traditional routing uses one port per logical network, whereas a router-on-a-stick uses subinterfaces to connect multiple logical networks to a single router port.
   D. Traditional routing uses multiple paths to the router and therefore requires STP whereas router-on-a-stick does not provide multiple connections and therefore eliminates the need for STP.

3. Subinterface G0/1.10 on R1 must be configured as the default gateway for the VLAN 10 192.168.10.0/24 network. Which command should be configured on the subinterface to enable inter-VLAN routing for VLAN 10?
   A. encapsulation dot1q 10
   B. encapsulation vlan 10
   C. switchport mode access
   D. switchport mode trunk

4. What is important to consider while configuring the subinterfaces of a router when implementing inter-VLAN routing?
   A. The IP address of each subinterface must be the default gateway address for each VLAN subnet.
   B. The no shutdown command must be given on each subinterface.
   C. The physical interface must have an IP address configured.
   D. The subinterface numbers must match the VLAN ID number.
5. What are the steps that must be completed in order to enable inter-VLAN routing using router-on-a-stick?
   A. Configure the physical interfaces on the router and enable a routing protocol.
   B. Create the VLANs on the router and define the port membership assignments on the switch.
   C. Create the VLANs on the switch to include port membership assignment and enable a routing protocol on the router.
   D. Create the VLANs on the switch to include port membership assignment and configure subinterfaces on the router matching the VLANs.

6. What two statements are true regarding the use of subinterfaces for inter-VLAN routing? (Choose two.)
   A. Fewer router Ethernet ports required than in traditional inter-VLAN routing
   B. Less complex physical connection than in traditional inter-VLAN routing
   C. More switch ports required than in traditional inter-VLAN routing
   D. Simpler Layer 3 troubleshooting than with traditional inter-VLAN routing
   E. Subinterfaces have no contention for bandwidth

7. Which router-on-a-stick command and prompt on R1 correctly encapsulates 802.1Q traffic for VLAN 20?
   A. R1(config-if)# encapsulation 802.1q 20
   B. R1(config-if)# encapsulation dot1q 20
   C. R1(config-subif)# encapsulation 802.1q 20
   D. R1(config-subif)# encapsulation dot1q 20

8. What are two disadvantages of using the router-on-a-stick inter-VLAN routing method in a large network? (Choose two.)
   A. A dedicated router is required.
   B. It does not scale well.
   C. It requires multiple physical interfaces on a router.
   D. It requires subinterfaces to be configured on the same subnets.
   E. Multiple SVIs are needed.

9. What is a characteristic of a routed port on a Layer 3 switch? (Choose two.)
   A. It requires the switchport mode access interface config command.
   B. It requires the no switchport interface config command.
   C. It requires the switchport access vlan vlan-id interface config command.
   D. It supports trunking.
10. What are two advantages of using a Layer 3 switch with SVIs for inter-VLAN routing? (Choose two.)

A. A router is not required.
B. It switches packets faster than using the router-on-a-stick method.
C. SVIs can be bundled into EtherChannels.
D. SVIs can be divided using subinterfaces.
E. SVIs eliminate the need for a default gateway in the hosts.
SYMBOLS

4G/5G (cellular broadband), 352–353
802.1D standard, 140, 152, 161
802.1D-2004 standard, 162
802.1IQ trunk ports, 64, 70–71
802.1W standard, 152, 162
802.1X standard, 286–287
802.3ad standard, 171–172
802.11 standards, 353–354
802.11a standard, 353
802.1lac standard, 354
802.11ax standard, 354
802.11b standard, 354
802.11g standard, 354
802.11n standard, 354

A

A flag (Address Autoconfiguration flag), 226, 231
AAA (authentication, authorization and accounting), 283–286
access control, 281–287
802.1X standard, 286–287
AAA components, 283
accounting, 285–286
authentication, 283–285
authorization, 285
local password authentication, 281–282
access points. See APs (wireless access points)
access ports, troubleshooting, 125–127
accounting, 285–286
active mode, 369–370
active routers, 265–266, 268–269
AD (administrative distance), 470, 479–480, 517–518
ad hoc mode, 362–363
Address Autoconfiguration flag (A flag), 226
address prefix command, 246
address spoofing attacks, 289, 303
adjacency table, 458
AES (Advanced Encryption Standard), 386–387
aging, 319–320
algorithms, 484
alternate (blocked) ports, 156
AMP (advanced malware protection), 278
antennas, wireless, 360–362
application-specific-integrated circuits (ASICs), 48
APs (wireless access points), 353, 358–360
association with wireless clients, 367–368
discover modes, 368–369
discovery, 368–369
MAC functions, 371
rogue APs, 379, 381, 414
splitting traffic, 436–438
viewing information, 415–416
ARP attacks, 289, 300–302
mitigation techniques, 301, 332–335
ARP poisoning, 289, 301–302
mitigation techniques, 332–335
ARP spoofing, 289, 301
mitigation techniques, 332–335
AS (autonomous system), 482
ASICs (application-specific-integrated circuits), 48
assigning GUAs (global unicast addresses), 226–227
associating wireless clients and APs, 367–368
attacks
common types of, 277
LAN attacks, 292–306
address spoofing attacks, 303
ARP attacks, 300–302
CDP reconnaissance, 305–306
DHCP attacks, 296–300, 329
STP manipulation attacks, 303–305
VLAN attacks, 293–295, 327
MAC address table attacks, 290–292
on WLANs, 379–382
DoS (Denial of Service) attacks, 380
man-in-the-middle attacks, 381–382
rogue APs, 381
types of, 379
authentication
local password authentication, 281–282
for SSH servers, configuring, 23
types of, 283–285
for WLANs, 385–387
enterprise authentication methods, 388–389
WPA3, 389–390
authorization, 285
automatic buffering in store-and-forward switching, 49
automatically installed host routes, 522
auto-MDIX (automatic medium-dependent interface crossover), 13–14
autonegotiate, 19
autonegotiation protocols, 179–180
autonomous APs, 359
autonomous system (AS), 482

B
backup routers, 266
Basic Service Area (BSA), 364
Basic Service Set (BSS), 364–365
Basic Service Set Identifier (BSSID), 365
begin filter, 35, 466
best paths, 448
determining, 484–486
IPv4 addressing example, 449
IPv6 addressing example, 449
best practices for endpoint security, 278–279
BGP (Border Gateway Protocol), 482
BIDs (bridge IDs), 149
default, 151
root port election from, 157
binding DHCPv6 pools to interface, 241–242, 246–247
blacklisting, 280
BLE (Bluetooth Low Energy), 352
blocked (alternate) ports, 156
blocking state, 141, 147, 159
Bluetooth, 352
Bluetooth Basic Rate/Enhanced Rate (BR/EDR), 352
Bluetooth Low Energy (BLE), 352
BOOT environment variable, 3, 6
boot loader software, 2, 6–7
boot sequence for switches, 2–3
boot system command, 3
BOOT=flash command, 7
Border Gateway Protocol (BGP), 482
BPDU filter, 162
BPDU Guard, 165–166, 305, 336
configuring, 338–339
BPDUUs (Bridge Protocol Data Units), 149
BR/EDR (Bluetooth Basic Rate/Enhanced Rate), 352
bridge IDs. See BIDs (bridge IDs)
bridge priority, 149
bring your own devices (BYODs), 278
broadcast domains, 52–53
broadcast frames, 142
broadcast storms, 143–145
BSA (Basic Service Area), 364

C
CAM (content addressable memory), 47
Canonical Format Identifier (CFI), 70
CAPWAP, 370–373
carrier sense multiple access with collision avoidance
(CSMA/CA), 367
CDP (Cisco Discovery Protocol), 305–306
cdp enable command, 306
cdp run command, 306
CEF (Cisco Express Forwarding), 458
cellular broadband, 352–353
CFI (Canonical Format Identifier), 70
channel management, 373–379
canalsel, 375–377
cellular channel saturation, 373–375
planning WLAN deployment, 377–379
channel-group command, 191
child routes, 478
Cisco Discovery Protocol (CDP), 305–306
Cisco ESA (Email Security Appliance), 279–280
Cisco Express Forwarding (CEF), 458
Cisco Identity Services Engine (ISE), 278
Cisco IOS helper addresses, 212
Cisco Talos Intelligence Group, 279
Cisco WSA (Web Security Appliance), 280–281
class of service (CoS), 72
collision domains, 51–52
collisions, 17, 18
cmd history feature, 36
Common Spanning Tree (CST), 161
configuring
BPDU Guard, 338–339
DAI (Dynamic ARP Inspection), 333–335
default routes, troubleshooting, 533–539
DHCP scope, 428–430
DHCP snooping, 331–332
DHCPv4 clients, 214–215
DHCPv4 servers, 204–213
disabling, 210
example, 206–207
relay agents, 210–213
steps in, 205–206
verifying, 207–210
DHCPv6 pools, 241, 246–247
crypto key zeroize rsa command

