



CCNA

Curriculum

200-301

Implementing and Administering Cisco Solutions
Version 1.1

Labs powered by



Cisco Certified Network Associate

200-301 Curriculum

LM20200828/BV1.0



25 Century Blvd., Ste. 500, Nashville, TN 37214 | Boson.com

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 11 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Copyright © 2020 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. Puppet is a trademark or registered trademark of Puppet, Inc. and is used with permission. No endorsement by Puppet, Inc. is implied by the use of these marks. Ansible is a registered trademark of Red Hat, Inc. in the United States and other countries. Chef is a registered trademark of Chef, Inc. Media elements, including images and clip art, are available in the public domain. 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: Network Fundamentals	19
Overview.....	20
Objectives	20
The OSI Model.....	21
Application Layer.....	22
Presentation Layer	23
Session Layer.....	24
Transport Layer	25
Network Layer	26
Data Link Layer	27
Physical Layer	28
Network Devices.....	29
Hubs	30
Bridges	31
Switches	32
Routers	33
Servers	34
Endpoints.....	35
Next-Generation Firewalls and IPS Devices.....	36
WAPs.....	37
Controllers	38
Cisco Three-Tier Network Design Model.....	39
Core Layer.....	40
Distribution Layer	41
Access Layer	42
Cisco Two-Tier Network Design Model.....	43
Spine-Leaf Topology.....	44
WAN Topologies	45
SOHO Topologies	46
On-Premises and Cloud Deployments	47
SaaS.....	48
PaaS.....	49
IaaS	50
Interfaces and Cabling.....	51
Copper Cables	52
<i>Connecting UTP With RJ-45</i>	53
<i>Understanding Straight-Through and Crossover Cables</i>	56
Serial Cables	57
Fiber-Optic Cables	58
<i>Fiber-Optic Cable Types</i>	59
<i>Fiber-Optic Cable Connectors</i>	60
PoE	61
Troubleshooting Interfaces and Cabling	63

Excessive Noise	64
Collisions	66
Late Collisions	68
Duplex Mismatch	70
Speed Mismatch	72
Using the OSI Model to Troubleshoot Networks	74
<i>Understanding the Bottom Up Troubleshooting Technique</i>	74
<i>Understanding the Top Down Troubleshooting Technique</i>	74
<i>Understanding the Divide and Conquer Troubleshooting Technique</i>	75
Troubleshooting Connectivity	76
Troubleshooting Physical Layer Connectivity	77
Troubleshooting Data Link Layer Connectivity	79
Troubleshooting Network Layer Connectivity	80
Summary	81
Review Question 1	83
Review Question 2	85
Review Question 3	87

Module 2: Network Addressing and Transport 89

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information. 90

Overview 90
Objectives 90

Layer 2 Addressing	91
Ethernet Overview	92
<i>Ethernet Frames</i>	93
MAC Address	94
Layer 3 Addressing	96
IPv4 Overview	97
Binary Overview	99
Dotted Decimal Overview	100
Converting from Binary to Decimal	101
Converting from Decimal to Binary	103
Classful Networks	106
Classless Networks	108
Subnetting	110
<i>Subnetting and Route Summarization</i>	112
Automatic IP Address Configuration	113
Understanding the Differences Between IPv4 and IPv6	114
Understanding the Differences Between IPv4 and IPv6 Headers	115
Understanding IPv6 Address Composition	117
<i>Abbreviating IPv6 Addresses</i>	118
Understanding IPv6 Address Prefixes	120
Understanding IPv6 Address Types	121
Understanding Global Unicast Addresses and Route Aggregation	124

Understanding EUI-64 Interface IDs	126
Understanding Stateful and Stateless Address Configuration	127
Using IPv6 in an IPv4 World	128
<i>Dual Stack</i>	129
<i>Network Address Translation-Protocol Translation</i>	130
<i>Tunneling</i>	131
Verifying Layer 3 Addressing on Clients	133
<i>Verifying Layer 3 Addressing on Windows Clients</i>	134
<i>Verifying Layer 3 Addressing on Linux Clients</i>	135
<i>Verifying Layer 3 Addressing on Mac OS X Clients</i>	136
Layer 4 Addressing	137
UDP	138
TCP	140
Summary	142
Review Question 1	143
Review Question 2	145
Review Question 3	147
Review Question 4	149
Content in these modules is available in the full version of the	151
Module 3: Network Address Translation	153
Overview	154
Objectives	154
Radio Frequency	155
WLAN Topologies	156
IBSS	157
BSS	158
ESS	159
Wireless Bands and Channels	160
Wireless Standards	163
Associating With an AP	165
Open Authentication and WEP	166
WPA	167
WPA2	168
WPA3	169
802.1x	170
802.11 MAC Frames	171
Summary	173
Review Question 1	175
Review Question 2	177
Review Question 3	179
Module 4: Virtualization Fundamentals	181

Overview	182
Objectives	182
Understanding Virtualization.....	183
Device Virtualization	184
The Hypervisor.....	185
Type 1 Hypervisor.....	186
Type 2 Hypervisor.....	187
Network Virtualization.....	188
Virtual Switches.....	189
<i>Virtual Network Interfaces vs. Physical Network Interfaces</i>	190
Network Functions Virtualization.....	191
VLANs	192
VRFs.....	193
VPNs	194
Container-Based Virtualization	195
Summary	196
Review Question 1	197
Review Question 2	199

