ICND1
Curriculum

100-105
Interconnecting Cisco Networking Devices Part 1
Version 3.0
Interconnecting Cisco Networking Devices Part 1

100-105 Curriculum
The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator version 9 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator version 9 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Copyright © 2016 Boson Software, LLC. All rights reserved. Boson, Boson NetSim, Boson Network Simulator, and Boson Software are trademarks or registered trademarks of Boson Software, LLC. Catalyst, Cisco, and Cisco IOS are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Media elements, including images and clip art, are the property of Microsoft. All other trademarks and/or registered trademarks are the property of their respective owners. Any use of a third-party trademark does not constitute a challenge to said mark. Any use of a product name or company name herein does not imply any sponsorship of, recommendation of, endorsement of, or affiliation with Boson, its licensors, licensees, partners, affiliates, and/or publishers.
Module 1: Networking Basics

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Objectives</td>
<td>2</td>
</tr>
<tr>
<td>Network Types</td>
<td>3</td>
</tr>
<tr>
<td>Personal Area Networks</td>
<td>4</td>
</tr>
<tr>
<td>Local Area Networks</td>
<td>5</td>
</tr>
<tr>
<td>Metropolitan Area Networks</td>
<td>6</td>
</tr>
<tr>
<td>Wide Area Networks</td>
<td>7</td>
</tr>
<tr>
<td>Understanding WAN Technologies</td>
<td>8</td>
</tr>
<tr>
<td>The Public Switched Telephone Network</td>
<td>9</td>
</tr>
<tr>
<td>Leased Lines</td>
<td>10</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>11</td>
</tr>
<tr>
<td>Asynchronous Transfer Mode</td>
<td>12</td>
</tr>
<tr>
<td>Digital Subscriber Line</td>
<td>13</td>
</tr>
<tr>
<td>Cable</td>
<td>14</td>
</tr>
<tr>
<td>Network Topologies</td>
<td>15</td>
</tr>
<tr>
<td>Bus Topology</td>
<td>16</td>
</tr>
<tr>
<td>Ring Topology</td>
<td>17</td>
</tr>
<tr>
<td>Dual-Ring Topology</td>
<td>18</td>
</tr>
<tr>
<td>Star Topology</td>
<td>19</td>
</tr>
<tr>
<td>Extended Star Topology</td>
<td>20</td>
</tr>
<tr>
<td>Full-Mesh Topology</td>
<td>21</td>
</tr>
<tr>
<td>Partial-Mesh Topology</td>
<td>22</td>
</tr>
<tr>
<td>Physical vs. Logical Topologies</td>
<td>23</td>
</tr>
<tr>
<td>Network Devices</td>
<td>24</td>
</tr>
<tr>
<td>Hubs</td>
<td>25</td>
</tr>
<tr>
<td>Bridges</td>
<td>26</td>
</tr>
<tr>
<td>Switches</td>
<td>27</td>
</tr>
<tr>
<td>Routers</td>
<td>28</td>
</tr>
<tr>
<td>Servers</td>
<td>29</td>
</tr>
<tr>
<td>Hosts</td>
<td>30</td>
</tr>
<tr>
<td>Physical Media</td>
<td>31</td>
</tr>
<tr>
<td>Copper Cables</td>
<td>32</td>
</tr>
<tr>
<td>Connecting UTP with RJ-45</td>
<td>33</td>
</tr>
<tr>
<td>Understanding Straight-through and Crossover Cables</td>
<td>35</td>
</tr>
<tr>
<td>Fiber-Optic Cables</td>
<td>37</td>
</tr>
<tr>
<td>Radio Frequency</td>
<td>38</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>39</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>41</td>
</tr>
</tbody>
</table>

Module 2: Networking Models

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
ICND1 Table of Contents

Session Layer .......................................................................................................................... 48
Transport Layer ....................................................................................................................... 49
Network Layer .......................................................................................................................... 50
Data Link Layer ........................................................................................................................ 51
Physical Layer .......................................................................................................................... 52
Using the OSI Model to Troubleshoot Networks ................................................................... 53
  Understanding the Bottom Up Troubleshooting Technique .................................................. 53
  Understanding the Top Down Troubleshooting Technique .................................................... 53
  Understanding the Divide and Conquer Troubleshooting Technique .................................. 54
Non-OSI Model Troubleshooting Techniques .......................................................................... 55
  The Follow the Path Troubleshooting Technique ................................................................. 55
  The Move the Problem Troubleshooting Technique ............................................................... 55
  The Spot the Difference Troubleshooting Technique ............................................................. 56
The TCP/IP Model ..................................................................................................................... 57
  Application Layer .................................................................................................................. 58
  Transport Layer .................................................................................................................... 59
  Internet Layer ....................................................................................................................... 60
  Network Access Layer ......................................................................................................... 61
Network Model Comparison ..................................................................................................... 62
Cisco Hierarchical Network Design Model ................................................................................ 63
Cisco Hierarchical Network Design Model Comparison ......................................................... 64
Review Question 1 .................................................................................................................... 67
Review Question 2 .................................................................................................................... 69
Module 3: Network Addressing ............................................................................................... 71
  Overview ............................................................................................................................... 72
  Objectives .............................................................................................................................. 72
  Layer 2 Addressing ............................................................................................................... 73
    Ethernet Overview ............................................................................................................... 74
    MAC Address ....................................................................................................................... 76
  Layer 3 Addressing ............................................................................................................... 78
    IPv4 Overview .................................................................................................................... 79
    Binary Overview ................................................................................................................ 81
    Dotted Decimal Overview .................................................................................................. 82
    Converting from Binary to Decimal .................................................................................... 83
    Converting from Decimal to Binary .................................................................................... 85
    Classful Networks .............................................................................................................. 88
    Classless Networks ............................................................................................................ 90
    Subnetting ........................................................................................................................ 92
      Subnetting and Route Summarization ............................................................................. 94
    Automatic IP Address Configuration ................................................................................. 95
    Understanding the Differences Between IPv4 and IPv6 .................................................. 96
    Understanding IPv6 Address Composition ....................................................................... 97
      Abbreviating IPv6 Addresses ......................................................................................... 98
    Understanding IPv6 Address Prefixes .............................................................................. 100

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
</table>

| Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information. |

**Module 5: Device Management** ................................................................. 169

| Understanding IPv6 Address Types .......................................................... 101 |
| Understanding Global Unicast Addresses and Route Aggregation .............. 104 |
| Understanding EUI-64 Interface IDs .......................................................... 106 |
| Understanding Stateful and Stateless Address Configuration .................... 107 |
| Using IPv6 in an IPv4 World ................................................................. 108 |
| Dual Stack ............................................................................................... 109 |
| Network Address Translation-Protocol Translation ..................................... 110 |
| Tunneling ............................................................................................... 111 |
| Layer 4 Addressing .................................................................................. 112 |
| User Datagram Protocol ......................................................................... 113 |
| Transmission Control Protocol .................................................................. 115 |
| Review Question 1 ................................................................................... 117 |
| Review Question 2 ................................................................................... 119 |
| Review Question 3 ................................................................................... 121 |
| Lab Exercises .......................................................................................... 123 |
| Module 4: Packet Delivery ....................................................................... 125 |
| Overview ............................................................................................... 126 |
| Objectives .............................................................................................. 126 |
| Devices in the Packet Delivery Process .................................................... 127 |
| Hubs ........................................................................................................ 128 |
| Routers ................................................................................................. 130 |
| Gateways ............................................................................................... 132 |
| Hosts ........................................................................................................ 133 |
| The Flow of Data .................................................................................... 134 |
| Protocol Data Units and Service Data Units .......................................... 135 |
| Intra-layer Communication ..................................................................... 136 |
| Inter-layer Communication ..................................................................... 137 |
| The Packet Delivery Process in Action ..................................................... 138 |
| Application Layer ................................................................................... 139 |
| Transport Layer ..................................................................................... 140 |
| User Datagram Protocol ......................................................................... 141 |
| Transmission Control Protocol ............................................................. 142 |
| The TCP Three-Way Handshake ............................................................ 143 |
| Sliding Windowing ................................................................................... 145 |
| The Protocol Field .................................................................................. 146 |
| Address Resolution Protocol .................................................................. 147 |
| Network Access Layer ............................................................................ 148 |
| Host-to-Host Packet Delivery Example ..................................................... 150 |
| Review Question 1 ................................................................................ 163 |
| Review Question 2 ................................................................................ 165 |
| Review Question 3 ................................................................................ 167 |
ICND1 Table of Contents