DHCPv6 servers, 240–254
DHCPv6 relay agents, 252–254
router roles, 240
stateful DHCPv6 clients, 248–250
stateful DHCPv6 servers, 245–248
stateless DHCPv6 clients, 243–245
stateless DHCPv6 servers, 240–243
verification commands, 250–251
DTP (dynamic trunking protocol), 89–90, 32
EtherChannel, 18
GUAs (global unicast addresses), 224–225
LACP (Link Aggregation Control Protocol), 18
Layer 3 switches, 11
for routing, 117–119
LLAs (link-local addresses), 224–226, 243–244, 249
loop-free topology with STP, 148–158
alternate port election, 156
designated port election, 153–155
root bridge election, 150–152
root port election, 152–153, 156–158
native VLAN, 327–328
PortFast, 336–338
router-on-a-stick
subinterfaces, 107–108
troubleshooting, 127–129
VLAN trunks, 105–107
VLANs (Virtual LANs), 105–107
routers, 25–29, 459–467
commands for, 459–461
dual-stack topology, 27
filtering show command output, 466–467
interface configuration, 27–28
IPv4 loopback interfaces, 28–29
topology, 459
verification commands, 461–465
SSH (Secure Shell), 22–24
static routes
default routes, 514–515
floating, 518–520
host routes, 523, 524
IPv4 directly connected, 505–506
IPv4 fully specified, 507–509
IPv4 next-hop, 503–504
IPv6 directly connected, 506–507
IPv6 fully specified, 509–510
IPv6 next-hop, 504–505
troubleshooting, 533–539
switch ports, 11–20
auto-MDIX, 13–14
duplex communication, 11–12
input and output errors, 17–18
network access layer issues, 15–17
physical layer, 12–13
troubleshooting network access layer issues, 18–20
verification commands, 14
verifying, 14–15
switches, 2–10
boot sequence, 2–3
boot system command, 3
LED indicators, 3–5
recovering from system crash, 6–7
SVI configuration, 8–10
VLAN trunks, 83–87
commands, 83
eXample, 83–84
resetting to default, 86–87
for router-on-a-stick, 105–107
verifying, 85
VLANs (Virtual LANs), 73–82
changing port membership, 81–82
creation commands, 75
creation example, 75
data and voice VLANs, 78–79
deleting, 82
port assignment commands, 76–77
port assignment example, 77–78
ranges on Catalyst switches, 73–75
for router-on-a-stick, 105–107
verifying, 79–80
WLANs (Wireless LANs)
basic configuration on WLC, 412–420
remote site configuration, 398–412
WPA2 enterprise configuration on WLC, 421–433
congestion, 52
alleviating, 53–54
connected mode, 372
connectivity
router-on-a-stick, verifying, 108–109
static and default routes, troubleshooting, 536–539
WLAN clients, troubleshooting, 435–436
content addressable memory (CAM), 47
controller-based APs, 359–360, 412
converged, 458
CoS (class of service), 72
CoS priority value, 72
cost, 485
CPU subsystem, 2
CRC errors, 17–18
crypto key generate rsa command, 22–23
crypto key zeroize rsa command, 23
CSMA/CA (carrier sense multiple access with collision avoidance), 367
CST (Common Spanning Tree), 161
cut-through switching, 49–51

D
DAD (Duplicate Address Detection), 234
DAI (Dynamic ARP Inspection), 289, 301, 332–335
configuring, 333–335
guidelines, 333–334
data breaches, 277
data interception, 379
data structures, 483
data VLANs, 64
configuring, 78–79
Datagram Transport Layer Security (DTLS), 370, 372
DDoS (Distributed Denial of Service), 277
default bridge IDs (BIDs), 151
default gateway
configuring for switch management interface, 10
limitations, 262–263
default port costs, 152
default routes, 451, 467, 475–476, 496, 513–516
configuring, 514–515
troubleshooting, 533–539
commands for, 534–536
connectivity problems, 536–539
network changes, 534
verifying, 515–516
when to use, 513–514
default static routes. See default routes
default VLANs, 63–64
default-router command, 205–206
delete flash:vlan.dat command, 82
delete vlan.dat command, 82
deleting VLANs (Virtual LANs), 82
Denial of Service (DoS) attacks, 379–380
designated ports, 153–155
Device Provisioning Protocol (DPP), 390
DHCP (Dynamic Host Configuration Protocol), 200
DHCP Acknowledgment (DHCPACK), 203–204
DHCP attacks, 289, 296–300, 329
mitigation techniques, 296, 329–332
DHCP Discover (DHCPDISCOVER), 202
DHCP messages, 296
DHCP Offer (DHCPOFFER), 202
DHCP Request (DHCPREQUEST), 202–203
DHCP scope, configuring, 428–430
DHCP snooping, 289, 296, 329–332
configuring, 331–332
steps in, 330
verifying, 332
DHCP snooping binding table, 329
DHCP spoofing, 289, 297–300, 329
DHCP starvation, 289, 296, 329
DHCPv4, 200–204
operational overview, 201
DHCPv4 clients, 200–201
configuring, 214–215
leases
obtaining, 201–203
renewing, 203–204
steps in, 205–206
verifying, 207–210
operational overview, 201
DHCPv4 relay agents, 210–213
DHCPv4 servers, 200–201
configuring, 204–213
disabling, 210
example, 206–207
relay agents, 210–213
steps in, 205–206
verifying, 207–210
operational overview, 201
DHCPv6, 224
operational overview, 234–236
stateful DHCPv6
enabling, 239
operational overview, 238–239
stateless DHCPv6
enabling, 237–238
operational overview, 236–237
DHCPv6 ADVERTISE unicast messages, 236
DHCPv6 clients, 240
DHCPv6 INFORMATION-REQUEST messages, 236
DHCPv6 relay agents, 240
DHCPv6 REQUEST messages, 236
DHCPv6 servers, 240
configuring, 240–254
DHCPv6 relay agents, 252–254
router roles, 240
stateful DHCPv6 clients, 248–250
stateful DHCPv6 servers, 245–248
stateless DHCPv6 clients, 243–245
stateless DHCPv6 servers, 240–243
verification commands, 250–251
DHCPv6 SOLICIT messages, 235–236
dir flash: command, 7
directional antennas, 360
directly connected interfaces, 450
directly connected networks, 450
  packet forwarding to, 452
  in routing tables, 470–471
  verifying, 29–36
    command history feature, 36
    filtering show command output, 34–35
    interface configuration, 32
    interface status, 30–31
    interface verification commands, 30
    IPv6 link local and multicast addresses, 31
    routes, 32–33
  directly connected static routes, 497
    IPv4, 505–506
    IPv6, 506–507
  Direct-Sequence Spread Spectrum (DSSS), 373–374
  disabled state, 160
  disabling
    DHCPv4 servers, 210
    unused ports, 314–315
  discarding state, 163
  distance, 485
  distance vector routing protocols, 482
  Distributed Denial of Service (DDoS), 277
  distribution system (DS), 365
  dns-server command, 205–206
  domain-name command, 205–206
  DoS (Denial of Service) attacks, 379–380
  DPP (Device Provisioning Protocol), 390
  dropped packets, 453
  DS (distribution system), 365
  DSSS (Direct-Sequence Spread Spectrum), 373–374
  DTLS (Datagram Transport Layer Security), 370, 372
  DTP (dynamic trunking protocol), 87–90
    comparison with EtherChannel, 189
    configuration results, 89–90
    configuring, 327–328
    negotiated interface modes, 89
    operational overview, 88
    verifying, 90
  dual-stack topology, 27, 499
  duplex command, 12
  duplex communication, 11–12
  duplex mismatch, 20
  Duplicate Address Detection (DAD), 234
  Dynamic ARP Inspection. See DAI (Dynamic ARP Inspection)
  Dynamic Host Configuration Protocol. See DHCP
    (Dynamic Host Configuration Protocol)
  dynamic routing protocols, 450
  best paths, 484–486
  comparison with static routes, 481–482
  components of, 483–484
  evolution of, 482–483
  load balancing, 485–487
  purpose of, 483–484
  in routing tables, 474–475
  when to use, 481
  dynamic trunking protocol. See DTP (dynamic trunking protocol)