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

Module 3: Switching Fundamentals.....	203
Overview	204
Objectives	204
Understanding Switching Fundamentals	205
Layer 2 Switches	207
Layer 2 Frame Forwarding	208
<i>The CAM Table</i>	209
<i>Using the CAM Table</i>	210
<i>Configuring the CAM Table</i>	211
<i>The TCAM Table</i>	213
<i>Modifying the CAM and TCAM Tables</i>	214
<i>Switching Modes</i>	215
<i>Multilayer Switch Forwarding</i>	220
Switch Physical Interface Configuration	223
Configuring Interface Duplex	224
Configuring Interface Speed	226
Verifying Basic Switch Configuration	227
<i>The show interfaces Command</i>	228
<i>The show running-config Command</i>	230
Access Ports	232
<i>Configuring Access Ports</i>	233
<i>Verifying Access Ports</i>	234
<i>Verifying VLAN Membership</i>	235

Trunk Ports	236
<i>Trunk Encapsulation Methods</i>	237
<i>Configuring Trunk Ports</i>	239
<i>Verifying Trunk Ports</i>	240
<i>Understanding and Configuring DTP</i>	242
Understanding VLANs	244
<i>What Do VLANs Do?</i>	246
<i>VLANs and IP Addressing</i>	247
<i>Creating and Configuring VLANs</i>	248
<i>Verifying VLANs</i>	249
<i>Understanding the Voice VLAN</i>	250
<i>Configuring the Voice VLAN</i>	252
<i>Understanding and Configuring VTP</i>	253
<i>VTP Domains</i>	254
<i>VTP Version</i>	255
<i>VTP Modes</i>	256
<i>VTP Operation</i>	257
<i>VTP Pruning</i>	259
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.	260
<i>Common VLAN and Trunk Problems</i>	261
<i>CDP and LLDP</i>	262
<i>CDP vs. LLDP</i>	263
<i>Disabling and Enabling CDP</i>	264
<i>Disabling and Enabling LLDP</i>	265
<i>Verifying CDP and LLDP Configurations</i>	266
<i>Displaying CDP and LLDP Neighbors</i>	268
<i>Displaying CDP and LLDP Information About Specific Devices</i>	269
<i>Displaying CDP and LLDP Information About Advertisements</i>	270
<i>Debugging CDP and LLDP</i>	271
<i>Understanding STP</i>	272
<i>Root Switch Election</i>	273
<i>Verifying the Root Switch</i>	276
<i>Path Costs</i>	279
<i>Determining Port Roles</i>	280
<i>Root Port</i>	280
<i>Designated Port</i>	280
<i>STP Port States</i>	281
<i>STP Timers</i>	282
<i>Understanding RSTP</i>	283
<i>Differences Between STP and RSTP</i>	284
<i>Understanding RSTP Port States</i>	286
<i>RSTP Alternate and Backup Port Roles</i>	287
<i>Understanding Cisco Implementations of STP</i>	288

PVST+	289
<i>PVST+ Bridge IDs</i>	290
PVRST+	291
MSTP	292
Cisco Enhancements to STP	293
<i>PortFast</i>	294
<i>BPDU Guard</i>	295
<i>Loop Guard</i>	296
<i>Root Guard</i>	297
Understanding EtherChannel	298
Understanding EtherChannel Protocols	299
Understanding PAgP and LACP Modes.....	300
<i>The on Mode</i>	300
<i>PAgP Modes</i>	300
<i>LACP Modes</i>	301
Configuring EtherChannel	302
<i>Configuring PAgP EtherChannel</i>	304
<i>Configuring LACP EtherChannel</i>	305
<i>Configuring EtherChannel Protocols</i>	306
<i>Verifying EtherChannel</i>	308
<i>Troubleshooting EtherChannel</i>	310
<i>Aggregation Protocol Mismatches</i>	310
<i>Bundle Configuration Mismatches</i>	311
Summary	313
Review Question 1	315
Review Question 2	317
Review Question 3	319
Lab Exercises	321
Module 6: IP Routing.....	323
Overview	324
Objectives	325
Router Benefits	326
Layer 3 Forwarding	326
Broadcast Domains	327
Common Router Features	328
Modularity	328
Number of Physical Ports	328
Routed Ports	328
Supplemental Ports	329
Compact Flash Storage.....	329
Configuring Router Interfaces	330
Interface Overview	330

Configuring a LAN Interface.....	331
<i>Configuring an Ethernet Interface</i>	332
<i>Verifying an Ethernet Interface</i>	333
<i>Troubleshooting an Ethernet Interface</i>	334
Configuring a WAN Interface	336
<i>Understanding Common WAN Encapsulation Protocols.....</i>	336
<i>Configuring a Serial Interface.....</i>	338
<i>Verifying a Serial Interface</i>	340
<i>Troubleshooting a Serial Interface.....</i>	341
<i>Configuring a PPP Interface.....</i>	343
Understanding Router Path Selection	344
Router Packet Switching	345
<i>Process Switching</i>	346
<i>Fast Switching</i>	347
<i>CEF Switching</i>	348
Displaying Tables	351
<i>Displaying the IP Routing Table.....</i>	351
<i>Displaying the FIB.....</i>	352
<i>Displaying the ARP Table.....</i>	352
<i>Displaying the CEF Adjacency Table.....</i>	352
<i>Displaying the Fast-Switching Route Cache</i>	352
Clearing Tables.....	354
Route Types	355
<i>Directly Connected Routes</i>	357
<i>Verifying a Directly Connected Route.....</i>	358
<i>Static Routes</i>	359
<i>Dynamic Routes.....</i>	365
<i>Default Routes</i>	370
Understanding ASes	373
Understanding Routing Protocols	374
Understanding the Types of IGPs	375
<i>Classful or Classless Routing Protocols.....</i>	376
Understanding Distance-Vector Routing Protocols	377
<i>Learning Distance-Vector Routes.....</i>	378
<i>Updating Distance-Vector Routes</i>	379
<i>Preventing Distance-Vector Problems</i>	380
Understanding Link-State Routing Protocols	386
<i>Understanding Link-State Relationships</i>	387
<i>Understanding the Link-State Database</i>	388
<i>Learning Link-State Routes</i>	389
Understanding OSPF	390
<i>OSPF Overview.....</i>	391
<i>Choosing Between OSPF and EIGRP</i>	393