Overview................................................................................................................................. 170
Objectives................................................................................................................................. 170
Accessing Cisco Devices ........................................................................................................... 171
  Console Access...................................................................................................................... 172
  AUX Port Access................................................................................................................... 173
  VTY Access........................................................................................................................... 174
    Telnet ................................................................................................................................. 174
    Secure Shell......................................................................................................................... 175
IOS Overview............................................................................................................................ 176
  Device Modes......................................................................................................................... 177
    User EXEC Mode ............................................................................................................... 177
    Privileged EXEC Mode ....................................................................................................... 177
    Global Configuration Mode ............................................................................................... 178
    Interface Configuration Mode ............................................................................................ 178
    Line Configuration Mode ................................................................................................... 178
    Router Configuration Mode ............................................................................................... 178
CLI Features ............................................................................................................................. 179
  Context-sensitive Help ......................................................................................................... 179
  Command History ............................................................................................................... 179
  Syntax Verification ............................................................................................................... 180
  Enhanced bietet .................................................................................................................... 180
Understanding the IOS Boot Process ...................................................................................... 181
  Loading IOS Images............................................................................................................. 182
  Changing the IOS Image Load Location ............................................................................... 183
  Using the Configuration Register ....................................................................................... 184
  Handling IOS Load Errors .................................................................................................. 185
  Upgrading IOS...................................................................................................................... 186
    Troubleshooting IOS Upgrades ....................................................................................... 187
Initial Device Setup .................................................................................................................. 188
  Automated Setup .................................................................................................................. 188
  Manual Setup ........................................................................................................................ 189
Managing Configuration Files ................................................................................................... 190
Cisco Discovery Protocol.......................................................................................................... 191
  The show cdp neighbors Command ...................................................................................... 192
  The show cdp neighbors detail Command .......................................................................... 193
  The show cdp entry Command ............................................................................................ 195
  Disabling CDP ...................................................................................................................... 197
Using IOS to Troubleshoot Networks ...................................................................................... 198
  Understanding show Commands .......................................................................................... 199
  Understanding debug Commands ......................................................................................... 201
  Understanding the ping Command ....................................................................................... 202
  Understanding the traceroute Command ............................................................................ 204
Review Question 1 .................................................................................................................. 207
Review Question 2 .................................................................................................................. 209
Lab Exercises .......................................................................................................................... 211

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
## Module 6: Advanced Network Security with ACLs

Overview..........................................................................................................................214
Objectives ............................................................................................................................214
Understanding ACLs ........................................................................................................215
Understanding Wildcard Masks .........................................................................................216
Configuring Standard ACLs .............................................................................................217
Configuring Extended ACLs .............................................................................................220
Understanding ACL Sequencing .........................................................................................224
Applying ACLs to an Interface .........................................................................................227
Verifying and Troubleshooting ACLs ................................................................................229
Understanding Advanced ACLs .........................................................................................230
  Time-based ACLs ...........................................................................................................230
  Dynamic ACLs (lock and key) .........................................................................................230
  Reflexive ACLs .............................................................................................................231
Configuring ACLs to Control Router Access .....................................................................232
Other Uses for ACLs ..........................................................................................................233
Review Question 1 .............................................................................................................235
Review Question 2 .............................................................................................................237
Review Question 3 .............................................................................................................239
Lab Exercises ....................................................................................................................241

## Module 7: Switches

Overview .............................................................................................................................244
Objectives .............................................................................................................................244
Benefits of Switches ..........................................................................................................245
Physical Attributes of Switches ..........................................................................................247
  Switch LEDs ....................................................................................................................248
  Switch Port Types ..........................................................................................................250
  Ethernet .........................................................................................................................250
  Console ..........................................................................................................................250
  VTY ...............................................................................................................................250
Switching Modes ..................................................................................................................251
  Store-and-Forward Switching .......................................................................................252
  Cut-through Switching ..................................................................................................253
  Adaptive Cut-through Switching ...................................................................................254
  FragmentFree Switching ...............................................................................................255
Switch Interface Configuration .............................................................................................256
  Configuring Interface Duplex .......................................................................................257
  Configuring Interface Speed .........................................................................................259
  Verifying Switch Configuration ....................................................................................260
    The `show interfaces` Command ...............................................................................261
    The `show running-config` Command .......................................................................263
Troubleshooting Switches ..................................................................................................264
  Excessive Noise ............................................................................................................265
  Collisions .......................................................................................................................267

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
# ICND1 Table of Contents

**Module 9: Routers** ........................................................................................................... 329

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Late Collisions</td>
<td>269</td>
</tr>
<tr>
<td>Duplex Mismatch</td>
<td>271</td>
</tr>
<tr>
<td>Speed Mismatch</td>
<td>273</td>
</tr>
<tr>
<td>Broadcast Storms</td>
<td>275</td>
</tr>
<tr>
<td>Basic Switch Security</td>
<td>277</td>
</tr>
<tr>
<td>Disabling Unused Ports</td>
<td>278</td>
</tr>
<tr>
<td>Configuring Port Security</td>
<td>279</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
<td>281</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>283</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>285</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>287</td>
</tr>
</tbody>
</table>

**Module 8: Advanced Switching Concepts ................................................................. 289**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>290</td>
</tr>
<tr>
<td>Objectives</td>
<td>290</td>
</tr>
<tr>
<td>VLAN Overview</td>
<td>291</td>
</tr>
<tr>
<td>What Do VLANs Do?</td>
<td>293</td>
</tr>
<tr>
<td>IP Addressing Using VLANs</td>
<td>294</td>
</tr>
<tr>
<td>Creating and Configuring VLANs</td>
<td>295</td>
</tr>
<tr>
<td>Verifying VLANs</td>
<td>296</td>
</tr>
<tr>
<td>Access Ports</td>
<td>297</td>
</tr>
<tr>
<td>Configuring Access Ports</td>
<td>298</td>
</tr>
<tr>
<td>Verifying VLAN Membership</td>
<td>299</td>
</tr>
<tr>
<td>Trunk Ports</td>
<td>300</td>
</tr>
<tr>
<td>Trunk Encapsulation Methods</td>
<td>301</td>
</tr>
<tr>
<td>Configuring Trunk Ports</td>
<td>303</td>
</tr>
<tr>
<td>Verifying Port Configuration</td>
<td>304</td>
</tr>
<tr>
<td>Verifying Access Ports</td>
<td>305</td>
</tr>
<tr>
<td>Verifying Trunk Ports</td>
<td>306</td>
</tr>
<tr>
<td>Understanding and Configuring DTP</td>
<td>308</td>
</tr>
<tr>
<td>Understanding and Configuring VTP</td>
<td>310</td>
</tr>
<tr>
<td>VTP Domains</td>
<td>311</td>
</tr>
<tr>
<td>VTP Version</td>
<td>312</td>
</tr>
<tr>
<td>VTP Modes</td>
<td>313</td>
</tr>
<tr>
<td>VTP Operation</td>
<td>314</td>
</tr>
<tr>
<td>VTP Pruning</td>
<td>316</td>
</tr>
<tr>
<td>Verifying VTP</td>
<td>317</td>
</tr>
<tr>
<td>Understanding InterVLAN Routing</td>
<td>318</td>
</tr>
<tr>
<td>Configuring InterVLAN Routing</td>
<td>319</td>
</tr>
<tr>
<td>Troubleshooting VLANs and InterVLAN Routing</td>
<td>321</td>
</tr>
<tr>
<td>Review Question 1</td>
<td>323</td>
</tr>
<tr>
<td>Review Question 2</td>
<td>325</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>327</td>
</tr>
</tbody>
</table>

*Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.*
## Objectives ........................................................................................................................................ 330

## Router Benefits ............................................................................................................................. 331
- Layer 3 Forwarding ....................................................................................................................... 331
- Broadcast Domains ...................................................................................................................... 332

## Common Router Features ............................................................................................................ 333
- Modularity .................................................................................................................................. 333
- Number of Physical Ports ............................................................................................................ 333
- Routed Ports ............................................................................................................................... 333
- Supplemental Ports ..................................................................................................................... 334
- Compact Flash Storage ................................................................................................................ 334

## Configuring Router Interfaces .................................................................................................... 335
- Interface Overview ...................................................................................................................... 335
  - Modular Routers ....................................................................................................................... 336
  - Expansion Modules .................................................................................................................. 337
- Configuring a LAN Interface ........................................................................................................ 339
  - Configuring an Ethernet Interface ........................................................................................... 340
  - Verifying an Ethernet Interface ............................................................................................... 341
  - Troubleshooting an Ethernet Interface ..................................................................................... 342
- Configuring a WAN Interface ...................................................................................................... 344
  - Common WAN Encapsulation Protocols .................................................................................. 344
  - Point-to-Point Protocol ............................................................................................................. 344
  - Configuring a Serial Interface ................................................................................................. 346
  - Verifying a Serial Interface ....................................................................................................... 348
  - Troubleshooting a Serial Interface .......................................................................................... 349
  - Configuring a PPP Interface ..................................................................................................... 351

## Understanding the Routing Process ............................................................................................ 352

## Route Types .................................................................................................................................... 353
- Directly Connected Routes ......................................................................................................... 355
  - Verifying a Directly Connected Route ..................................................................................... 356
- Static Routes ................................................................................................................................ 357
  - Configuring a Static Route ....................................................................................................... 358
  - Verifying a Static Route ............................................................................................................ 360
  - Verifying a Static IPv6 Route .................................................................................................... 362
- Dynamic Routes .......................................................................................................................... 363
  - Routing Metrics ....................................................................................................................... 363
  - Administrative Distance .......................................................................................................... 364
- Default Routes ............................................................................................................................. 365
  - Configuring a Default Route .................................................................................................... 366
  - Verifying a Default Route ......................................................................................................... 367

## Review Questions ......................................................................................................................... 369
- Review Question 1 ....................................................................................................................... 371
- Review Question 2 ....................................................................................................................... 373
- Review Question 3 ....................................................................................................................... 375

## Lab Exercises ............................................................................................................................... 375

## Module 10: Advanced Routing Concepts .................................................................................... 377
- Overview ..................................................................................................................................... 378