E

EAP (Extensible Authentication Protocol), 386, 389
  edge routers, 513
  EGP (Exterior Gateway Protocol), 482
egress, 46
egress ports, 46
  EIGRP (Enhanced Interior Gateway Routing Protocol), 450, 482, 485
  electing
    alternate (blocked) ports, 156
    designated ports, 153–155
    root bridge, 150–152
    root ports, 152–153, 156–158
  email security appliance (ESA), 278–280
  enabling
    IPv6 routing, 230, 241, 243, 246, 249
    port security, 316–317
    SLAAC (Stateless Address Autoconfiguration), 229–230
    SSH version 2, 23–24
    stateful DHCPv6, 239
    stateless DHCPv6, 237–238
  encapsulation, 452
  encapsulation dot1q command, 107, 128
  encryption
    with DTLS, 372
    for WLANs, 387–388
  endpoint security, 277–281
    best practices, 278–279
    Cisco ESA, 279–280
    Cisco WSA, 280–281
    common types of attacks, 277
    network security devices, 278
  end-to-end packet forwarding, 453–456
  Enhanced Interior Gateway Routing Protocol (EIGRP), 450, 482, 485

...
enterprise authentication methods for WLANs, 388–389

equal cost load balancing, 486
equal-cost paths, root port election from, 156–158
erase startup-config command, 82
error checking in store-and-forward switching, 49
error-disabled state, 322–324

errors
input and output, 17–18
types of, 17

ESA (email security appliance), 278–280

ESA (Extended Service Area), 365

ESS (Extended Service Set), 365

EtherChannel, 177–178
advantages of, 177–178
configuring, 183–185
implementation restrictions, 178–179
LACP (Link Aggregation Control Protocol), 181–183
link aggregation, 176
PAgP (Port Aggregation Protocol), 180–181
troubleshooting, 188–192
verifying, 186–188

EUI-64 (Extended Unique Identifier method), 233

examples
assign VLAN to port and verify configuration, 126–127
assigning port to VLAN, 78
basic network setup, 403
basic router configuration, 26
begin filter, 35
bind DHCPv6 pool to interface, 242, 247
checking EtherChannel status, 190
checking protocol status, 16
checking with IOS supports SSH, 22
child routes in routing table, 478
Cisco IOS DHCPv4 server configuration, 207
configuration to mitigate VLAN hopping attacks, 328
configure access ports, 106, 115
configure additional DHCP information, 241
configure banner, 26
configure boot image, 7
configure DHCPv6 pool, 246–247
configure IP domain, 22
configure routed port, 117
configure routing, 118
configure trunking ports, 106
configure user authentication, 23
configure VTY lines, 23
configuring and verifying BPDU Guard, 338–339
configuring and verifying IPv6 static host route with link-local as next-hop, 524
counters and statistics, 16–17
interface verification, 15
ip helper-address command, 212
ipconfig /all command, 213
ipconfig /release command, 211
ipconfig /renew command, 212
IPV4 and IPV6 floating static route configuration, 519
IPV4 and IPV6 routing tables, 519–520
IPV4 and IPV6 static host route configuration, 523
IPV4 default route in routing table, 516
IPV4 default static route, 515
IPV4 directly connected static route configuration, 505
IPV4 fully specified static route configuration, 508
IPV4 next-hop static route configuration, 504
IPV6 default route in routing table, 516
IPV6 default static route, 515
IPV6 directly connected static route configuration, 506
IPV6 fully specified static route, 509
IPV6 next-hop static route configuration, 504
IPV6 routing table structure, 478–479
LACP configuration, 185
local IPV4 and IPV6 routes, 522
log messages on R1, 521
log messages show port security violation, 323
login via SSH, 25
loopback interface configuration, 29
MAC address table, 290
macof utility output on Linux host, 292
modifying port security to restrict, 322
normal range VLANs, 74
obsolete routing table with classful addressing architecture, 477
password setting on VTY lines, 282
ping command, 465
ping IPV6 address, 33
ping next-hop router, 537
ping R3 LAN from s0/1/0, 537
ping remote LAN, 537, 539
piping show run to check EtherChannel configuration, 190–191
port security command options, 317
R1 can ping R2, 501, 503
R1 cannot ping R3 LAN, 501, 503
R1 configuration, 460–461
R1 IPV4 routing table, 500, 504, 506, 509
R1 IPV6 routing table, 501, 505, 507, 510
R1 routing table, 468
R1 subinterface configuration, 108
R2 IPV4 routing table, 500
R2 IPV6 routing table, 502
R2 routing table, 468
R3 IPV4 routing table, 500
R3 IPV6 routing table, 502
re-create and verify VLAN 10, 123
reenable and verify port, 125
reenabling disabled ports, 324
remote allowed VLANs and reset native VLAN, 86
remove VLAN assignment configuration, 81
reset port to access mode, 87
router as DHCPv4 client configuration, 214–215
S2 configuration, 10
section filter, 34
setting and displaying command history, 36
show cdp neighbors command, 536
show etherchannel port-channel command, 187–188
show etherchannel summary command, 187
show interfaces command, 462–463
show interfaces etherchannel command, 188
show interfaces port-channel command, 186
show ip interface brief command, 461, 536
show ip interface command, 212, 463–464
show ip route command, 465, 535
show ipv6 interface brief command, 461–462
show ipv6 interface command, 464
show ipv6 route command, 465
show running-config interface command, 462
show running-config interface command, 462
show vlan summary command, 80
shutting down unused ports, 315
SSH configuration and VTY line setup for SSH, 282
static IPV4 and IPV6 routes, 473
switch port configuration verification, 15
testing floating static route, 520–521	traceroute command, 535
trunk configuration, 84
verify clients assigned DHCPv6 addressing, 251
verify configuration of subinterface in running-config, 128
verify connectivity, 118–119
verify details of subinterface, 111
verify DHCPv4 bindings, 208
verify DHCPv4 client configuration, 209–210
verify DHCPv4 configuration, 208
verify DHCPv4 statistics, 208–209
verify DHCPv6 pool parameters, 251
verify DTP mode, 90
verify host received IPv6 addressing information, 248
verify interface configuration, 32, 124
verify interface status, 30–31
verify interface's VLAN membership, 122
verify inter-VLAN routing by pinging from PC1, 109, 116
verify IP configuration, 10
verify IPv6 link local and multicast addresses, 31
verify new static route is installed, 539
verify port configuration, 126
verify port configuration in running-config, 126
verify R2 routing table, 538
verify router received IPv4 addressing information, 215
verify routes, 32–33
verify routing, 118
verify SSH, 25
verify SSH support, 22
verify status of subinterfaces, 127
verify subinterface IP addresses and status, 110
verify subinterfaces in routing table, 110
verify trunk is in default state, 86
verify trunk link status, 111
verify trunking, 124
verify VLAN for PC1, 121
verify VLAN removed, 82
verify VLANS configured on each subinterface, 128
verify Windows host configuration, 109, 115
verifying AP has connectivity, 416
verifying auto-MDIX setting, 14
verifying client router received GUA, 244, 249–250
verifying client router received other IPv6 addressing, 245, 250
verifying DHCP snooping, 332
verifying DHCPv6 hosts are assigned IPv6 GUA, 253
verifying EtherChannel is operational, 192
verifying floating static routes installed, 521
verifying interface as correct VLAN assignments, 80
verifying interface is in DHCPv6 relay mode, 253
verifying IPv4 and IPv6 static host routes, 523–524
verifying IPv6 addressing on interface, 230
verifying IPv6 floating static route, 520
verifying learned MAC addresses, 326
verifying maximum number of MAC addresses, 317
verifying PC received IPv6 addressing information, 253–254
verifying port is disabled, 323–324
verifying port security on all interfaces, 325
verifying port security on specific interface, 325
verifying secure MAC addresses, 326
verifying SLAAC is enabled on interface, 230
verifying trunk configuration, 85
verifying VLAN 5 interface, 425
verifying voice VLAN configuration, 73
verifying Windows host randomly generated its interface ID, 233
verifying Windows host received IPv6 addressing from DHCPv6 server, 242–243
verifying Windows host received IPv6 addressing from SLAAC, 232
viewing Windows host IPv6 link-local address, 226
VLAN 10 deleted, 122
VLAN configuration, 76
VLAN default port assignments, 64
exclude filter, 35, 466
excluding IPv4 addresses, 205
exit interface, 45
3–456, 470
extended ping command, 535
extended range VLANs, 7
Extended Service Area (ESA), 365
Extended Service Set (ESS), 365
extended system ID, 149
Extended Unique Identifier method (EUI-64), 233
Extensible Authentication Protocol (EAP), 386, 389
Exterior Gateway Protocol (EGP), 482