OSPF Route Processing	394
OSPF Interface Types	395
Understanding OSPF Areas.....	397
<i>Understanding Nonbackbone Areas.....</i>	398
<i>Understanding Single-Area and Multiarea Configurations.....</i>	399
Understanding OSPF Router Roles	400
<i>ASBRs</i>	400
<i>ABRs.....</i>	400
<i>Backbone and Nonbackbone Routers.....</i>	401
Understanding OSPF Router IDs	402
Understanding OSPF Adjacencies.....	403
<i>OSPF Adjacency Caveats</i>	405
Understanding DR and BDR Elections	406
Understanding the LSDB.....	407
Configuring OSPF	409
<i>Configuring Single-Area OSPFv2</i>	410
<i>Configuring Multiarea OSPFv2.....</i>	410
<i>Configuring Areas in OSPFv3</i>	411
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information,	412
<i>Verifying OSPF Link States.....</i>	414
<i>Verifying OSPF Adjacencies</i>	415
<i>Troubleshooting OSPF Adjacencies.....</i>	418
<i>Using Cost to Load Balance OSPF</i>	420
Understanding FHRPs	423
<i>Understanding HSRP</i>	424
<i>HSRP Versions.....</i>	425
<i>Understanding Virtual MAC Addresses</i>	427
<i>HSRP Hello Packets.....</i>	428
<i>HSRP Hello and Hold Timers.....</i>	429
<i>Configuring HSRP and Timers</i>	430
<i>Configuring Preemption</i>	431
<i>Verifying HSRP</i>	432
<i>Understanding VRRP</i>	434
<i>Differences From HSRP</i>	435
<i>Recognizing the Differences between VRRP and VRRPv3.....</i>	437
<i>VRRP Timers.....</i>	438
<i>Configuring VRRP</i>	439
<i>Verifying VRRP</i>	440
<i>Understanding GLBP</i>	442
<i>GLBP Virtual MAC Addresses.....</i>	443
<i>GLBP Hello Packets</i>	444
<i>The AVG</i>	445
<i>The AVF.....</i>	446

<i>How GLBP Load Balancing Works</i>	447
<i>GLBP Load Balancing Methods</i>	448
<i>How GLBP Gateway Failover Works</i>	449
<i>How GLBP Forwarder Failover Works</i>	450
<i>Configuring GLBP</i>	451
<i>Configuring GLBP Timers</i>	453
<i>Verifying GLBP</i>	454
Summary	456
Review Question 1	459
Review Question 2	461
Review Question 3	463
Lab Exercises	465
Module 7: IP Services	467
Overview	468
Objectives	468
DHCP	470
The DHCP Process	471
<i>DHCP Discover</i>	472
<i>DHCP Offer</i>	473
<i>DHCP Request</i>	474
<i>DHCP Acknowledgment</i>	475
DHCP Client Configuration	476
Automatic IPv6 Addressing on Clients	477
<i>SLAAC</i>	477
<i>Stateless DHCPv6</i>	478
<i>Stateful DHCPv6</i>	478
DHCP Server Configuration	479
DHCP Server Options Configuration	480
DNS	482
DNS Client Configuration	483
DNS Server Configuration	484
NAT/PAT	485
NAT/PAT Address Terminology	486
NAT Translation Methods	487
<i>Static NAT</i>	488
<i>Dynamic NAT</i>	489
<i>PAT</i>	490
NAT/PAT Interface Configuration	491
Static NAT Configuration	492
Dynamic NAT Configuration	493
PAT Configuration	495
NTP	497

NTP Client Configuration.....	498
NTP Server Configuration	499
NTP Authentication	500
Verifying NTP	502
FTP	503
FTP Usage on Cisco Devices	504
<i>Copying Files Between a Cisco Device and an FTP Server</i>	505
TFTP	506
TFTP Usage on Cisco Devices	507
Telnet	508
Telnet Server Configuration.....	509
<i>Connecting to a Telnet Server</i>	510
The Problem With Telnet.....	511
SSH.....	512
SSH Configuration.....	513
SNMP.....	514
SNMP Configuration	515
SNMP Views Configuration	517
SNMP Data.....	518
Syslog.....	520
Syslog Configuration	521
Log Severity Levels	522
<i>Log Severity Level Configuration</i>	523
QoS.....	524
Normal Traffic Flow.....	526
Buffers and Memory Pools.....	527
Congested Traffic Flow.....	528
Traffic Classification and Marking	529
<i>Classification</i>	530
<i>Marking</i>	532
Congestion Management	533
<i>Queuing Mechanisms</i>	534
<i>Scheduling Mechanisms</i>	535
Congestion Avoidance	536
Policing and Shaping.....	538
Summary	539
Review Question 1.....	541
Review Question 2.....	543
Review Question 3.....	545
Review Question 4.....	547
Lab Exercises	549
Module 8: Security Fundamentals.....	551