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
Module 12: Network Security Basics

Overview.............................................................................................................................................. 445

Adversaries.................................................................................................................................................. 446
Goals and Motivations.................................................................................................................................. 447

Classes of Attacks...................................................................................................................................... 448

Common Threats........................................................................................................................................ 449

Physical Threats.......................................................................................................................................... 450
Electronic Threats..................................................................................................................................... 451
Hardware Threats...................................................................................................................................... 452
Environmental Threats............................................................................................................................ 453
Administrative Threats............................................................................................................................. 454

Reconnaissance Attacks............................................................................................................................... 455
Packet Sniffing.......................................................................................................................................... 456
Ping Sweeps............................................................................................................................................ 457
Port Scans................................................................................................................................................ 458

Access Attacks.......................................................................................................................................... 459
Password Attacks...................................................................................................................................... 460
Buffer Overflow Attacks........................................................................................................................... 461

Protecting Assets.......................................................................................................................................... 462

Securing Cisco Devices................................................................................................................................. 463

Warning Banners....................................................................................................................................... 464
Login Banners.......................................................................................................................................... 465
MOTD Banners......................................................................................................................................... 466
EXEC Banners.......................................................................................................................................... 467

Securing Access........................................................................................................................................... 468
Requiring Authentication........................................................................................................................... 469
Configuring User Names and Passwords................................................................................................. 470
Forcing SSH Access.................................................................................................................................. 471

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
ICND1 Table of Contents

Configuring an Enable Password ................................................................. 473
Logging ........................................................................................................ 474
Configuring Accurate Time ........................................................................ 475
Configuring Log Severity Levels ............................................................... 476
Securing Switch Ports ................................................................................ 477
Disabling Unused Ports ............................................................................. 478
Securing Trunk and Access Ports ............................................................... 479
Restricting Ports by Client MAC Address .................................................. 480
Verifying Port Security ............................................................................. 481
Review Question 1 .................................................................................... 482
Review Question 2 ..................................................................................... 483
Review Question 3 ..................................................................................... 484
Lab Exercises ......................................................................................... 485
Index ......................................................................................................... 486

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.
Module 1

Networking Basics
Overview

Computer networks are used for a variety of reasons to facilitate many different objectives, from simple home networks consisting of just a few computers to corporate networks consisting of thousands of computers. When more than one computing device is connected in a way that allows for the sharing of information and hardware, a network is formed. This module covers the basics of networking, highlights the different types of environments, and discusses some of the characteristics and equipment involved in creating the environments in which communications and transfer of data are achieved.

Objectives

After completing this module, you should have the basic knowledge required to complete all of the following tasks:

- Understand major network types.
- Analyze the differences between various network topologies.
- Identify the common devices and physical media used in networks.
Network Types

- PANs
- LANs
- MANs
- WANs

This section covers four basic network types: personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).
A PAN can be used to connect and share data among devices that are located within a very close proximity of each other. For example, a personal computer, a telephone, a printer, and a wireless headset might all be a part of a home office setup using a PAN. Bluetooth and ZigBee are two technologies commonly used in a PAN setting.

Bluetooth is a short-range wireless technology that can be used to securely connect devices together. For example, Bluetooth can be used to transfer voice and data traffic between fixed or mobile devices. Bluetooth devices transmit data at the 2.4 to 2.485 gigahertz (GHz) frequency range. You can use Bluetooth to connect devices such as a mouse, a set of speakers, a scanner, a cell phone, and a printer to a computer. Several versions of Bluetooth exist. Bluetooth 1.2 supports a theoretical maximum data transfer speed of 1 megabit per second (Mbps), whereas Bluetooth 2.1 supports a theoretical maximum data transfer speed of up to 3 Mbps.

ZigBee is a wireless communications protocol used in electronics such as switches, timers, remote controls, and sensors. The protocol was developed as a low-cost alternative to other wireless PANs, and it can be less costly, mainly because of the low power and battery consumption requirements of the devices it is used in. For example, a sensor for a home lawn sprinkler system using ZigBee will be in sleep mode while not in use and will use power at only the scheduled time in order to activate the sprinklers, thus saving power and reducing the battery capacity required to operate for long periods of time.
Local Area Networks

LANs are typically used for communications within a single group or organization and typically within a single building or site where buildings are within close proximity of each other. Two common types of LANs include Ethernet networks and Token Ring networks.

Ethernet networks originated with the use of coaxial cable. However, most modern Ethernet networks use unshielded twisted-pair (UTP) cables because they are inexpensive, are easy to install, and typically support network speeds of up to 1 gigabit per second (Gbps). UTP cables typically use RJ-45 connectors. The Ethernet cabling scheme uses one pair of wires to transmit data and another pair to receive data from end-station devices, such as computers or IP telephones, and networking devices, such as switches, hubs, or routers.

Token Ring networks use token passing to control media access. When token passing is used, a single token is sent around the ring from device to device. Because a device must wait until it has possession of the token before it can send data, only one device can transmit at a time. After the device has sent the data, the token is passed to the next device in the ring.
Metropolitan Area Networks

A MAN can be used to connect networks that reside within a single metropolitan area. For example, if a company has multiple locations within the same city, the company could configure a MAN to connect the LANs in each office together.
Wide Area Networks

A WAN is a network that covers a large geographical area. Often, a WAN is spread across multiple cities and even multiple countries. Computers connected to a WAN are typically connected through public networks, leased lines, or satellites. The largest example of a WAN is the Internet.
Understanding WAN Technologies

- PSTNs
- Leased lines
- Frame Relay
- ATM
- DSL
- Cable

Various access technologies can be used to enable WAN connectivity between remote sites. These technologies differ in many ways, including link speed, link latency, and cost. Some of the more common WAN access technologies are the following:

- Public Switched Telephone Networks (PSTNs)
- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- Digital Subscriber Line (DSL)
- Cable
The Public Switched Telephone Network

- Circuit-switched
- Low speed
- Low cost

The Public Switched Telephone Network

The low-cost PSTN is a circuit-switched network commonly used for telephone service. Although the PSTN was designed for voice services, several methods have been developed to use the PSTN infrastructure for data services as well. The most common method for data service uses a modem to translate the digital signals used in computer networks into an analog signal that can be transported across the PSTN. However, because the PSTN was not designed for data services, the methods used to transport digital data are limited by the capabilities of the existing infrastructure. For example, data speeds on the PSTN typically do not exceed 56 kilobits per second (Kbps) because the infrastructure was not designed to support speeds beyond 64 Kbps.
Leased lines are dedicated circuits that are typically used as endpoint connections between sites. Because the circuits are dedicated and not switched, leased lines are more expensive for service providers to implement than switched circuits are. Leased lines are commonly available in a variety of speeds, such as 56 Kbps, 1.544 Mbps, and 45 Mbps.
Frame Relay

- Packet-switched
- Medium speed
- Medium cost

Frame Relay is a cost-effective packet-switching technology that is suitable for data-only, medium-speed requirements. Frame Relay, which operates at the Data Link and Physical layers of the Open Systems Interconnection (OSI) model, uses statistical multiplexing and variable frame size to ensure network access and efficient delivery. Furthermore, Frame Relay allows multiple connections via virtual circuits (VCs) through a single interface. Frame Relay links are typically purchased in full or fractional T1 configurations.
Asynchronous Transfer Mode

ATM is a high-speed packet switching technology similar to Frame Relay. However, ATM supports video and voice as well as data traffic. The most common ATM link speed is 155 Mbps; however, gigabit speeds are used between ATM switches. Because of their high speed, these connections are typically more expensive than Frame Relay.
Digital Subscriber Line

DSL is a WAN technology that offers low bandwidth and high latency relative to other WAN technologies. For example, Asymmetric DSL (ADSL) typically offers up to 12 Mbps of bandwidth in the downstream direction, which is the direction from the provider to the subscriber. However, because of its asymmetric nature, ADSL typically offers up to only 1 Mbps in the upstream direction, which is the direction from the subscriber to the provider. These speeds are miniscule when compared with WAN technologies, such as Synchronous Optical Network (SONET), which can offer up to 10 Gbps of synchronous bandwidth.

ADSL has a low initial cost and a low monthly cost. Because ADSL is a consumer-oriented WAN technology that offers limited bandwidth, the monthly cost, or tariff, is relatively low. Additionally, because a service provider can deliver ADSL to a subscriber’s site without the addition of hardware such as repeaters, the initial cost of ADSL installation is also relatively low. However, because ADSL is typically implemented on existing copper lines, the reliability of an ADSL connection cannot be guaranteed. Thus ADSL cannot be considered a highly reliable WAN technology.
Cable networks are medium-speed, low-cost packet-switched networks. In a cable network, a cable modem termination system (CMTS) receives analog signals from the coaxial cable line and converts them into digital signals. The CMTS generally resides at the provider’s location, or head end, and demodulates analog signals received from the coaxial cable line into digital signals suitable for transmission throughout the provider’s network. The signals that pass to the CMTS from the coaxial cable are considered upstream signals and originate from the cable modem (CM) at the subscriber site, as illustrated below:

Conversely, the signals that pass to the CMTS from the provider network are considered downstream signals. The CMTS converts digital signals from the provider network into modulated analog signals that can be transmitted onto the coaxial cable line. The modulated analog signals are received by a CM at the subscriber site, where they are demodulated into a digital data stream suitable for transmission directly to the subscriber.
Network Topologies

• Types of topologies
  – Bus
  – Ring / dual-ring
  – Star / extended star
  – Full-mesh / partial-mesh

• Physical vs. logical topologies

This section covers some basic network topologies: bus, ring, dual-ring, star, extended star, full-mesh, and partial-mesh. Additionally, it includes basic differences between physical topologies and logical topologies.
Bus Topology

A bus topology has a single main line to which all computers on the network are attached. Bus topologies typically use coaxial cable and have several disadvantages, such as limited cable length and a limited number of hosts. Another disadvantage to a bus topology is that a failure on the main cable affects every host on the network.
Ring Topology

A ring topology has a central ring of cable to which all hosts on the network connect. In a ring topology, each host is connected to exactly two other hosts. The flow of traffic in a ring topology goes in a single direction, with each node on the network handling each packet then passing it off to the next node in the ring. Similar to a bus topology, a failure in the ring affects every host on the network. The failure could be within the cable or one of the nodes. If a failure occurs, traffic flow will be disrupted until the issue is repaired or the faulty node is removed from the ring.