F

fast switching, 456–457
fast-switching cache, 456
FCS (frame check sequence), 49
FHRP (First Hop Redundancy Protocols), 262–267
default gateway limitations, 262–263
implementation options, 266–267
router failover, 265–266
router redundancy, 264–265
FHSS (Frequency-Hopping Spread Spectrum), 374
FIB (Forwarding Information Base), 458
File Transfer Protocol (FTP), 289
filtering show command output, 34–35, 466–467
firewalls, 278
firmware updates, 438–439
First Hop Redundancy Protocols. See FHRP
(First Hop Redundancy Protocols)
flash init command, 6
FlexConnect, 372–373
floating static routes, 496, 517–521
administrative distance (AD) and, 517–518
configuring, 518–520
testing, 520–521
Forward Delay timer, 158
Forwarding Information Base (FIB), 458
forwarding state, 160
fragment free switching, 50
frame check sequence (FCS), 49
frame forwarding, 46–51. See also packet forwarding
cut-through switching, 49–51
Layer 2 loops, 142–143
learn-and-forward method, 48
MAC address table, 47, 290
methods of, 291–292
operational overview, 46
store-and-forward switching, 49–50
frequency channel saturation, 373–375
Frequency-Hopping Spread Spectrum (FHSS), 374
FTP (File Transfer Protocol), 289
full-duplex, 11
fully specified static routes, 497
IPv4, 507–509
IPv6, 509–510
G

giants, 17, 18
GLBP (Gateway Load Balancing Protocol), 267
GLBP for IPv6, 267
Gobbler, 296, 329
 gratuitous ARP, 300–301
GUAs (global unicast addresses)
 assigning, 226–227
 configuring, 224–225
 RA message flags, 226–228
H