Overview	552
Objectives	552
Common Threats	553
Physical Threats	554
<i>Electrical Threats</i>	555
<i>Hardware Threats</i>	556
<i>Environmental Threats</i>	557
<i>Administrative Threats</i>	558
Reconnaissance Attacks	559
<i>Packet Sniffing</i>	560
<i>Ping Sweeps</i>	561
<i>Port Scans</i>	562
Access Attacks	563
<i>Password Attacks</i>	564
<i>Buffer Overflow Attacks</i>	565
Access Controls	566
User Awareness and Training	567
Passwords	569
<i>Local Passwords</i>	570
<i>Creating a Secure Password for Privileged EXEC Mode Access</i>	573
<i>Password Management</i>	576
Password Alternatives	580
<i>PKI and Certificates</i>	581
<i>Biometrics</i>	582
Authentication Factors	583
<i>Combining Authentication Factors</i>	584
ACLs	586
<i>Standard ACLs</i>	587
<i>Extended ACLs</i>	590
<i>Configuring Time-Based ACLs</i>	594
<i>Configuring IPv4 ACLs to Control Remote Access</i>	595
<i>Configuring IPv4 ACLs to Control Interface Access</i>	596
<i>Configuring IPv6 ACLs to Control Remote Access</i>	598
<i>Configuring IPv6 ACLs to Control Interface Access</i>	599
Layer 2 Security	600
DHCP Snooping	601
<i>Configuring DHCP Snooping</i>	602
DAI	604
<i>Configuring DAI</i>	605
Securing Switch Ports	606
<i>Disabling Unused Ports</i>	607
<i>Securing Trunk and Access Ports</i>	608
<i>Restricting Ports by Client MAC Address</i>	609

<i>Verifying Port Security</i>	612
Wireless Security	614
WPA	615
WPA2	616
WPA3	617
Configuring Cisco WLAN Layer 2 Security	618
Configuring Cisco WLAN Layer 3 Security	619
AAA	620
RADIUS vs. TACACS+	621
Configuring AAA	622
Configuring RADIUS	623
Configuring TACACS+	625
Remote Access and Site-to-Site VPNs	627
The Benefits of a VPN	628
The Two Types of VPNs	629
Site-to-Site VPNs	630
Remote Access VPNs	632
The IPSec Protocol	634
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.	635
<i>IPSec Data Integrity Methods</i>	636
<i>IPSec Authentication Methods</i>	637
GRE Tunnels	638
Differences Between Secure VPNs and GRE Tunnels	639
Configuring GRE Tunnels	640
Verifying GRE Tunnels	644
DMVPN	646
DMVPN Hub-and-Spoke Topology (Phase 1)	647
DMVPN Hub-and-Spoke Topology (Phase 2 and 3)	648
Summary	649
Review Question 1	651
Review Question 2	653
Lab Exercises	655
Module 9: Automation and Programming	657
Overview	658
Objectives	658
Administrative Overhead	660
The Logical Network	661
Control Plane	662
Data Plane	663
Management Plane	664
Application Plane	665
Device Management on Traditional Networks	666

Device Management on Controller-Based Networks.....	667
SDN and Cisco SDA	668
Underlay Network.....	669
Overlay Network.....	670
Fabric.....	671
Northbound APIs	672
<i>The REST API</i>	673
Southbound APIs	679
NETCONF	680
RESTCONF	681
OpFlex	682
OpenFlow	682
OnePK	682
Cisco DNA Center	683
Configuration Management Mechanisms	684
Puppet	685
Chef	686
Ansible.....	687
<i>Puppet Bot</i>	688
<i>Salt</i>	688
<i>Salt SSH</i>	688
Summary	689
Review Question 1.....	691
Review Question 2	693
Review Question 3	695
Module 10: Preparing for the CCNA Exam.....	697
Overview	698
Objectives	698
Types of Exam Experiences	699
How to Schedule Your Exam	700
What to Expect When Testing Online	701
What to Expect on Exam Day at the Testing Center	703
Arrive Early	704
Bring Only What You Need	705
Identify Yourself.....	706
Take the Test	707
Finish the Test	708
What to Expect if You Fail	709
What to Expect if You Pass	710
Recommendations for Additional Study	711
ExSim-Max Practice Exams.....	711

NetSim Network Simulator	711
Boson Instructor-Led Training	711
Summary	712
Review Question 1	713
Review Question 2	715
Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.	
Index	717

Module 1

Network Fundamentals

Network Fundamentals Overview

- The OSI model
- Network components
- Network topology architectures
- Interfaces and cabling

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 fundamentals of networking, discusses some of the characteristics and equipment involved in creating networks, highlights the different types of network topology architectures, and discusses the interface types that are used to connect network devices.

Objectives

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

- Understand the Open Systems Interconnection (OSI) model.
- Understand the differences between network components.
- Understand network topology architectures.
- Understand the advantages and drawbacks between on-premises and cloud-based topologies.
- Understand, configure, and troubleshoot interfaces and cabling.

The OSI Model

Layer	PDU	Format Examples
7 – Application	Data	HTTP, DNS, SMTP
6 – Presentation	Data	MP3, JPG, GIF
5 – Session	Data	PAP, RPC
4 – Transport	Segments	TCP, UDP
3 – Network	Packets	IPv4, IPv6, OSPF, EIGRP
2 – Data Link	Frames	PPP, CDP, Frame Relay
1 – Physical	Bits	USB, FireWire, ADSL

The OSI Model

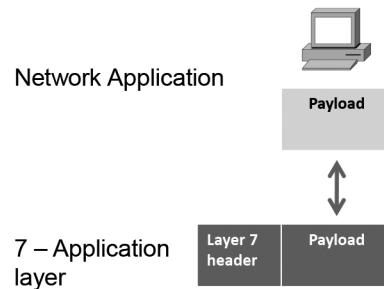
The OSI model is used to divide data communications into seven distinct layers:

- Layer 7 – Application layer
- Layer 6 – Presentation layer
- Layer 5 – Session layer
- Layer 4 – Transport layer
- Layer 3 – Network layer
- Layer 2 – Data Link layer
- Layer 1 – Physical layer

Technologies operating at each layer of the OSI model pass relevant information to technologies operating at adjacent layers. When information is passed down the OSI layers, each layer encapsulates the information with its own formatting and passes it to the next-lower layer; eventually, the information is transmitted as bits at the Physical layer. When information is passed up the OSI layers, each layer removes its formatting, or de-encapsulates the information, and organizes the information so that it can be interpreted by the next-higher layer. The protocol data unit (PDU), or what the information is called at each layer, changes as it moves through the layers.