For some simpler network environments, the ring topology has advantages over a more complex topology; one advantage is the ability to connect computers and share data without the need to purchase costly servers.
Dual-Ring Topology

As compared to a standard ring topology, a dual-ring topology has a secondary ring which allows traffic to flow in the opposite direction of the first ring so that traffic can flow in both directions at the same time. This additional ring creates a backup path for traffic; in the event that one ring fails, traffic can still flow on the other ring. Having this redundancy does improve the reliability of the ring topology; however, this is limited to protecting against damage to the cables. If one of the nodes on the ring goes down, the traffic flow will still be interrupted on both rings.
A star topology is the most common home and office network topology and is typically used on UTP Ethernet networks, but it can also be used with fiber-optic and coaxial cables. A star topology has a central connectivity device, such as a hub or a switch, to which all hosts on the network segment connect. In a very basic star topology scenario, data from one node on the network has to pass through only the central connectivity device before being sent to the intended recipient; traffic does not have to flow through all nodes in a star topology in order to reach the intended recipient. Not only can this topology improve performance, since data does not have to travel through unnecessary nodes, it also reduces the points of failure. Any given node on the network, or segment of cable, could fail and the rest of the network would still be able to communicate. However, a disadvantage of having this single point of failure is that if the central connectivity device fails, all traffic flow will stop until it has been repaired.
Extended Star Topology

An extended star topology offers the same performance and reliability found in a star topology with the addition of the ability to cover greater distances from the central switch to the end nodes by adding repeaters or additional connectivity devices to the segments. The extended star topology makes more sense in a larger physical environment and allows you to reduce degradation of signal in places such as the far reaches of a large corporate office. Although additional points of failure are added with each extension device, the points of failure on any given segment of the network remain fairly easy to pinpoint. If one segment becomes unavailable in an extended star topology, hosts connected to other devices in the topology will still be able to communicate. By contrast, if the central device in a star topology fails, no devices will be able to communicate on the network.
A full-mesh topology is a very reliable network topology because of the redundancy built into it. For example, in a full-mesh network topology, each host is connected to every other host on the network. Reliability of this topology is greatly increased over other topologies because if even one segment or connection from a host to another host is down or inoperable, another path should be available for data to travel. However, even though a full-mesh topology is highly reliable, it is very difficult and expensive to implement, especially on networks that have many hosts. Thus, a full-mesh topology might be suitable for a small network environment, but it would be more costly and difficult to maintain as the network grew in physical size as well as number of nodes on the network.
Partial-Mesh Topology

Unlike a full-mesh topology, in a partial-mesh topology, each host does not connect to all other hosts on the network. Instead, in a partial-mesh topology, each host connects to only some of the other hosts, which reduces full redundancy yet maintains some failsafe reliability. Using a partial-mesh topology can reduce the maintenance and cost of cabling while still providing additional paths for traffic to flow in the event that one path becomes unavailable.
Physical vs. Logical Topologies

- Physical – Based on actual arrangement of devices and cables, or hardware-structured
- Logical – Based on the actual path of data flow, or protocol-structured

The physical topology of a network does not necessarily have to match the logical topology.

Physical vs. Logical Topologies

The physical topology refers to the hardware structure of the network and how the devices and cables are physically arranged. For example, a physical star topology consists of a central device, such as a hub or a switch, to which all other devices are physically connected. A physical ring topology consists of devices that are connected together in a ring; each device is connected to two other devices. In a bus topology, devices are physically connected in a bus layout.

The logical topology refers to the path the data follows as it moves around the network, without regard to how the hardware is physically configured. For example, data in a physical star topology could flow across the network in a ring network. In such a scenario, the logical topology would be that of a ring network, whereas the physical topology would be a star network. It is also possible for the physical and logical topologies to be the same, such as when data travels linearly from each computer in a physical bus topology.
Network Devices

This section covers the basic network devices: hubs, bridges, switches, routers, servers, and hosts.
A hub is a multiport physical repeater that is used primarily to connect end-user workstations. An incoming frame received on any hub port is simply rebroadcast out all the other ports except the port on which the frame was received. Hubs are inexpensive devices that do not create separate broadcast or collision domains.

A collision domain is a network segment where collisions can occur when frames are sent among the devices on that network segment. For example, if four computers are connected to a hub, all four devices share the same bandwidth and each device can use only a portion of the total available bandwidth; therefore, collisions can occur when frames are sent simultaneously by multiple computers attached to the hub. A hub does not make any forwarding decisions based on Media Access Control (MAC) address or IP address. When connected to a hub, Ethernet devices rely on Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to mitigate collision. With CSMA/CD, a transmitting device listens to the network segment before attempting to send data. If no transmissions are detected, the transmitting device sends its data and then listens to determine whether a collision occurs. If a collision is detected, each of the transmitting devices involved in the collision waits a random period of time before attempting to retransmit its data. Collision detection can function only when the devices do not attempt to transmit and receive at the same time; thus hubs are restricted to half-duplex mode. Devices connected to hubs cannot transmit and receive at the same time and therefore must also operate in half-duplex mode.
Like a hub, a network bridge is a device to which endpoint devices can be connected. A bridge uses the MAC addresses of data recipients to deliver frames. Bridges maintain a forwarding database in which the MAC addresses of the attached hosts are stored. When a packet is received by a bridge, the sender’s MAC address is recorded in the forwarding database, if it is not already there. If the recipient’s address is also stored in the forwarding database, the packet will be sent directly to the recipient. However, if the recipient’s MAC address is not in the forwarding database, the packet will be broadcast out all the ports with the exception of the port the packet arrived on. Each host will receive the packet and then use the MAC address to determine whether or not the data was intended for that host; if not, the host will discard the packet. When the intended recipient responds to the packet, the bridge will send the reply directly to the original sender because the original sender’s MAC address is already stored in the forwarding database.

Bridges can be used to increase the number of collision domains. Each port on a bridge creates a separate collision domain. However, bridges do not create separate broadcast domains; all devices connected to a bridge will reside in the same broadcast domain.
Switches

Like bridges, switches can be used to provide network connectivity to endpoint devices. Switches also function similarly to bridges. A switch uses information in the data packet headers to forward packets to the correct ports. This results in fewer collisions, improved traffic flow, and faster performance. Switches essentially break a large network into smaller networks. Switches perform microsegmentation of collision domains, which creates a separate, dedicated network segment for each switch port.

Switches use physical addresses, known as MAC addresses, to carry out their primary responsibility of switching frames. Switches store known MAC addresses in a special area of memory known as the Content Addressable Memory (CAM) table or switching table. The switching table associates MAC addresses with the physical interface through which those addresses can be reached. MAC addresses are dynamically learned as the switch forwards traffic between Ethernet devices. For example, when a switch receives a frame, the switch adds the source MAC address to the switching table, if the address does not already exist, so that the switch knows to which port to send frames that are destined for that MAC address. Then the switch will check the switching table to see if the destination MAC address in the received frame is listed. If so, the switch will direct the frame to the appropriate port. If the destination MAC address is not listed, the switch will broadcast the frame out all ports except the port from which the frame was received.

If four computers are connected to a switch, each computer will reside in its own collision domain, so all four computers can send data to the switch simultaneously. However, because switches forward broadcasts, all devices connected to a switch will reside within a single broadcast domain unless virtual LANs (VLANs) are used to separate the broadcast domains.
A router is used to forward packets between computer networks. Unlike switches, which create separate collision domains, routers create separate broadcast domains. Devices that are connected to a router reside in a separate broadcast domain. A broadcast that is sent on one network segment attached to the router will not be forwarded to any other network segments attached to the router. Layer 3 switches share many features and capabilities with dedicated routers; therefore, in this module and throughout the rest of the curriculum, the general term *router* refers to any device capable of processing packets at Layer 3.

A router makes path decisions based on logical addresses, such as IP addresses. Routers store IP address information in a routing table. The routing table is stored in a special section of memory known as a Ternary CAM (TCAM) table. Like the CAM table on a Layer 2 switch, a TCAM table is used to provide wire speed access to data for queries. However, unlike the CAM table, which can provide only exact, binary matches for queries, a TCAM table can provide a nonexact match for a particular query. Routers can implement multiple TCAM tables, and these tables are commonly used to facilitate the implementation of access control list (ACL) rules, Quality of Service (QoS) policies, and other Layer 3 operations that rely on table queries, such as routing table lookups.