half-duplex, 11
HDLC (High-Level Data Link Control), 453
Hello timer, 158
hierarchical network addressing, 61
high port density, 54
high-performance computing (HPC) applications, 50
High-Speed WAN Interface Card (HWIC), 27
HIPSs (host-based intrusion prevention systems), 278
 home routers
 authentication, 386–387
 as DHCPv4 clients, 215
 wireless, 357–358
 hop count, 485
 hop limit, 141–142
 host routes, 521
 automatically installed, 522
 static, 523–524
 configuring, 523, 524
 verifying, 523–524
host-based intrusion prevention systems (HIPSs), 278
hotspots, 363
HPC (high-performance computing) applications, 50
HSRP (Hot Standby Router Protocol), 266–270
 operational overview, 267–268
 preemption, 268–269
 priority, 268
 states and timers, 269–270
HSRP for IPv6, 266
HWIC (High-Speed WAN Interface Card), 27
IBSS (independent basic service set), 362–363
ICMP Router Discovery Protocol (IRDP), 267
ICMPv6 Neighbor Advertisement (NA) messages, 234
ICMPv6 Neighbor Solicitation (NS) messages, 234
ICMPv6 Router Advertisement (RA) messages, 224
 message flags, 226–228
 in SLAAC, 228–229
ICMPv6 Router Solicitation (RS) messages, 232–233
IEEE (Institute of Electrical and Electronics Engineers), 355
IEEE 802.1Q header, 69–70
IGPs (Interior Gateway Protocols), 482
IGRP (Interior Gateway Routing Protocol), 482
 include filter, 34–35, 466
 independent basic service set (IBSS), 362–363
 infrastructure mode, 363
 ingress, 46
 ingress ports, 46
 initial state (HSRP), 269
 input errors, 17–18
 Institute of Electrical and Electronics Engineers (IEEE), 355
 integrated routers, 398–400
 interception of data, 379
 interface command, 107
 interface IDs, 233
 interface range command, 77
 interface vlan command, 113
 interfaces
 for routers
 configuration verification, 32
 configuring, 27–28
 status verification, 30–31
 verification commands, 30
VLAN interface on WLC, 425–428
Interior Gateway Protocols (IGPs), 482
Interior Gateway Routing Protocol (IGRP), 482
Intermediate System-to-Intermediate System (IS-IS), 482
internal root path cost, 152–153
International Telecommunication Union (ITU), 355
Internet of Things (IoT) Onboarding, 390
inter-VLAN routing, 98
on Layer 3 switches, 112–119
operational overview, 102–103, 112–113
routing scenario and configuration, 116–119
scenario, 113
switch configuration, 114–115
verifying, 115–116
legacy inter-VLAN routing, 98–100
router-on-a-stick, 103–111
connectivity verification, 108–109
operational overview, 100–102
scenario, 103–105
subinterface configuration, 107–108
verifying, 110–111
VLAN and trunking configuration, 105–107
troubleshooting, 119–129
common issues, 119–120
missing VLANs, 121–124
router configuration issues, 127–129
scenario, 120–121
switch access port issues, 125–127
switch trunk port issues, 124–125
IoT (Internet of Things) Onboarding, 390
ip address command, 27, 107
ip address dhcp command, 214
IP address spoofing, 289, 303
ip dhcp pool command, 205
ip domain-name command, 22
ip helper-address command, 212–213
ip route command, 497–498
ip routing command, 115, 117
IP routing tables. See routing tables
IP Source Guard (IPSG), 289, 303
ip ssh version 2 command, 22–23
ipconfig /all command, 209, 213, 242, 247, 253
ipconfig command, 108, 115, 224, 233
ipconfig /release command, 211
ipconfig /renew command, 207, 211–212, 403
IPSG (IP Source Guard), 289, 303
IPv4 addressing
configuring for switch management interface, 9
excluding addresses, 205
ip route command, 497–498
longest match example, 449
loopback interfaces, 28–29
NAT for IPv4 for remote site WLAN configuration, 408–410
packet forwarding, 452
routing tables
starting, 499–501
structure of, 477–478
static routes
default routes, 513–514
directly connected static routes, 505–506
displaying, 511
floating static routes, 518–520
fully specified static routes, 507–509
host routes, 523
next-hop static routes, 503–504
ipv6 address autoconfig command, 244
ipv6 address command, 27, 224
ipv6 address dhcp command, 249
IPv6 addressing
configuring for switch management interface, 9
global unicast addresses
assigning, 226–227
configuring, 224–225
RA message flags, 226–228
ipv6 route command, 498
link local addresses
configuring, 224–226, 243–244, 249
as next-hop addresses, 524
verifying, 31
longest match example, 449
multicast addresses, verifying, 31
packet forwarding, 452
routing tables
starting, 501–503
structure of, 478–479
static routes
default routes, 514
directly connected static routes, 506–507
displaying, 512–513
floating static routes, 518–520
fully specified static routes, 509–510
host routes, 523–524
next-hop static routes, 504–505
verifying addresses, 229–230, 242–243, 247–248
ipv6 dhcp pool command, 241, 246
ipv6 dhcp relay destination command, 252
ipv6 dhcp server command, 241, 247
ipv6 enable command, 243–244, 249
ipv6 nd managed-config-flag command, 239, 247
<table>
<thead>
<tr>
<th>LACP (Link Aggregation Control Protocol), 181–183</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuring, 185</td>
</tr>
<tr>
<td>LAGs (link aggregation groups), 360</td>
</tr>
<tr>
<td>LAN attacks, 292–306</td>
</tr>
<tr>
<td>address spoofing attacks, 303</td>
</tr>
<tr>
<td>ARP attacks, 300–302</td>
</tr>
<tr>
<td>CDP reconnaissance, 305–306</td>
</tr>
<tr>
<td>DHCP attacks, 296–300, 329</td>
</tr>
<tr>
<td>STP manipulation attacks, 303–305</td>
</tr>
<tr>
<td>VLAN attacks, 293–295, 327</td>
</tr>
<tr>
<td>LAPs (lightweight APs), 359–360, 412</td>
</tr>
<tr>
<td>late collisions, 17, 18</td>
</tr>
<tr>
<td>Layer 2 loops, 139, 142–143</td>
</tr>
<tr>
<td>Layer 2 security threats, 287–289</td>
</tr>
<tr>
<td>categories of, 288–289</td>
</tr>
<tr>
<td>MAC address table attacks, 290–292</td>
</tr>
<tr>
<td>mitigation techniques, 289</td>
</tr>
<tr>
<td>Layer 2 switches. See switches</td>
</tr>
<tr>
<td>Layer 3 switches, inter-VLAN routing, 112–119</td>
</tr>
<tr>
<td>operational overview, 102–103, 112–113</td>
</tr>
<tr>
<td>routing scenario and configuration, 116–119</td>
</tr>
<tr>
<td>scenario, 113</td>
</tr>
<tr>
<td>switch configuration, 114–115</td>
</tr>
<tr>
<td>verifying, 115–116</td>
</tr>
<tr>
<td>learn state (HSRP), 269</td>
</tr>
<tr>
<td>learn-and-forward method, 48</td>
</tr>
<tr>
<td>learning state, 158, 160</td>
</tr>
<tr>
<td>lease command, 206</td>
</tr>
<tr>
<td>leases, 200–201</td>
</tr>
<tr>
<td>obtaining, 201–203</td>
</tr>
<tr>
<td>renewing, 203–204</td>
</tr>
<tr>
<td>LED indicators for switches, 3–5</td>
</tr>
<tr>
<td>legacy inter-VLAN routing, 98–100</td>
</tr>
<tr>
<td>Lightweight Access Point Protocol (LWAPP), 359, 412</td>
</tr>
<tr>
<td>lightweight APs (LAPs), 359–360, 412</td>
</tr>
<tr>
<td>line vty command, 23</td>
</tr>
<tr>
<td>link aggregation, 176</td>
</tr>
<tr>
<td>Link Aggregation Control Protocol (LACP), 181–183</td>
</tr>
<tr>
<td>configuring, 185</td>
</tr>
<tr>
<td>link aggregation groups (LAGs), 360</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP), 306</td>
</tr>
<tr>
<td>link-state routing protocols, 482</td>
</tr>
<tr>
<td>listen state (HSRP), 270</td>
</tr>
<tr>
<td>listening state, 158, 160</td>
</tr>
<tr>
<td>LLAs (link-local addresses)</td>
</tr>
<tr>
<td>configuring, 224–226, 243–244, 249</td>
</tr>
<tr>
<td>as next-hop addresses, 524</td>
</tr>
<tr>
<td>verifying, 31</td>
</tr>
<tr>
<td>LLDP (Link Layer Discovery Protocol), 306</td>
</tr>
<tr>
<td>load balancing, 177, 485–487</td>
</tr>
<tr>
<td>local AAA authentication, 284</td>
</tr>
<tr>
<td>local host routes, 522</td>
</tr>
<tr>
<td>local password authentication, 281–282</td>
</tr>
<tr>
<td>local route interfaces, 471</td>
</tr>
<tr>
<td>logging in</td>
</tr>
<tr>
<td>to wireless routers, 399–400</td>
</tr>
<tr>
<td>to WLC, 414–415</td>
</tr>
<tr>
<td>login local command, 23</td>
</tr>
<tr>
<td>long path cost, 152</td>
</tr>
<tr>
<td>longest matches, 448</td>
</tr>
<tr>
<td>IPv4 addressing example, 449</td>
</tr>
<tr>
<td>IPv6 addressing example, 449</td>
</tr>
<tr>
<td>loop guard, 162</td>
</tr>
<tr>
<td>loop-free interfaces, 28–29</td>
</tr>
<tr>
<td>loopback interfaces, 28–29</td>
</tr>
<tr>
<td>loop-free topology, configuring, 148–158</td>
</tr>
<tr>
<td>alternate port election, 156</td>
</tr>
<tr>
<td>designated port election, 153–155</td>
</tr>
<tr>
<td>root bridge election, 150–152</td>
</tr>
<tr>
<td>root port election, 152–153, 156–158</td>
</tr>
<tr>
<td>LWAPP (Lightweight Access Point Protocol), 359, 412</td>
</tr>
<tr>
<td>M flag (Managed Address Configuration flag), 227, 231</td>
</tr>
<tr>
<td>MAC address filtering, 384</td>
</tr>
<tr>
<td>MAC address flooding, 288, 290–291</td>
</tr>
<tr>
<td>MAC address spoofing, 289, 303</td>
</tr>
<tr>
<td>MAC address table, 47, 290</td>
</tr>
<tr>
<td>learn-and-forward method, 48</td>
</tr>
<tr>
<td>MAC address table attacks, 288, 290–292</td>
</tr>
<tr>
<td>mitigation techniques, 291–292, 314–326</td>
</tr>
<tr>
<td>MAC address table overflow, 315</td>
</tr>
</tbody>
</table>
MAC addresses
limiting, 317–319
in root bridge election, 150, 151
MAC broadcast domain, 52
MAC database instability, 142–143
macof utility, 291–292
malware, 277
Managed Address Configuration flag (M flag), 227
management VLANs, 64–65
man-in-the-middle attacks (MITM), 301, 302, 381–382
master routers, 266
Max Age timer, 158
mdix auto command, 13
Message Integrity Check (MIC), 387
messages (DHCP), 296
metrics, 470, 485
MIC (Message Integrity Check), 387
MIMO (multiple-input and multiple-output), 353, 361
missing VLANs, troubleshooting, 121–124
mitigation techniques
address spoofing attacks, 303
ARP attacks, 301, 332–335
DHCP attacks, 296, 329–332
Layer 2 security threats, 289
MAC address table attacks, 291–292, 314–326
STP attacks, 305, 335–339
VLAN attacks, 295, 327–328
MITM (man-in-the-middle attacks), 301–302, 381–382
mls qos trust command, 79
Mode button, 4
mode settings
in LACP, 182–183
in PAgP, 180–181
MST (Multiple Spanning Tree), 162
MSTP (Multiple Spanning Tree Protocol), 162
multicast addresses, verifying, 31
multilayer switches. See Layer 3 switches
multiple equal-cost paths, root port election from, 156–158
multiple-input and multiple-output (MIMO), 353, 361
multi-switched environment, VLANs in, 66–73
native VLAN tagging, 70–71
network with VLANs example, 68
network without VLANs example, 67
tagging, 69–72
VLAN trunks, 66–67
voice VLAN tagging, 71–72
voice VLAN verification, 72–73

NA messages. See ICMPv6 Neighbor Advertisement (NA) messages
NACs (network access controls), 278
naming
DHCPv4 pools, 205
DHCPv6 pools, 241, 246
NAT for IPv4 for remote site WLAN configuration, 408–410
native VLANs, 64
configuring, 327–328
tagging in, 70–71
negotiated interface modes in DTP, 89
neighbors, 472
netbios-name-server command, 206
network access controls (NACs), 278
network access layer issues
input and output errors, 17–18
troubleshooting, 18–20
types of, 15–17
network command, 205–206
network discovery, 474
network security devices, 278
network setup for remote site WLAN configuration, 401–404
next-hop IP addresses, 470, 524
next-hop routers, 451, 453, 537
next-hop static routes, 497
IPv4, 503–504
IPv6, 504–505
NGFWs (next-generation firewalls), 278
NGIPS (next-generation intrusion prevention system), 278
no cdp enable command, 306
no cdp run command, 306
no ipv6 nd managed-config-flag command, 247
no ipv6 nd prefix default no-autoconfig command, 247
no lldp receive command, 306
no lldp run command, 306
no lldp transmit command, 306
no service dhcp command, 210
no shutdown command, 27–28, 107
no switchport access vlan command, 81
no switchport command, 116
no switchport trunk allowed vlan command, 86
no switchport trunk native vlan command, 86
no vlan command, 82
normal range VLANs, 74
NS messages. See ICMPv6 Neighbor Solicitation (NS) messages
radio frequencies for WLANs

O
O flag (Other Configuration flag), 227, 231
OFDM (Orthogonal Frequency-Division Multiplexing), 375
omnidirectional antennas, 360
open networks, 390
Open Shortest Path First (OSPF), 450, 485
open system authentication, 385
Opportunistic Wireless Encryption (OWE), 390
Orthogonal Frequency-Division Multiplexing (OFDM), 375
OSI reference model, 287
OSPF (Open Shortest Path First), 450, 485
Other Configuration flag (O flag), 227
out-of-band management, 289
output errors, 17–18
OWE (Opportunistic Wireless Encryption), 390