The functions that are handled at each layer of the OSI model are standardized so that hardware components, applications, and protocols can be designed to interoperate easily. Troubleshooting is also simplified because of how data is handled at each layer of the OSI model.

Application Layer



- Delivers appropriately formatted payload to the correct instance of an application
- Includes protocols such as HTTP, SMTP, and DNS

Application Layer

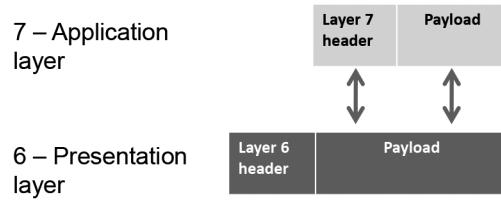
When an application wants to transfer data, the Application layer, Layer 7 of the OSI model, determines whether adequate resources exist for communication. If adequate resources exist, the Application layer will manage communication between applications and then direct data to the correct program. The Application layer is responsible for converting data into a format that is usable by applications and directing the data to the proper application window. If multiple instances of the application exist, such as multiple File Transfer Protocol (FTP) clients or multiple web browsers, the Application layer will ensure that the data is delivered to the appropriate application instance.

When the payload is passed down through the Application layer, it is encapsulated and the Layer 7 header is added before the payload is forwarded to the Presentation layer. When the payload is passed up to the network application from the Presentation layer, the Layer 7 header is removed before the payload is delivered.

Protocols used by the Application layer include the following:

- **Hypertext Transfer Protocol (HTTP)** is used to transfer webpages over the Internet.
- **File Transfer Protocol (FTP)** is used to transfer files over a network.
- **Trivial File Transfer Protocol (TFTP)** is used to transfer files over a network.
- **Dynamic Host Configuration Protocol (DHCP)** is used to assign Internet Protocol (IP) addressing information to clients.
- **Domain Name System (DNS)** is used to translate host names to IP addresses.
- **Simple Mail Transfer Protocol (SMTP)** is used to send email messages.
- **Post Office Protocol 3 (POP3)** is used to receive email messages.
- **Telnet** is used to create a terminal connection to remote devices.
- **Secure Shell (SSH)** is used to create a secure remote terminal connection to a networked device.

Presentation Layer



- Converts data into different formats
- Includes formats such as MP3, JPEG, and GIF

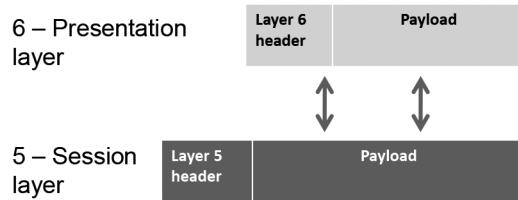
Presentation Layer

The Presentation layer, Layer 6 of the OSI model, is responsible for converting and representing the payload in different formats, including data-based, character-based, image-based, audio-based, and video-based presentation formats. Compression and encryption are often handled by the Presentation layer. When the payload is passed down through the Presentation layer, it is encapsulated and the Layer 6 header is added before the payload is forwarded to the Session layer. When the payload is passed up to the Application layer from the Presentation layer, the Layer 6 header is removed before the payload is delivered.

Formats used by the Presentation layer include the following:

- **Graphics Interchange Format (GIF)**
- **Joint Photographic Experts Group (JPEG)**
- **Motion Picture Experts Group (MPEG)**
- **QuickTime**

Session Layer



- Data traverses the Session layer
- The Session layer establishes and maintains communications
- The Session layer includes protocols such as PAP and RPC

Session Layer

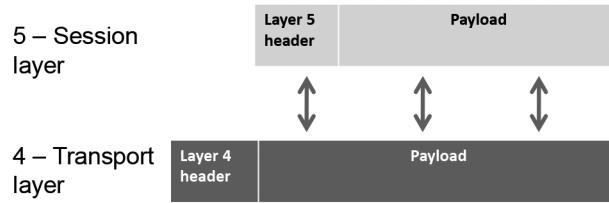
The Session layer, Layer 5 of the OSI model, is responsible for establishing, maintaining, and terminating data communications between applications or devices. A session is made up of requests and responses; the Session layer identifies the data as belonging to a particular session that has been established between two parties and ensures that these requests and responses are sent back and forth between the two parties.

When the payload is passed down through the Session layer, it is encapsulated and the Layer 5 header is added before the payload is forwarded to the Transport layer. When the payload is passed up to the Presentation layer from the Session layer, the Layer 5 header is removed before the payload is delivered.

Protocols that operate at the Session layer include the following:

- **Password Authentication Protocol (PAP)** is an authentication method that uses a simple user name and password pair for authentication.
- **Remote Procedure Call (RPC)** allows a client to initiate a process that is executed on a remote server.

Transport Layer



- Segments traverse the Transport layer
- The Transport layer applies flow control and error detection
- The Transport layer includes protocols such as TCP and UDP

Transport Layer

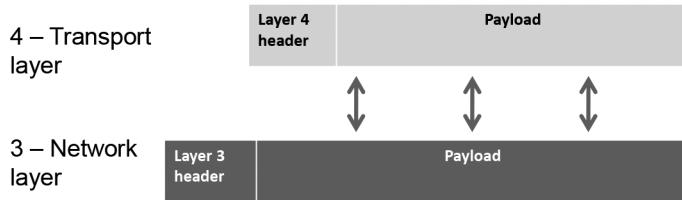
The Transport layer, Layer 4 of the OSI model, is responsible for the error-free delivery of information between devices. In addition, the Transport layer is responsible for flow control and sequencing.