When a router receives a packet, it will forward the packet to the destination network based on information in the routing table. If a router receives a packet that is destined for a remote network that is not listed in the routing table, and neither a static default route nor a gateway of last resort has been configured, then the packet is dropped and an Internet Control Message Protocol (ICMP) Destination Unreachable error message is sent to the interface from which the packet was received.
There are many different types of network servers and various functions associated with them. A server can be either a specific piece of hardware or a software program and is typically set up to provide specific services to a group of other computers on a network. Servers provide a centralized way to control, manage, and distribute a variety of technologies, such as simple data files, applications, security policies, and network addresses. Some examples of servers include the following:

- **File servers** – You can configure a file server to allow users to access shared files or folders stored on the server. File servers are used as a central storage location of shared files and folders.
- **Domain servers** – You can configure a domain server to manage the resources that are available on the domain. For example, you can use a domain server to configure access and security policies for users on a network.
- **Print servers** – You can set up a print server to provide access to a limited number of printers to many computer users, rather than requiring a local printer to be installed at each computer.
- **DHCP servers** – You could use a Dynamic Host Configuration Protocol (DHCP) server to automatically provide IP addresses to client computers. When a DHCP server is configured on the network, client computers can connect to the server and automatically obtain an IP address, rather than requiring an administrator to manually configure an IP address on each computer.
- **Web servers** – You could use a web server to allow customers to access your company’s website. Web servers typically contain content that is viewable in a web browser, such as Internet Explorer.
- **Proxy servers** – You can configure a proxy server as an intermediary between a web browser and the Internet. When a computer on the internal network attempts to connect to the Internet, the computer first connects to the proxy server. Then the proxy server performs one of the following actions: the server forwards the traffic to the Internet, the server blocks the traffic, or the server returns a cached version of the requested webpage to the computer.
Hosts

The hosts on a network are the individual computing devices that access the services available on the network. A host could be a personal computer (PC), a personal digital assistant (PDA), a laptop, or even a thin client or a terminal. The hosts act as the user interface, or the endpoint at which the user can access the data or other devices that are available on a network.
Physical Media

- Copper cables
- Fiber-optic cables
Copper Cables

Copper is a soft metal that is an excellent conductor of both heat and electricity. Copper wires are used to transmit data as electrical signals. For example, Ethernet, Token Ring, and Copper Distributed Data Interface (CDDI) networks all use copper cabling to transmit data. Most modern Ethernet networks use copper UTP cables because they are inexpensive, are easy to install, and typically support network speeds of up to 1 Gbps. UTP cable segments should be no more than 100 meters in length.

UTP cables are segregated into different category ratings. A minimum rating of Category 3 is required to achieve a data transmission rate of up to 10 Mbps, which is also known as 10BaseT Ethernet. A minimum of Category 5 is required to achieve data rates of 100 Mbps, which is also known as Fast Ethernet or 100BaseTX Ethernet, or 1 Gbps, which is also known as Gigabit Ethernet or 1000BaseT Ethernet.

In the past, coaxial cables, which are another kind of copper cable, were used to connect devices together. Coaxial cables support longer segment runs than UTP cables. However, because of the low cost and high speeds of UTP cables, most modern Ethernet networks no longer use coaxial cables.
Connecting UTP with RJ-45

- Connectors contain eight pins
- Pins are numbered from left to right as you view the face of the connector, which is the side opposite of the clip
- Pins 1 and 2 are transmit pins for Ethernet and Fast Ethernet connections
- Pins 3 and 6 are receive pins for Ethernet and Fast Ethernet connections
- Gigabit Ethernet uses all eight pins and cable wires

Connecting UTP with RJ-45

UTP cables contain four pairs of color-coded wires: white/green and green, white/blue and blue, white/orange and orange, and white/brown and brown. The eight total wires must be crimped into the eight pins within an RJ-45 connector, which is a connector that resembles an oversized telephone cable connector. The pins in the RJ-45 connector are arranged in order from left to right if you are viewing the face of the connector and have the connector positioned so that the row of pins is at the top.

In a typical Ethernet or Fast Ethernet cabling scheme, the wires that are connected to Pin 1 and Pin 2 transmit data and the wires that are connected to Pin 3 and Pin 6 receive data. By contrast, Gigabit Ethernet transmits and receives data on all four pairs of wires.
There are two different Telecommunications Industry Association (TIA) wire termination standards for an RJ-45 Ethernet connector: T568A and T568B. The T568A standard is compatible with Integrated Services Digital Network (ISDN) cabling standards. However, the T568B standard is compatible with a standard established by AT&T.

The difference between the two standards is that the wires used for transmit and receive in one standard are inverse in the other.

The T568A standard uses the white/green and green wires for Pins 1 and 2, respectively, and uses the white/orange and orange wires for Pins 3 and 6, respectively. Therefore, the T568A standard transmits over the white/green and green wires and receives over the white/orange and orange wires.

The T568B standard uses the white/orange and orange wires for Pins 1 and 2, respectively and uses the white/green and green wires for Pins 3 and 6, respectively. Therefore, the T568B standard transmits over white/orange and orange and receives over white/green and green.

The white/blue and blue and white/brown and brown wires are typically connected to the same pin regardless of which standard you use.
Understanding Straight-through and Crossover Cables

- Crossover cables use a different pinout standard at each end
  - Connect similar devices with a crossover cable
- Straight-through cable pinouts match at each end
  - Connect dissimilar devices with a straight-through cable

There are times when you should use the T568A-standard pinout on one side of a UTP Ethernet cable and the T568B-standard pinout on the other side of the cable. A crossover cable uses a different standard at each end. A crossover cable should be used to connect two workstations, two switches, or two routers together over the same Ethernet cable. By contrast, dissimilar Ethernet devices, such as a router and a switch, or a switch and a workstation, must be connected with a straight-through Ethernet cable. A straight-through cable uses the same pinout standard at each end.

If two dissimilar networking devices are connected with a straight-through Ethernet cable, the transmit pair on one device is connected to the receive pair on the other device. However, if two similar networking devices are connected with a straight-through Ethernet cable, the transmit pins on one device are connected to the transmit pins on the other device, and the devices will not be able to communicate. When you are
troubleshooting network connectivity problems, a basic first approach is to verify that the cable that connects the two devices is the correct type and then reseat all cable connectors.

Because Gigabit Ethernet uses all eight wires of a UTP cable, the crossover pinout for a cable that is to be used over a Gigabit Ethernet connection is slightly more complex than an inverse T568-standard pinout. In addition to inverting the T586-standard transmit and receive wires, the white/blue and blue wires on one end of the cable should be inverse to the white/brown and brown wires on the other end of the cable.
Unlike copper cables, which transmit data as electrical signals, fiber-optic cables transmit data as pulses of light; in addition, fiber-optic cables are not susceptible to radio frequency interference (RFI) or electromagnetic interference (EMI). Therefore, implementing fiber-optic cabling can be useful in buildings that contain sources of electrical or magnetic interference. Fiber-optic cables are also useful for connecting buildings that are electrically incompatible.

Because fiber-optic cables support greater bandwidth and longer segment distances than UTP cables, fiber-optic cables are commonly used for network backbones and for high-speed data transfer. Fiber-optic cables can be used to create Fiber Distributed Data Interface (FDDI) LANs, which are 100-Mbps dual-ring LANs. However, Cisco switches and Cisco routers do not require fiber-optic cable connections in order to communicate with each other. Although fiber-optic cables are useful in situations where there are problems or incompatibilities related to electrical issues, fiber-optic cables typically cost more than copper UTP, shielded twisted-pair (STP), or coaxial cables.
RF is an electrical signal that is sent over the air. RF signals are typically received by radio antennas and can be used to transmit video, audio, and data. Wireless LANs (WLANs) typically use RF signals to transmit data between devices. In WLANs, hosts connect to access points (APs), which provide the hosts with access to the rest of the network. In medium-to-large Cisco networks, a wireless LAN controller (WLC) can be used along with Lightweight Access Point Protocol (LWAPP) to manage APs. Cisco WLCs allow an administrator to centralize security configurations among APs and to provide mobility services at both Layer 2 and Layer 3 of the OSI model.

RF networks are susceptible to electrical interference. Electrical devices in your office building could cause interference to occur. Wireless devices that are close to the source of the interference could experience a disruption in wireless connectivity. Sources of interference can include microwave ovens, cordless phones, and high-power electric lines. Metal shelves, cabinets, and machinery can also block a wireless signal. To ensure that the devices on your network do not lose connectivity due to interference or signal blockage, you should install multiple APs on the network.
Review Question 1

Which of the following network types is typically used to share data among devices that are in close physical proximity?