P
packet forwarding, 451–458. See also frame forwarding
decision process, 451–453
direct packet forwarding, 453–456
mechanisms for, 455–458
in static routes, 532–533
PAgP (Port Aggregation Protocol), 180–181
parabolic dish antennas, 360
parent routes, 478
passive mode, 368–369
passwords, local password authentication, 281–282
path determination, 447–451
   best path equals longest match, 448
   building routing table, 450–451
   IPv4 address longest match example, 449
   IPv6 address longest match example, 449
   router functions, 447–448
path vector routing protocols, 482
Per-VLAN Spanning Tree (PVST+), 160, 162
phishing, 279
physical layer, switch port configuration, 12–13
ping command, 33, 108, 109, 116, 465, 535–537, 539
planning WLAN deployment, 377–379
PMF (Protected Management Frames), 386
PoE (Power over Ethernet) Mode LED, 5
Point-to-Point protocol (PPP), 453
pools (DHCPv4)
   configuring, 205–206
   naming, 205
pools (DHCPv6)
   binding to interface, 241–242, 246–247
   configuring, 241, 246–247
   naming, 241, 246
Port Aggregation Protocol (PAgP), 180–181
port assignment in WLANs
   changing, 81–82
   commands, 76–77
   example, 77–78
port channel interface, 177
Port Duplex LED, 5
port forwarding, 410–412
port IDs, 158
port priority, 157–158
port security, 289, 292, 314–315
   aging, 319–320
   disabling unused ports, 314–315
   enabling, 316–317
   error-disabled state, 322–324
   limiting MAC addresses, 317–319
   verifying, 324–326
   violation modes, 321–322
Port Speed LED, 5
port states
   RSTP, 163–165
   STP, 159–160
Port Status LED, 5
port triggering, 411–412
PortFast, 165–166, 336
   configuring, 336–338
POST (power-on self-test), 2
Power over Ethernet (PoE) Mode LED, 5
PPP (Point-to-Point protocol), 453
process switching, 456–457
Protected Management Frames (PMF), 386
PSK (pre-shared key), 386
PSTN (public switched telephone network), 46
PVST+ (Per-VLAN Spanning Tree), 160, 162

Q
QoS (Quality of Service) for remote site WLAN
   configuration, 410–411
quad-zero routes, 514

R
RA messages. See ICMPv6 Router Advertisement (RA) messages
radio frequencies for WLANs, 354–355
RADIUS (Remote Authentication Dial-In User Service), 284, 386, 388–389, 421, 423–424
ransomware, 277
rapid frame switching, 49
Rapid PVST+162–163
Rapid Spanning Tree Protocol (RSTP), 162–165
reconnexion attacks, 305–306
recovering from system crash, 6–7
recursive lookup, 497–498
redundancy
  in Layer 2 switched networks, 139, 141–142
  router redundancy, 264–265
Redundant Power System (RPS) LED, 4
relay agents (DHCPv4), 210–213
remote access control. See access control
remote management
  switch configuration, 8–10
  switch security, 20–25
  SSH (Secure Shell), 20–25
telnet, 20–21
remote networks, 450
remote site WLAN configuration, 398–412
  NAT for IPv4, 408–410
  network setup, 401–404
  port forwarding, 410–412
  QoS (Quality of Service), 410–411
  wireless mesh network configuration, 408
  wireless routers, 398–400
  wireless setup, 404–408
renewing leases, 203–204
resetting VLAN trunks to default, 86–87
restoring switch default settings, 82
RIP (Routing Information Protocol), 482, 485
RIPng, 483
RIPv1, 482
RIPv2, 482
rogue APs (access points), 379, 381, 414
root bridge, 145
  electing, 150–152
root guard, 162
root path cost, 152
root ports, 152–153, 156–158
route lookup process, 477
route timestamp, 470
routed ports, 116–117
router-on-a-stick, 103–111
  connectivity verification, 108–111
  operational overview, 100–102
  scenario, 103–105
  subinterface configuration, 107–108
  troubleshooting, 127–129
VLAN and trunking configuration, 105–107
routers
  configuring, 25–29, 459–467
  commands for, 459–461
dual-stack topology, 27
  filtering show command output, 466–467
  interface configuration, 27–28
IPv4 loopback interfaces, 28–29
topology, 459
  verification commands, 461–465
as DHCPv4 clients, 214–215
as DHCPv4 servers, 204–213
  configuration example, 206–207
  configuration steps, 205–206
  disabling, 210
  relay agents, 210–213
  verifying, 207–210
DHCPv6 roles, 240
directly connected network verification, 29–36
command history feature, 36
  filtering show command output, 34–35
  interface configuration, 32
  interface status, 30–31
  interface verification commands, 30
IPv6 link local and multicast addresses, 31
routes, 32–33
failover, 265–266
functions of, 447–448
packet forwarding, 451–458
decision process, 451–453
end-to-end packet forwarding, 453–456
  mechanisms for, 455–458
path determination, 447–451
  best path equals longest match, 448
  building routing table, 450–451
IPv4 address longest match example, 449
IPv6 address longest match example, 449
router functions, 447–448
redundancy, 264–265
wireless, 398–400
routes
  configuring on Layer 3 switches, 117–119
  verifying, 32–33
routing algorithms, 484
Routing Information Protocol (RIP), 482, 485
routing protocol messages, 483
routing tables, 467–480
  AD (administrative distance), 479–480
  building, 450–451
show interface trunk command

- default routes in, 475–476
- directly connected networks in, 470–471
- dynamic routing protocols in, 474–475
- entries, 469–470
- IPv4
  - starting routing tables, 499–501
  - structure of, 477–478
- IPv6
  - starting routing tables, 501–503
  - structure of, 478–479
- principles, 469
- route sources, 467–469
- static routes in, 471–473
- verifying, 538
- RPS (Redundant Power System) LED, 4
- RS messages. See ICMPv6 Router Solicitation (RS) messages
- RSA key pairs, generating, 22–23
- RSTP (Rapid Spanning Tree Protocol), 162–165
- runts, 17–18