When the payload is passed down through the Transport layer, it is encapsulated and the Layer 4 header is added before the payload is forwarded to the Network layer. Information that is traversing the Transport layer is called a segment. When the payload is passed up to the Session layer from the Transport layer, the Layer 4 header is removed before the payload is delivered.

Protocols that operate at the Transport layer include the following:

- **User Datagram Protocol (UDP)** provides connectionless, unreliable data transfer between networked computers.
- **Transmission Control Protocol (TCP)** provides connection-oriented, reliable data transfer between networked computers.

Network Layer



- Packets traverse the Network layer
- The Network layer includes devices such as routers
- The Network layer includes protocols such as IPv4, IPv6, and IPX

Network Layer

The Network layer, Layer 3 of the OSI model, is responsible for logical addressing and routing on a network. Logical addressing methods include those defined by IP version 4 (IPv4) and IP version 6 (IPv6).

When the payload is passed down through the Network layer, it is encapsulated and the Layer 3 header is added before the payload is forwarded to the Data Link layer. Information that is traversing the Network layer is called a packet. When the payload is passed up to the Transport layer from the Network layer, the Layer 3 header is removed before the payload is delivered.

Examples of protocols that are used at this layer include the following:

- **IP version 4 (IPv4)** is used to uniquely identify devices on a network.
- **IP version 6 (IPv6)** is used to uniquely identify devices on a network.
- **Open Shortest Path First (OSPF)** is a link-state routing protocol.
- **Enhanced Interior Gateway Routing Protocol (EIGRP)** is a Cisco-created hybrid routing protocol.

Data Link Layer



- Frames traverse the Data Link layer
- The Data Link layer includes devices such as switches
- The Data Link layer includes protocols such as Ethernet, Frame Relay, Token Ring, PPP, and CDP

Data Link Layer

The Data Link layer, Layer 2 of the OSI model, defines how devices communicate over a network and is responsible for managing physical addressing and switching on a network. For example, physical addresses, which are also known as Media Access Control (MAC) addresses, are handled by the Data Link layer.

When the payload is passed down through the Data Link layer, it is encapsulated and the Layer 2 header is added before the payload is forwarded to the Physical layer. Information that is traversing the Data Link layer is called a frame. When the payload is passed up to the Network layer from the Data Link layer, the Layer 2 header is removed before the payload is delivered.

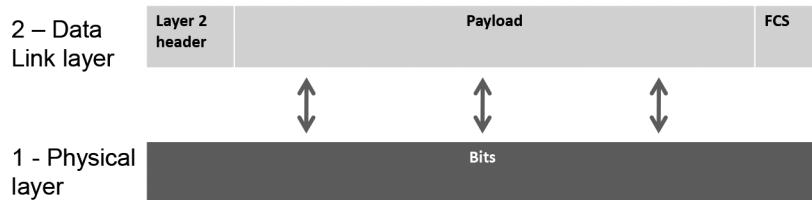
Data Link layer devices include switches and bridges. Switching is handled at the Data Link layer because switches use physical addresses to forward packets to the correct port.

Protocols that operate at the Data Link layer include the following:

- **Ethernet**, which can operate at Layer 1 and Layer 2
- **Frame Relay**
- **Point-to-Point Protocol (PPP)**
- **Cisco Discovery Protocol (CDP)**

Like Ethernet, some portions of the 802.11 wireless standard function at the Data Link layer and some portions function at the Physical layer.

Physical Layer



- Bits traverse the Physical layer
- The Physical layer defines the physical characteristics and transmission of media between devices
- The Physical layer includes devices such as NICs, hubs, and repeaters
- The Physical layer includes protocols such as Ethernet, USB, and ADSL

Physical Layer

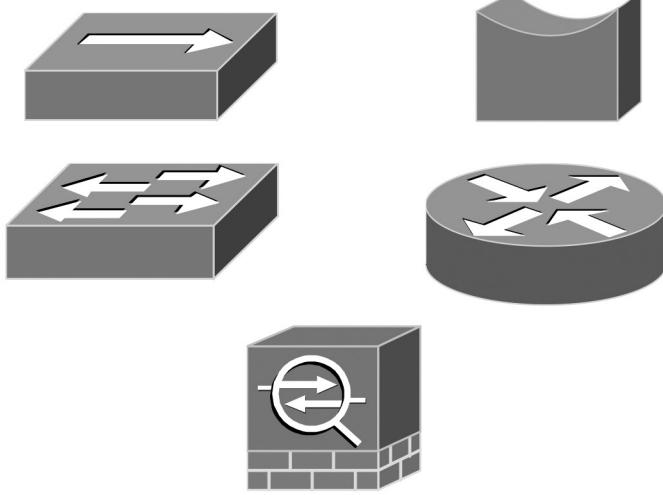
The Physical layer, or Layer 1, of the OSI model defines how bits are passed over a medium. Bits can be passed electrically, mechanically, optically, or by radio signals. Media can include coaxial cable, twisted-pair copper cable, and fiber-optic cable. The Physical layer also includes the connectors used to connect the cables to the devices that operate at this layer.

The Physical layer passes bits between the Data Link layer and physical devices on a network. Examples of devices that operate at this layer are network interface cards (NICs), hubs, and repeaters. The devices that operate at the Physical layer receive and forward bits to other devices without making any path determination about the bits. That is, these devices simply forward the bits to the next hop in the network.

Protocols that operate at the Physical layer include the following:

- **Ethernet**
- **Universal serial bus (USB)**
- **Asynchronous Digital Subscriber Line (ADSL)**

Network Devices



Network Devices

This section covers several different network devices: hubs, bridges, switches, routers, endpoints, firewalls, Intrusion Prevention System (IPS) devices, wireless access points (WAPs), and controllers.