A. LAN
B. MAN
C. PAN
D. WAN
A personal area network (PAN) can be used to connect and share data among devices that are located within a very close proximity of each other. For example, a personal computer, a telephone, a printer, and a wireless headset might all be a part of a home office setup using a PAN.
Review Question 2

Which of the following network topologies offers the most redundancy?
A. star
B. extended star
C. full-mesh
D. dual ring
A full-mesh topology is a very reliable network topology because of the redundancy built into it. For example, in a full-mesh network topology, each host is connected to every other host on the network. Reliability of this topology is greatly increased over other topologies because if even one segment or connection from a host to another host is down or inoperable, another path should be available for data to travel.
Symbols

4to6 tunneling, 111
6to4 tunneling, 111
802.11, 51
802.1Q, 301, 303, 306, 310, 320, 324
802.3, 74

A

AAA (Authentication, Authorization, and Accounting), 114
Access ports, 297, 298, 305
ACL (access control list), 28, 65, 213–221, 227–233, 236, 238, 240, 293, 415
ACL sequencing, 224, 236
AD (administrative distance), 354, 358, 364, 370
Adaptive cut-through switching, 251, 254
ADSL (Asymmetric Digital Subscriber Line), 13, 52, 61, 70
ALG (application layer gateway), 132, 136
AP (access point), 38
API (Application Programming Interface), 135, 139
APIPA (Automatic Private IP Addressing), 80, 95, 423
ARP (Address Resolution Protocol), 61, 70, 148–154, 164, 341, 366
AS (autonomous system), 380
ATM (Asynchronous Transfer Mode), 8
Attacks, 449, 456, 460–462
  Access, 450, 460
  Active, 449, 456, 492
  Buffer overflow, 462
  Close-in, 449
  Distribution, 449
  Insider, 449
  Passive, 449, 456, 492
  Password, 460, 461
  Reconnaissance, 456, 492
AUI (Attachment Unit Interface), 334
Automated setup, 188, 189
AUX (auxiliary), 171, 173, 178, 334, 435, 470, 471

B

Banners
  EXEC, 465, 468, 488

C

Cabling
  Copper cables, 32
    1000BaseT, 32
    100BaseTX, 32
    10BaseT, 32
    Category 3, 32
    Category 5, 32
    Coaxial, 19–22, 32–35, 334
    STP, 37
    UTP, 5
  Crossover cables, 35, 36
  Straight-through cables, 35
CAM (Content Addressable Memory), 27
CAM (content addressable memory), 129
CAM table, 28
CDDI (Copper Distributed Data Interface), 32
CDP (Cisco Discovery Protocol), 51, 170, 191, 192, 195, 197, 302
CEF (Cisco Express Forwarding), 332
CF (Compact Flash), 334
CHAP (Challenge Handshake Authentication Protocol), 345
CIDR (Classless Inter-Domain Routing), 90–92, 94
Cisco hierarchical network design model, 63
  Access layer, 63, 65, 66
  Core layer, 63–65
  Distribution layer, 63, 65, 66
Classful Networks
  Class A, 387
Classful networks, 88
  Class A, 88, 89, 120, 392
  Class B, 88, 89, 120, 387
  Class C, 88, 89, 120, 387
  Class D, 88, 120
  Class E, 88, 120

Login, 465, 466, 488
MOTD, 465, 467, 488
BGP (Border Gateway Protocol), 381, 400
BIA (burned-in address), 73, 118
Binary system, 81, 83
Bluetooth, 4
Boson NetSim labs, 123, 211, 241, 287, 327, 375, 403, 443, 493
Bottom up troubleshooting technique, 53
BRI (Basic Rate Interface), 334
Bridges, 26
Broadcast domains, 332
Broadcast storms, 264, 275
Bus topology, 16
Commands

access-class, 232
access-list, 218–224, 232, 236, 238, 240, 415, 417
address prefix, 430
arp -a, 148
auto-summary, 392
bandwidth, 347
banner, 465
  banner exec, 468
  banner incoming, 468
  banner login, 466
  banner motd, 467
boot
  boot host, 190
  boot network, 190
  boot system, 183
  boot system flash, 183
  boot system rom, 183
  boot system tftp, 183
cdp enable, 197
cdp run, 197
clear ip dhcp binding, 432
clear ip route *, 395
clear ipv6 dhcp binding, 432
clock rate, 347
clock timezone, 434
config-register, 184
configure terminal, 178, 180
copy
  copy running-config startup-config, 177, 190, 280, 482
  copy startup-config running-config, 190
  copy startup-config tftp, 190
  copy tftp flash, 186, 187
  copy tftp running-config, 190
crypto key generate rsa, 472, 492
debug, 201
  debug ppp negotiation, 351
default-information originate, 393
deny, 215, 218, 226
description, 335
disable, 177
dns-server, 431
domain-name, 431
duplex, 257, 258, 263
enable password, 473, 490
enable secret, 473, 490
encapsulation
  encapsulation dot1q, 320
  encapsulation hdlc, 346
  encapsulation ppp, 351
end, 178
errdisable recovery interval, 280, 483
exec-timeout, 172
exit, 177, 178
help, 179
hostname, 180, 189
interface, 178, 258, 259, 279, 319, 340, 481
ip
  ip access-group, 227, 228
  ip access-list extended, 222, 223
  ip access-list standard, 218, 219, 225
  ip address, 189, 319, 340, 347
  ip address dhcp, 427
  ip classful, 382
  ip default-gateway, 366
  ip default-network, 366
  ip dhcp client lease, 427
  ip dhcp excluded-address, 430
  ip dhcp pool, 430
  ip dns server, 421
  ip domain name, 420, 472, 492
  ip helper-address, 427
  ip host, 421
  ip name-server, 420
  ip nat inside, 413
  ip nat inside source list, 415, 417
  ip nat inside source static, 414
  ip nat outside, 413, 417
  ip nat pool, 415
  ip rip advertise, 391
  ip route, 358, 360, 366, 393
  ip routing, 366
  ip ssh version, 175
ipv6
  ipv6 address, 189, 340
  ipv6 address autoconfig, 428, 429
  ipv6 address dhcp, 429
  ipv6 dhcp client lease, 427
  ipv6 enable, 189
  ipv6 host-name, 421
  ipv6 nd other-config-flag, 431
  ipv6 route, 359
ipv6 unicast-routing, 359
keepalive
  no keepalive, 350
lease, 431
line, 178
line aux, 173
line console, 172
line vty, 232
lldp run, 197
logging console, 201, 476, 477
logging host, 477
logging trap, 477
login, 470
login local, 471
logout, 177
name (VLAN), 295
network, 387, 388, 392, 394, 430
ntp master, 435
ntp refclock, 435
ntp server, 434, 435, 475
passive-interface, 394
password, 172, 173, 470
permit, 215, 218, 226, 236
ping, 187, 202–205
reload, 187
resume, 174
router ospf, 178
router rip, 387, 394
service config, 190
service dhcp, 430
service password-encryption, 470, 473
show, 200
  show access-lists, 229, 415, 417
  show cdp entry, 195, 196
  show cdp neighbors, 192, 193, 208
  show cdp neighbors detail, 193–195, 208
  show controllers, 199, 347
  show flash, 186, 199
  show interfaces, 199, 200, 260–271, 275, 278,
  295, 304, 305, 307, 341, 342, 348–351, 479
  show interfaces status, 200, 272, 274
  show ip access-lists, 229
  show ip arp, 148, 279
  show ip dhcp binding, 432
  show ip dhcp conflict, 431
  show ip interface, 229
  show ip interface brief, 356, 360, 374
  show ip nat translations, 414, 416, 418
  show ip protocols, 389, 390, 395
  show ip rip database, 392
  show ip route, 353, 354, 356, 361, 367, 389, 395
  show ip ssh, 175
  show ipv6 dhcp binding, 432
  show ipv6 interface, 341
  show ipv6 interface brief, 362
  show ipv6 route, 362
  show logging, 477
  show ntp associations, 436
  show ntp status, 436
show port-security, 280
show port-security interface, 484, 485
show processes, 275, 276
show protocols, 199
show running-config, 199, 200, 260, 263, 351,
  387
show startup-config, 199
show version, 184, 186, 187, 199
show vlan, 296, 299
show vtp status, 317
shutdown, 278, 280, 321, 340, 343, 347, 350, 479,
  483
speed, 173, 259, 263
ssh, 175
switchport
  switchport access vlan, 298, 324
  switchport mode access, 298, 480
  switchport mode dynamic auto, 308
  switchport mode dynamic desirable, 308
  switchport mode encapsulation, 480
  switchport mode trunk, 303, 308, 480
  switchport nonegotiate, 309, 480
  switchport port-security, 279, 481, 484
  switchport port-security mac-address, 279,
  280, 481, 482
  switchport port-security maximum, 279, 481,
  484
  switchport port-security violation, 279, 280,
  481, 483
  switchport trunk allowed vlan, 316
  switchport trunk encapsulation, 303
system mtu, 131
system mtu jumbo, 131
telnet, 174
terminal monitor, 201				
timers basic, 391
traceroute, 55, 204, 205
tracert, 205
transport input, 232, 472, 492
  transport input all, 232
  transport input none, 232
  transport input ssh, 175, 232, 472, 492
  transport input telnet, 174, 232
  transport input telnet ssh, 175
username password, 471
version 2, 378, 384, 388, 390, 394, 400
vlan, 295, 303
vtp
  vtp domain, 311
  vtp mode, 313
  vtp password, 311
  vtp pruning, 316
  vtp version, 312