S

- SAE (Simultaneous Authentication of Equals), 389
- SANS Institute, 279
- satellite broadband, 353
- SCP (Secure Copy Protocol), 289
- sdm prefer dual-ipv4-and-ipv6 default command, 9
- section filter, 34, 466
- Secure FTP (SFTP), 289
- Secure Shell. See SSH (Secure Shell)
- Secure Sockets Layer (SSL), 289
- security
  - access control, 281–287
  - 802.1X standard, 286–287
  - AAA components, 283
  - accounting, 285–286
  - authentication, 283–285
  - authorization, 285
  - local password authentication, 281–282
- endpoint security, 277–281
- best practices, 278–279
- Cisco ESA, 279–280
- Cisco WSA, 280–281
- common types of attacks, 277
- network security devices, 278
- LAN attacks, 292–306
- address spoofing attacks, 303
- ARP attacks, 300–302
- CDP reconnaissance, 305–306
- DHCP attacks, 296–300, 329
- STP manipulation attacks, 303–305
- VLAN attacks, 293–295, 327
- Layer 2 security threats, 287–289
  - categories of, 288–289
- MAC address table attacks, 290–292
- mitigation techniques
  - ARP attacks, 332–335
  - DHCP attacks, 329–332
  - Layer 2 security threats, 289
  - STP manipulation attacks, 335–339
  - VLAN attacks, 327–328
- port security, 314–326
  - aging, 319–320
  - disabling unused ports, 314–315
  - enabling, 316–317
  - error-disabled state, 322–324
  - limiting MAC addresses, 317–319
  - verifying, 324–326
  - violation modes, 321–322
- switch remote management, 20–25
- SSH (Secure Shell), 20–25
- telnet, 20–21
- WLANs (Wireless LANs), 383–390
  - authentication methods, 385–387
  - encryption methods, 387–388
  - enterprise authentication methods, 388–389
  - MAC address filtering, 384
  - SSID cloaking, 383–384
  - threats, 379–382
  - WPA3, 389–390
- server-based AAA authentication, 284–285
- service dhcp command, 210
- service set identifier (SSID), 357
- set command, 6
- SFTP (Secure FTP), 289
- shared key authentication, 385–386
- short path cost, 152
- show cdp neighbors command, 536
- show commands, filtering output, 34–35, 466–467
- show controllers ethernet-controller command, 13
- show dtp interface command, 90
- show etherchannel port-channel command, 187–188
- show etherchannel summary command, 187, 189, 192
- show flash command, 14
- show history command, 14, 36
- show interface fa0/18 switchport command, 72
- show interface switchport command, 122
- show interface trunk command, 85
show interfaces command, 14, 15–20, 32, 111, 128, 462–463
show interfaces etherchannel command, 188
show interfaces fa0/1 switchport command, 85
show interfaces fa0/18 switchport command, 80–81
show interfaces port-channel command, 186
show interfaces switchport command, 125
show interfaces trunk command, 111, 124
show interfaces vlan command, 80
show ip dhcp binding command, 207–208
show ip dhcp server statistics command, 207–208
show ip interface brief command, 10, 30, 110, 127, 424–425, 461, 536
show ip interface command, 14, 32, 212, 463–464
show ip route command, 30, 32, 110, 465, 477, 511, 535
show ip route static command, 511, 515–516
show ip ssh command, 22–23
show ipv6 dhcp binding command, 251, 253
show ipv6 dhcp interface command, 252
show ipv6 dhcp interface g0/0/1 command, 245, 250
show ipv6 dhcp pool command, 250
show ipv6 interface brief command, 10, 30–31, 244, 249, 461–462
show ipv6 interface command, 14, 32, 229–230, 464
show ipv6 interface gigabitethernet 0/0/0 command, 31
show ipv6 route command, 30, 32, 465, 512
show ipv6 route static command, 512, 516
show mac address-table command, 14
show mac-address-table command, 14
show run | begin interface port-channel command, 190
show running-config | section dhcp command, 207
show running-config | section ip route command, 511
show running-config | section ipv6 route command, 512–513
show running-config command, 14
show running-config interface command, 30, 32, 124, 462
show startup-config command, 14
show version command, 14, 22
show vlan brief command, 63, 81, 121
show vlan command, 79–80
show vlan summary command, 80
Simple Mail Transfer Protocol (SMTP), 279, 289
Simple Network Management Protocol (SNMP), 421–423
Simultaneous Authentication of Equals (SAE), 389
SLAAC (Stateless Address Autoconfiguration), 224, 228–234
DAD (Duplicate Address Detection), 234
enabling, 229–230
ICMPv6 Router Solicitation (RS) messages, 232–233
interface ID generation, 233
operational overview, 228–229
SLAAC only method, 231–232
slow network, troubleshooting, 436–438
SMTP (Simple Mail Transfer Protocol), 279, 289
SNMP (Simple Network Management Protocol), 421–423
solicited-node multicast addresses, 234
source IP and destination IP load balancing, 177
source MAC and destination MAC load balancing, 177
Spanning Tree Algorithm (STA), 145–147
spanning tree instance, 151
Spanning Tree Protocol. See STP (Spanning Tree Protocol)
speak state (HSRP), 270
spear phishing, 279
speed command, 12
split MAC architecture, 371–373
splitting wireless traffic, 436–438
SSH (Secure Shell), 20–25
configuring, 22–24
operational overview, 20–21
verifying configuration, 24–25
verifying support for, 22
SSID (service set identifier), 357
SSID cloaking, 383–384
SSL (Secure Sockets Layer), 289
STA (Spanning Tree Algorithm), 145–147
standalone mode, 372–373
standard static routes, 496
standby preempt command, 268
standby priority command, 268
standby routers, 265, 266, 268–269
standby state (HSRP), 270
stateful DHCPv6
clients, configuring, 248–250
enabling, 239
operational overview, 238–239
servers, configuring, 245–248
stateful packet inspection, 278
Stateless Address Autoconfiguration. See SLAAC (Stateless Address Autoconfiguration)
stateless DHCPv6
clients, configuring, 243–245
enabling, 237–238
operational overview, 236–237
servers, configuring, 240–243
switches, 603

states (HSRP), 269–270
static routes, 450
  comparison with dynamic routing protocols, 481–482
default routes, 513–516
  configuring, 514–515
  verifying, 515–516
  when to use, 513–514
dual-stack topology, 499
floating, 517–521
  administrative distance (AD) and, 517–518
  configuring, 518–520
  testing, 520–521
host routes, 523–524
  configuring, 523, 524
  verifying, 523–524
ip route command, 497–498
IPv4
  default routes, 513–514
  directly connected static routes, 505–506
  displaying, 511
  floating static routes, 518–520
  fully specified static routes, 507–509
  host routes, 523
  next-hop static routes, 503–504
  starting routing tables, 499–501
IPv6
  default routes, 514
  directly connected static routes, 506–507
  displaying, 512–513
  floating static routes, 518–520
  fully specified static routes, 509–510
  host routes, 523, 524
  next-hop static routes, 504–505
  starting routing tables, 501–503
ipv6 route command, 498
next-hop options, 497
packet forwarding, 532–533
in routing tables, 471–473
troubleshooting, 533–539
  commands for, 534–536
  connectivity problems, 536–539
  network changes, 534
types of, 496–497
  verifying, 510–513
  when to use, 481
store-and-forward switching, 49–50
STP (Spanning Tree Protocol)
  alternatives to, 166–168
  BPDU Guard, 165–166
  interoperation with EtherChannel, 191
  loop-free topology configuration, 148–158
    alternate port election, 156
    designated port election, 153–155
    root bridge election, 150–152
    root port election, 152–153, 156–158
    port states, 159–160
    PortFast, 165–166
  purpose of, 139–147
  broadcast storms, 143–145
  Layer 2 loops, 142–143
  operational overview, 140–141
  recalculation, 141
  redundancy in networks, 139, 141–142
  STA (Spanning Tree Algorithm), 145–147
  PVST+ (Per-VLAN Spanning Tree), 160
  RSTP (Rapid Spanning Tree Protocol), 162–165
timers, 158
  versions of, 161–162
STP attacks, mitigation techniques, 305, 335–339
STP diameter, 159
STP manipulation attacks, 289, 30–305
  mitigation techniques, 335–339
stub networks, 472
stub routers, 472
subinterfaces, 100
  configuring, 107–108
  router-on-a-stick scenario, 104
summary static routes, 496
SVI (switched virtual interface), 102, 113
  configuring, 8–10
switches
  broadcast domains, 52–53
  collision domains, 51–52
  configuring, 2–10
    boot sequence, 2–3
    boot system command, 3
    LED indicators, 3–5
    recovering from system crash, 6–7
    SVI configuration, 8–10
  congestion, alleviating, 53–54
  frame forwarding, 46–51
  cut-through switching, 49–51
  learn-and-forward method, 48
  MAC address table, 47, 290
  methods of, 48–51
  operational overview, 46
  store-and-forward switching, 49–50
  inter-VLAN routing on Layer 3, 112–119
  operational overview, 102–103, 112–113
  routing scenario and configuration, 116–119
scenario, 113

switch configuration, 114–115

verifying, 115–116

mitigation techniques, 289

ARP attacks, 301, 332–335

DHCP attacks, 296, 329–332

Layer 2 security threats, 289

MAC address table attacks, 290–292, 314–326

STP attacks, 305, 335–339

VLAN attacks, 295, 327–328

port configuration, 11–20

auto-MDIX, 13–14

duplex communication, 11–12

input and output errors, 17–18

network access layer issues, 15–17

physical layer, 12–13

troubleshooting network access layer issues, 18–20

verification commands, 14

verifying, 14–15

remote management security, 20–25

SSH (Secure Shell), 20–25
telnet, 20–21

restoring default settings, 82

security threats, 287–289
categories of, 288–289

MAC address table attacks, 290–292

troubleshooting

access port issues, 125–127

trunk port issues, 124–125

switchport access vlan command, 77, 79, 81

switchport mode access command, 76–77

switchport mode command, 89

switchport mode dynamic auto command, 88

switchport mode trunk command, 83, 88

switchport nonegotiate command, 88, 89

switchport trunk allowed vlan command, 83

switchport trunk native vlan command, 83

switchport voice vlan command, 78

Syslog, 289

system crash, recovering from, 6–7

System LED, 4

T

TACACS+ (Terminal Access Controller Access Control System), 284
tag protocol ID (TPID), 69
tagged traffic, 64

on native VLANs, 70
tagging in VLANs, 64, 69–72

native VLANs, 70–71

voice VLANs, 71–72
telnet, 20–21, 289

Temporal Key Integrity Protocol (TKIP), 386–387

Terminal Access Controller Access Control System (TACACS+), 284
terminal history size command, 36
terminal length command, 34
testing floating static routes, 520–521
tethering, 363