Hubs



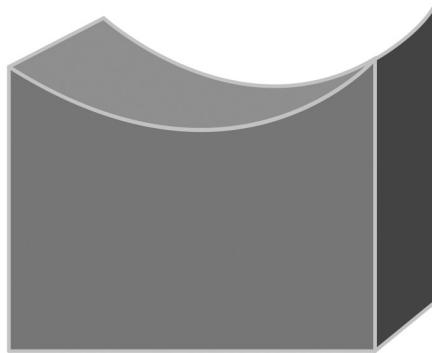
Hubs

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 will 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 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 collisions. With CSMA/CD, a transmitting device listens to the network segment before it attempts to send data. If no transmissions are detected, the transmitting device will send its data and then listen to determine whether a collision occurs. If a collision is detected, each of the transmitting devices involved in the collision will wait 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.

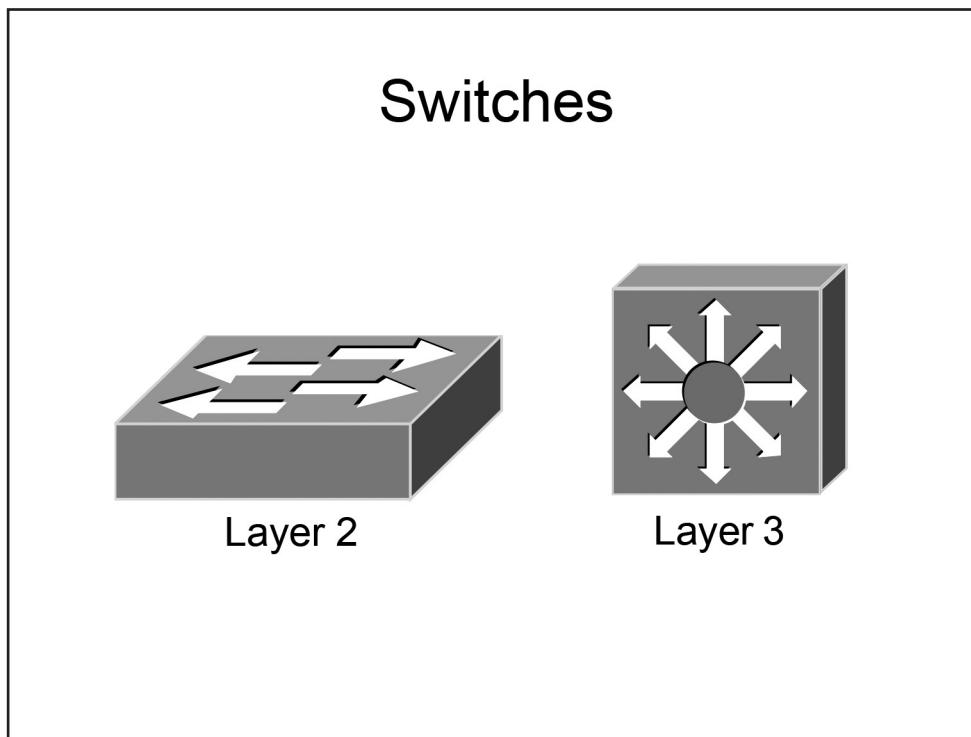
Bridges



Bridges

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

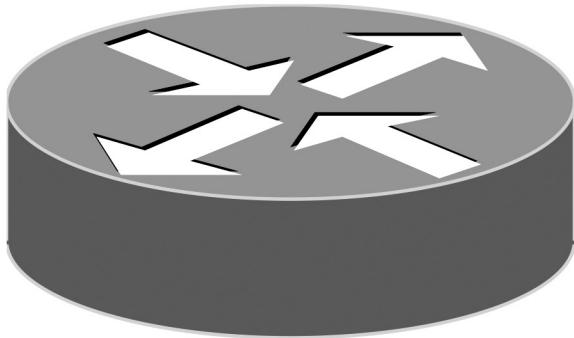
Like bridges, switches can be used to provide network connectivity to endpoint devices. Switches can operate at Layer 2 or Layer 3. Layer 2 switches function similarly to bridges, whereas Layer 3 switches add routing functionality.

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.

Layer 2 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, which is discussed in greater detail in [The Cam Table](#) section of **Module 5: Switching and Network Access**. 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 future 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 Layer 2 switch will reside within a single broadcast domain. Layer 3 switches can use virtual local area networks (VLANs) to separate the broadcast domains.

Routers



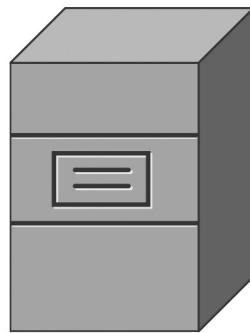
Routers

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, which is discussed in greater detail in [The TCAM Table](#) section of **Module 5: Switching and Network Access**. 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 will be dropped and an Internet Control Message Protocol (ICMP) Destination Unreachable error message will be sent to the interface from which the packet was received.

Servers

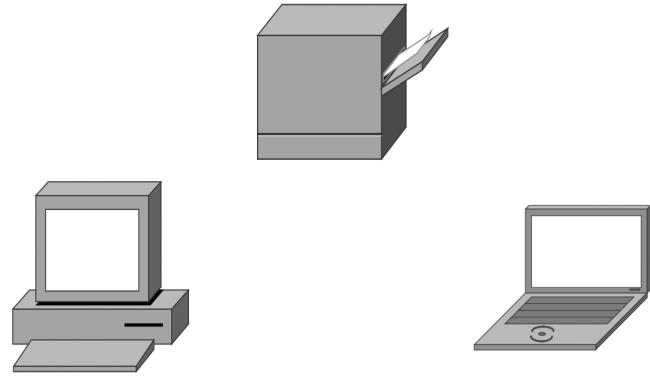


Servers

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 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.