Configuring router interfaces, 335–352
Configuring switches, 256–276
Connection-oriented protocols, 49, 150
Connectionless protocols, 49, 113, 141
Console access, 172
Console ports, 170–173, 250, 334
Converting
  Binary to decimal values, 81, 83, 84
  Decimal to binary values, 81, 85–87
Copper cables, 128
  1000BaseT, 32, 74
  100BaseT, 74
  100BaseTX, 32
  10BaseT, 32, 74
  Category 3, 32
  Category 5, 32, 128
STP, 37
UTP, 32
CRC (cyclic redundancy check), 252, 261, 262, 265–270, 301, 342, 350
Crossover cables, 35
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 25, 74, 75
CSU/DSU (channel service unit/data service unit), 349
Ctrl key sequences, 174, 175, 178
CTS (clear-to-send), 435
Cut-through switching, 251, 253–255

D

Data Link layer, 45, 50–54, 128–131, 333, 344
DCE (data communications equipment), 199, 346, 347
Default routes, 353, 365, 393
DHCP (Dynamic Host Configuration Protocol), 29, 46, 95, 96, 107, 113, 148, 406, 440
DHCP broadcast packets
  DHCPACK, 426
  DHCPDECLINE, 425
  DHCPDISCOVER, 423, 440
  DHCPNAK, 426
  DHCPOFFER, 423–426
  DHCPREQUEST, 424–426
DHCP clients, 422, 423, 425–427, 440
DHCP relay, 427
DHCP servers, 422, 423, 425–429, 427, 430, 431, 440
DHCPv6 (Dynamic Host Configuration Protocol version 6), 96, 103, 107, 422, 428, 429, 430, 431
Dijkstra algorithm, 398
Directly connected routes, 353–355, 364, 370
Distance-vector routing protocols, 379, 383–385, 385, 400
Divide and conquer troubleshooting technique, 54
DNS (Domain Name System), 46, 58, 107, 139, 202, 204, 406, 442
DoS (Denial of Service), 449
Dotted decimal notation, 82, 92, 93
DRAM (dynamic random access memory), 181, 190
DSL (Digital Subscriber Line), 8, 13
DTE (data terminal equipment), 199, 346
DTP (Dynamic Trunking Protocol), 308, 309, 480
Dual-ring topology, 18
Dual-stack configuration, 109
Duplex mode, 245, 249, 256–259
  Full-duplex, 75, 245, 249, 257, 258, 267, 271, 272, 284
  Half-duplex, 25, 74, 75, 249, 257, 258, 267, 271
Dynamic ACLs, 230
Dynamic NAT, 409, 411, 412, 415
Dynamic routes, 353, 363
Dynamic routing protocols, 379

E

EGP (exterior gateway protocol), 379, 381
EMI (electromagnetic interference), 37
Encapsulation methods
  HDLC, 344
  PPP, 344–345
EtherType values
  0x0800, 149
  0x0806, 149
EU (extended unique identifier), 103, 106, 189
EU–64, 103, 106, 107, 189
Extended ACLs, 214, 220–223, 230, 232, 240
Extended star topology, 20
Exterior routing protocols, 379, 380

F

FCS (Frame Check Sequence), 129, 130
FDDI (Fiber Distributed Data Interface), 37, 295
FIB (Forwarding Information Base), 332
Fiber-optic cables, 19–22, 37, 128, 334
Flow of data, 134–137
FragmentFree switching, 251, 255
Frame Relay, 8, 11, 12, 51
FTP (File Transfer Protocol), 46, 58, 114, 116, 139, 150, 159–161, 222, 463
Full-duplex mode, 75, 245, 249, 257, 258, 271, 272, 284
Full-mesh topology, 21
ICMP messages

Destination Unreachable, 28, 141, 202, 204, 365
Echo, 202
Echo Reply, 80, 202, 458
Echo Request, 205, 458
Redirect, 202
Source Quench, 202
TEM (Time Exceeded Message), 204

ICMPv6 (Internet Control Message Protocol version 6), 96
IDS (Intrusion Detection System), 459, 463, 464
IEEE (Institute of Electrical and Electronics Engineers), 73–77, 118, 301, 306
IETF (Internet Engineering Task Force), 103
IGP (interior gateway protocol), 379–383
IHL (IP Header Length), 79
Implicit deny rule, 215, 219, 223
Inter-layer communication, 134, 137
Interesting octet, 92, 93
Interesting traffic, 214, 233, 415
Interface configuration mode, 178, 179, 189, 197, 257, 295, 298, 303, 324, 340, 346, 351, 413, 427, 480, 483
Interior routing protocols, 379, 380
Internet layer, 57–60, 128–132, 147, 148, 150, 151, 155–158, 160, 161, 164
InterVLAN routing, 65, 290, 293, 294, 318, 319, 321
Intra-layer communication, 134, 136
IP (Internet Protocol), 44, 50, 70, 458
IP addressing, See IPv4 (Internet Protocol version 4); See IPv6 (Internet Protocol version 6)
IPS (Intrusion Prevention System), 459, 462, 463
IPSec (Internet Protocol Security), 96
IPv6 unicast addresses, 102
Global unicast, 102–104
Link-local unicast, 102, 103
Unique local unicast, 102
IPX (Internetwork Packet Exchange), 50
ISATAP (Intra-site Automatic Tunnel Addressing Protocol), 111
ISDN (Integrated Services Digital Network), 34, 334
ISL (Inter-Switch Link), 301, 303, 306, 310, 324
ISP (Internet service provider), 78, 102, 104, 105

JPEG (Joint Photographic Experts Group), 47, 68

LAN (local area network), 3, 5, 291, 292, 330, 335–339, 345, 346
Ethernet, 5
Token Ring, 5
Layer 2 addressing, 73, 78, 118
Layer 3 addressing, 78
Layer 3 forwarding, 331
Layer 4 addressing, 112
Layers of the Cisco hierarchical model, See Cisco hierarchical network design model
Layers of the OSI model, See OSI model
Layers of the TCP/IP model, See TCP/IP model
LCP (Link Control Protocol), 345
LED (light emitting diode), 247–249
Line configuration mode, 174, 175, 178, 232, 435, 472, 492
Link-state routing protocols, 379, 383–385, 398, 400
LLDP (Link Layer Data Protocol), 191
Logging in to a Cisco device, 171–175
Logging server, 477
Log severity levels, 476
LSA (link-state advertisement), 384–386, 402
LWAPP (Lightweight Access Point Protocol), 38

M

MAC addresses, 26, 27, 74, 76, 77, 106, 129, 131, 148, 151, 152, 153, 154, 155, 156, 157, 158, 160, 161, 246, 279, 280, 331, 341, 348, 481, 482, 483, 484
MAN (metropolitan area network), 3, 6
Manual setup, 188, 189

Memory

DRAM, 181, 190
Flash, 181–189, 199, 210, 315
NVRAM, 181, 184, 190, 313, 315
ROM, 181–185, 210
Message logging, 477

MLP (Multilink Point-to-Point Protocol), 345
MOTD (Message-of-the-Day), 465, 467, 488
MPEG (Motion Picture Experts Group), 47, 68
MTU (maximum transmission unit), 130, 341, 348

N

NAC (Network Admission Control), 66
Named access lists, 225
NAT (Network Address Translation), 80, 89, 96, 110, 111, 132, 233, 332, 406, 407–415, 438
NAT-PT (Network Address Translation-Protocol Translation), 108, 110
NAT overloading, 407, 409, 412
NAT translation, 409
Many-to-many mapping, 409, See also Dynamic NAT
Many-to-one mapping, 409, See also NAT overloading; See also PAT (Port Address Translation)
One-to-one mapping, 409, See also Static NAT
NCP (Network Control Protocol), 345
NetSim labs, 123, 211, 241, 287, 327, 375, 403, 443, 493
Network Access layer, 57, 61, 62, 70, 128
Network layer, 45, 49–51, 54, 60, 334
Network security
Adversaries, 447, 448
Attacks, 449
Threats, 450–455
Network topologies
Bus, 15, 16, 17, 23
Dual-ring, 15, 18, 37
Extended star, 15, 20
Full-mesh, 15, 21, 22, 42
Partial-mesh, 15, 22
Ring, 15, 17, 18, 23
Star, 15, 19, 20, 23

Numbered access lists, 225
NVRAM (non-volatile random access memory), 181, 184, 190, 313, 315

O

OS (operating system), 112, 135, 141, 142, 168, 176, 202, 419
OSI (Open Systems Interconnection), 11, 44, 72, 79, 128, 188, 331, 344
OSI model, 44–60, 55, 128
Application layer, 45–47, 53–57, 112, 113, 116, 422
Bottom up troubleshooting technique, 53
Data Link layer, 11, 45, 50–54, 128–131, 333, 344
Divide and conquer troubleshooting technique, 54
Layer 1, 343, 350, 374
Layer 2, 28, 250, 281, 331, 343, 346, 350, 374
Layer 2 addressing, 73, 78
Layer 3, 28, 193, 293, 294, 318, 321, 331, 339, 346
Layer 3 addressing, 78
Layer 4, 45, 49, 331
Layer 4 addressing, 112
Q