TFTP (Trivial File Transfer Protocol), 289

threat actors, 278, 287

threats. See attacks; security

Time to Live (TTL), 14

1–142

timers (HSRP), 26

9–270

timers (STP), 158

TKIP (Temporal Key Integrity Protocol), 386–387

TLS (Transport Layer Security), 289
topologies
dual-stack topology, 499

router configuration, 459

with VLAN 5 addressing, 424–425

wireless topology modes, 362–364

WLCs (WLAN controllers), 412–413

TPID (tag protocol ID), 69
trace route command, 535

transport input ssh command, 23

Transport Layer Security (TLS), 289

troubleshooting

EtherChannel, 188–192

inter-VLAN routing, 119–129
common issues, 119–120

missing VLANs, 121–124

router configuration issues, 127–129

scenario, 120–121

switch access port issues, 125–127

switch trunk port issues, 124–125

network access layer issues, 18–20

router-on-a-stick, 127–129

static and default route configuration, 533–539

commands for, 534–536

connectivity problems, 536–539

network changes, 534

WLANs (Wireless LANs), 433–439

client connection issues, 435–436

firmware updates, 438–439

slow network, 436–438

steps in, 433–434

trunks. See VLAN trunks

TTL (Time to Live), 141–142
VLANs (Virtual LANs) 605

VLANs (Virtual LANs), 79–80

voice VLANs, 7–27

violation modes for port security, 321–322

Virtual LANs. See VLANs (Virtual LANs)

virtual private networks (VPNs), 278

Virtual Router Redundancy Protocol (VRRP), 266

virtual routers, 26–265

VLAN 5 addressing, topologies with, 424–425

VLAN attacks, 288, 293–295, 327

mitigation techniques, 295, 327–328

vlan command, 75, 76

VLAN double-tagging, 288, 293–295, 327

VLAN hopping, 288, 293, 327

VLAN tag field, 6–9

VLAN trunking protocol (VTP), 74

VLAN trunking protocol (VTP), 74–75

VLANs (Virtual LANs)
benefits of, 6–16

counting port membership, 81–82

creation commands, 75

creation example, 75–76

data and voice VLANs, 78–79

deleting, 82

port assignment commands, 76–77

port assignment example, 77–78

ranges on Catalyst switches, 73–75

for router-on-a-stick, 105–107

verifying, 79–80

in multi-switched environment, 66–73

native VLAN tagging, 70–71

network with VLANs example, 68

network without VLANs example, 67

tagging, 69–72

VLAN trunking protocol (VTP), 74

voice VLAN tagging, 71–72

voice VLAN verification, 72–73

operational overview, 60–61

SVI configuration, 8–10

types of, 63–65

U

unequal cost load balancing, 486

unknown unicast frames, 142

untagged frames, 70–71

unused ports, disabling, 314–315

updating firmware, 438–439

URL filtering, 278, 280

user priority, 69

username command, 23

V

verification commands for switches, 14

verifying

auto-MDIX setting, 14

BPDU Guard, 338–339

default routes, 515–516

DHCP snooping, 332

DHCPv4 server configuration, 207–210

DHCPv6 relay agents, 252–254

DHCPv6 server configuration, 250–251

directly connected networks, 29–36

command history feature, 36

filtering show command output, 34–35

interface configuration, 32

interface status, 30–31

interface verification commands, 30

IPv6 link local and multicast addresses, 31

routes, 32–33

DTP mode, 90

EtherChannel, 186–188

floating static routes, 521

IP configuration, 10

IPv6 addresses, 229–230, 242–243, 247–248

Layer 3 switch inter-VLAN routing, 115–116

connectivity, 118–119

routing, 118

port security, 324–326

PortFast, 337–338

router configuration, 461–465

router-on-a-stick

configuration, 110–111

connectivity, 108–109

routing tables, 538

SLAAC configuration, 230

SSH configuration, 24–25

SSH support, 22

dynamic host routes, 523–524

static routes, 510–513

switch port configuration, 14–15

VLAN trunks, 85

VLANs (Virtual LANs), 79–80

voice VLANs, 72–73

violation modes for port security, 321–322

Virtual LANs. See VLANs (Virtual LANs)

virtual private networks (VPNs), 278
voice VLANs, 65
- configuring, 78–79
- tagging in, 71–72
- verifying, 72–73
VoIP (Voice over IP), 65
VPN-enabled routers, 278
VPNs (virtual private networks), 278
VRRP (Virtual Router Redundancy Protocol), 266
VRRPv2, 266
VRRPv3, 267
VTP (VLAN trunking protocol), 74
VTY lines, configuring, 23

W

WannaCry, 277
web security appliance (WSA), 278, 280–281
WEP (Wired Equivalent Privacy), 386
Wi-Fi Alliance, 355
Wi-Fi Protected Access (WPA), 386
Wi-Fi Protected Setup (WPS), 390
Wi-Fi range extenders, 358
WiMAX (Worldwide Interoperability for Microwave Access), 352
Wired Equivalent Privacy (WEP), 386
wireless access points. See APs (wireless access points)
wireless antennas, 360–362
wireless home routers, 357–358
wireless intruders, 379
wireless LAN controllers. See WLCs (WLAN controllers)
Wireless LANs. See WLANs (Wireless LANs)
Wireless MANs (WMANs), 350
wireless mesh network (WMN), 408
wireless NICs, 356
Wireless Personal-Area Networks (WPANs), 349
wireless routers, 398–400
wireless setup for remote site WLAN configuration, 404–408
wireless standards organizations, 355
wireless technologies, 350–353
wireless topology modes, 362–364
Wireless Wide-Area Networks (WWANs), 350
WLAN controllers. See WLCs (WLAN controllers)
WLANs (Wireless LANs), 350
- 802.11 standards, 353–354
- basic configuration on WLC, 412–420
- advanced settings, 416–417
- logging in, 414–415
- steps in, 416–420
topology, 412–413
viewing AP information, 415–416
benefits of, 349
BSS and ESS, 364–365
CAPWAP operation, 370–373
channel management, 373–379
channel selection, 375–377
frequency channel saturation, 373–375
planning WLAN deployment, 377–379
client and AP association, 367–368
components of, 356–362
wireless access points (APs), 358–360
wireless antennas, 360–362
wireless home routers, 357–358
wireless NICs, 356
CSMA/CA, 367
discover modes, 368–370
frame structure, 365–366
radio frequencies, 354–355
remote site configuration, 398–412
NAT for IPv4, 408–410
network setup, 401–404
port forwarding, 410–412
QoS (Quality of Service), 410–411
wireless mesh network configuration, 408
wireless routers, 398–400
wireless setup, 404–408
security, 383–390
authentication methods, 385–387
encryption methods, 387–388
telephone authentication methods, 388–389
MAC address filtering, 384
SSID cloaking, 383–384
WPA3, 389–390
threats, 379–382
DoS (Denial of Service) attacks, 380
man-in-the-middle attacks, 381–382
rogue APs, 381
types of, 379
troubleshooting, 433–439
client connection issues, 435–436
firmware updates, 438–439
slow network, 436–438
steps in, 433–434
types of, 349–352
wireless standards organizations, 355
wireless technologies, 350–353
wireless topology modes, 362–364
WPA2 enterprise configuration on WLC, 421–433
DHCP scope configuration, 428–433
interface configuration, 425–428
SNMP and RADIUS, 421–424
topology with VLAN 5 addressing, 424–425
WLCs (WLAN controllers), 278, 359–360
  basic configuration on, 412–420
  advanced settings, 416–417
  logging in, 414–415
  steps in, 416–420
  topology, 412–413
  viewing AP information, 415–416
MAC functions, 371
WPA2 enterprise configuration on, 421–433
  DHCP scope configuration, 428–433
  interface configuration, 425–428
  SNMP and RADIUS, 421–424
  topology with VLAN 5 addressing, 424–425
WMANs (Wireless MANs), 350
WMN (wireless mesh network), 408
Worldwide Interoperability for Microwave Access (WiMAX), 352
WPA (Wi-Fi Protected Access), 386
WPA2, 386
WPA3, 386, 389–390
WPA3-Enterprise, 390
WPA3-Personal, 389
WPANs (Wireless Personal-Area Networks), 349
WPS (Wi-Fi Protected Setup), 390
WSA (web security appliance), 278, 280–281
WWANs (Wireless Wide-Area Networks), 350

Y
Yagi antennas, 360

Z
zombies, 277