QoS (Quality of Service), 28, 233, 293
QuickTime, 47, 68

P

Packet delivery process, 126, 127, 138
PAN (personal area network), 3, 4, 40
Blurtooth, 4
Zigbee, 4
PAP (Password Authentication Protocol), 48
Partial-mesh topology, 22
PAT (Port Address Translation), 96, 406, 407–409, 412, 413, 417
PDU (Protocol Data Unit), 45, 135–161, 168
Physical layer, 45, 51–54, 128, 129, 137
Physical media
  Copper cables, 31, 32, 37, 52, See also Copper cables
  Fiber-optic cables, 31, 52, 334, See also Fiber-optic cables
Physical port, 250
Poison reverse, 385, 386
POP3 (Post Office Protocol 3), 46, 116
Ports
  AUI, 334
  AUX, 173, 334, 435
  BRI, 334
Port security, 277, 279, 280
Port states
  Error-disabled, 483
Port states (STP)
  Blocking, 281
  Forwarding, 281
PPP (Point-to-Point Protocol), 51, 61, 70, 330, 344–346, 350, 351
Presentation layer, 45–48, 68
Privileged EXEC mode, 177, 178, 199, 201, 203, 204, 229, 296, 392, 395, 469, 473
PSTN (Public Switched Telephone Network), 8, 9

R

RADIUS (Remote Authentication Dial-In User Service), 114, 471
RAM (random-access memory), 199
Reflexive ACLs, 231
RF (radio frequency), 38
RFC (Request for Comments), 423
  RFC 1010, 147
  RFC 1918, 89, 408
  RFC 3927, 80–106, 423
  RFC 790, 147
RFI (radio frequency interference), 37
Ring topology, 17, 18, 23
RIP (Routing Information Protocol), 353, 354, 356, 361, 364, 367, 370, 381, 383, 400
RIPv1 (Routing Information Protocol version 1), 385, 387, 400
RIRs (Regional Internet Registries), 102, 104, 105
RJ-45 connectors, 5, 33, 34
ROM (read-only memory), 181–185, 210
ROMmon mode, 182
Routed protocols, 78
Router-on-a-stick, 318
Router configuration mode, 178
  Modular routers, 336
Route summarization, 91, 94, 104
Route types
  Default, 365–367, 372, 393
  Directly connected, 353–355
  Dynamic, 363
  Static, 356–360, 364–367, 372
Routing loops, 385, 386
Routing metrics, 363
Routing protocols, 78, 294, 318, 347, 363, 364, 370, 378–384, See also Distance-vector routing protocols; See also Hybrid routing protocols; See also Link-state routing protocols
Routing updates, 379, 383
RPC (Remote Procedure Call), 48
RPS (Redundant Power System), 249
RSTP (Rapid Spanning Tree Protocol), 246

S

SDU (Service Data Unit), 135, 137, 150, 156, 158
Servers, 29
  DHCP, 29, 95, 422–430
  Domain, 29
  File, 29
  Print, 29
ICND1 Index

Proxy, 29
Web, 29, 133, 139
Session layer, 45–49
Severity levels, 476
SLAAC (Stateless Address Automatic Configuration), 428, 429
SLB (server load balancing), 132
Sliding windowing, 146
SMTP (Simple Mail Transfer Protocol), 46, 58, 116
SNMP (Simple Network Management Protocol), 113, 317
SONET (Synchronous Optical Network), 13
Speed mismatch, 273, 286
SPF (shortest path first), 383, 398, 402
Split horizon, 385, 386
SSH (Secure Shell), 46, 170, 174, 175, 201, 232, 250, 295, 334, 465, 472, 488, 492
Standard ACLs, 214, 217–219, 221, 225, 232, 240
Standards
802.11, 51
802.1Q, 301, 303, 306, 320, 324
802.3, 74
T568A, 34, 35
T568B, 34, 35
Star topology, 19, 20, 23
Stateful address configuration, 107
Stateless address configuration, 107
Static NAT, 409–411, 414
Static routes, 353, 357, 361, 364, 370
Store-and-forward switching, 251–254
STP (shielded twisted-pair), 37
STP (Spanning Tree Protocol), 246, 249, 276, 281
Straight-through cables, 35
Subinterface configuration mode, 319, 320
Subnetting, 91–94
Interesting octet, 92, 93
Subnetworks, 72, 80, 92–94, 330, 331
Switches, 27, 75, 127, 129, 243–247, 264, 284
Broadcast storms, 264, 275
Collision domains, 284
Collisions, 264, 267, 269
Duplex mismatch, 264, 271
Excessive noise, 264, 265
Full-duplex mode, 245, 284
Late collisions, 264
Multilayer switches, 252
Speed mismatch, 264, 273, 286
Switching loops, 246, 281
Switching modes, 251
  Adaptive cut-through, 251, 254
  Cut-through, 251–254
  FragmentFree, 251, 255
  Store-and-forward, 251–254
Switching table, 27
Switch port types, 250
  Console, 250
  Ethernet, 250
Switch security, 277–279
Syntax (CLI), 180
Syslog, 477
Syslog messages, 477

T
TCAM (Ternary Content Addressable Memory), 28
TCP (Transmission Control Protocol), 44, 49, 57–62, 70, 80, 115, 116, 221, 223, 227, 331, 419, 442, 449, 459
TCP/IP (Transmission Control Protocol/Internet Protocol), 44, 57–62, 70, 80, 126, 166, 202
TCP/IP model, 57–62, 126, 128–138, 150, 161, 166
  Application layer, 57, 128, 132–141, 144, 150, 159–161, 166, 168
  Internet layer, 57, 59, 60, 128–132, 144, 147–151, 155–161, 164
  Network Access layer, 57, 61, 62, 70, 128, 129, 131, 134, 137, 147–161, 164
  Transport layer, 57, 128, 132, 135–142, 144, 147, 150, 155–161, 166, 168
TEM (Time Exceeded Message), 204
Teredo tunneling, 111
TFTP (Trivial File Transfer Protocol), 46, 114, 182–190, 210, 431, 470
Three-way handshake, 49, 115, 142, 143, 150, 156, 157, 159
Time-based ACLs, 230
Token Ring, 5, 32, 295
Top down troubleshooting technique, 53
Triggered updates, 386
Troubleshooting ACLs, 229
Troubleshooting an Ethernet interface, 342, 343
Troubleshooting a Serial interface, 349, 350
Troubleshooting IOS upgrades, 187
Troubleshooting network connectivity problems, 36
Troubleshooting network devices, 171
Troubleshooting networks with the IOS, 198–204
Troubleshooting networks with the OSI model, 53, 54
Troubleshooting switches, 264–275
Troubleshooting techniques, 55
  Bottom up, 53
  Divide and conquer, 54
  Follow the path, 55

© 2016 Boson Software, LLC
Move the problem, 55
Spot the difference, 56
Top down, 53
Troubleshooting VLANs and interVLAN routing, 321
Trunk encapsulation methods
  802.1Q, 301
  ISL, 301
TTL (Time To Live), 79, 131, 204, 205
Tunneling, 111
  4to6, 111
  6to4, 111
  ISATAP, 111
  Teredo, 111

U
UDP (User Datagram Protocol), 49, 59, 113–115, 141, 142, 204, 331, 419, 427, 442, 459
Unicast addresses, 74, 77, 79, 101–105
UPS (uninterruptible power supply), 452
URL (Uniform Resource Locator), 132, 133
USB (universal serial bus), 52, 182
User EXEC mode, 175, 177, 181, 189
UTC (Coordinated Universal Time), 434
UTP (unshielded twisted-pair), 5, 19, 32, 33, 35, 36, 37
  RJ-45, 5, 33, 34

V
Virtual port, 250
VLAN (virtual local area network), 27, 193, 208, 263, 290–301, 307, 310, 313, 316–319, 321, 324, 326, 332, 427
VLSM (variable-length subnet mask), 90, 91, 294, 382, 387, 398
VMPS (VLAN Management Policy Server), 298
VoIP (Voice over IP), 191, 233, 431
VPN (virtual private network), 233
VTP (VLAN Trunking Protocol), 193, 208, 290, 310–317, 326
VTP pruning, 316, 317
VTY (virtual terminal), 171, 174, 175, 178, 188, 232, 334, 470, 473
VTY access, 174, 175
VTY port, 250

W
WAN (wide area network), 3, 7, 8, 13, 330, 333–338, 344–346
  ADSL, 13
  ATM, 12
  Cable, 14
  DSL, 13
  Frame Relay, 11
  Internet, 7
  Leased lines, 10
  PSTN, 9
Well-known port numbers, 112
WIC (WAN interface card), 333–338
Wildcard masks, 216, 218–223
Windowing, 145, 146
Wireless standards
  802.11, 51
  802.3, 74
Wire termination standards
  T568A, 34, 35
  T568B, 34, 35
WLAN (wireless local area network), 38
WLC (wireless LAN controller), 38
Z
Zigbee, 4
Zigbee, 4
Certification Candidates

Boson Software’s ExSim-Max practice exams are designed to simulate the complete exam experience. These practice exams have been written by in-house authors who have over 30 years combined experience writing practice exams. ExSim-Max is designed to simulate the live exam, including topics covered, question types, question difficulty, and time allowed, so you know what to expect. To learn more about ExSim-Max practice exams, please visit www.boson.com/exsim-max-practice-exams or contact Boson Software.

Organizational and Volume Customers

Boson Software’s outstanding IT training tools serve the skill development needs of organizations such as colleges, technical training educators, corporations, and governmental agencies. If your organization would like to inquire about volume opportunities and discounts, please contact Boson Software at orgsales@boson.com.

Contact Information

E-Mail: support@boson.com
Phone: 877-333-EXAM (3926)
        615-889-0121
Fax: 615-889-0122
Address: 25 Century Blvd., Ste. 500
         Nashville, TN 37214