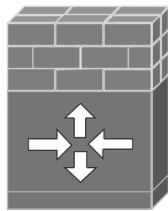
Endpoints



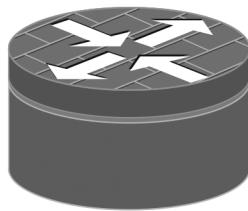
Endpoints

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

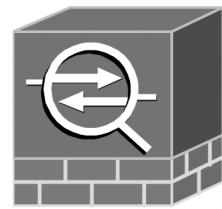
Next-Generation Firewalls and IPS Devices



Cisco IOS
Firewall



Router with
Firewall



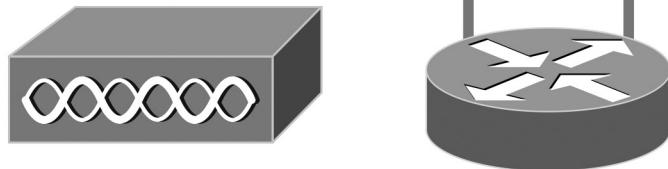
Cisco
ASA/IPS

Next-Generation Firewalls and IPS Devices

A firewall is a device that filters packets inbound from untrusted networks. Typically, a firewall filters packets without analysis. Cisco Adaptive Security Appliances (ASAs) are next-generation, multifunction appliances that can provide firewall, virtual private network (VPN), intrusion prevention, and content security services.

An IPS is a device that detects and can automatically mitigate network intrusion attempts. An IPS can determine whether a given packet might be malicious and, depending on the results of its tests, take various actions to mitigate the threat.

WAPs



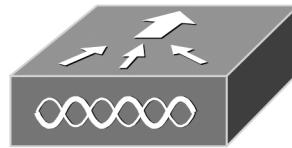
WAPs

A WAP is a device that enables wireless clients to connect to a wireless LAN (WLAN) by using radio frequency (RF) communication. WAPs are available in single-band or dual-band form. WAPs that are designed for modern versions of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard are typically dual-band WAPs. One band operates at the 2.4-gigahertz (GHz) frequency while the other operates at the 5-GHz frequency.

Controllers



DNA Center



WLAN
Controller

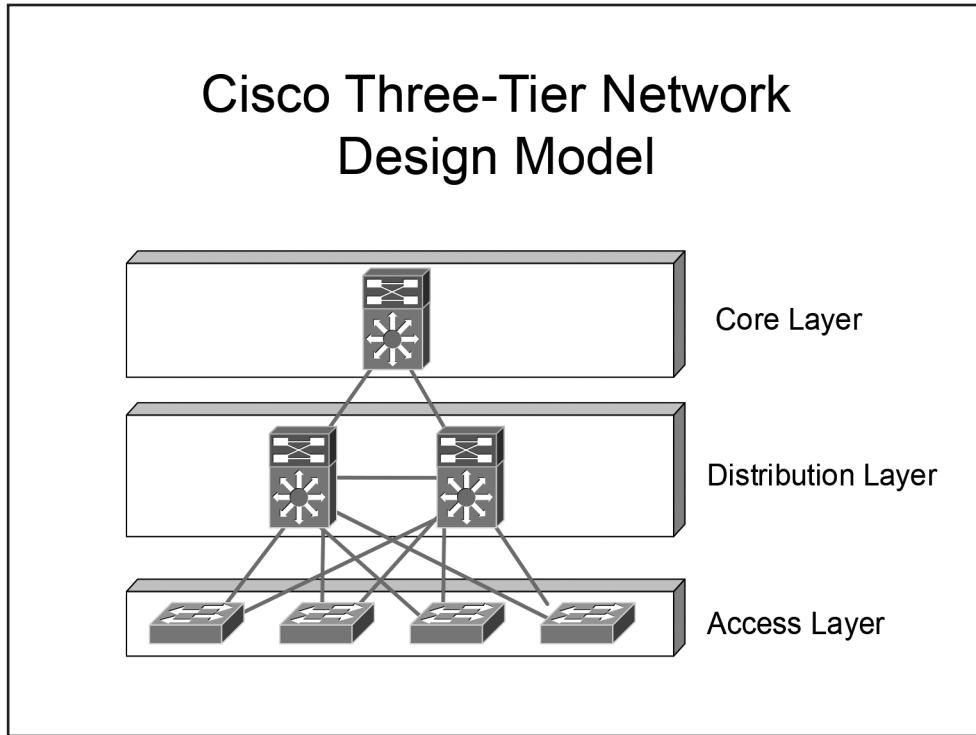
Controllers

Controllers manage other network devices. Examples of controllers include the Cisco DNA Controller and wireless LAN controllers (WLCs).

Cisco DNA is a software-centric network architecture that uses a combination of Application Programming Interfaces (APIs) and a graphical user interface (GUI) to simplify network operations. The Cisco DNA controller, which is similar to a Software-Defined Networking (SDN) controller, is the central component of a Cisco Software-Defined Access (SDA) network. Cisco SDA is a Cisco-developed means of building local area networks (LANs) by using policies and automation.

Whereas autonomous WLANs require that each access point (AP) handle both traffic and management functions, Cisco Unified Wireless Networks use WLCs to centralize security configurations among APs and to provide mobility services at both Layer 2 and Layer 3 of the OSI model. WLCs provide user authentication, RF management, security and policy enforcement, and QoS to lightweight APs (LAPs).

A LAP requires a WLC in order to function. If the WLC becomes unavailable, the LAP will reboot and drop all client associations until the WLC becomes available or until another WLC is found on the network. A LAP communicates over Lightweight Access Point Protocol (LWAPP) to establish two tunnels to its associated WLC: one tunnel for data and one tunnel for control traffic. Traffic sent through the data tunnel is not encrypted, but traffic sent through the control tunnel is encrypted.

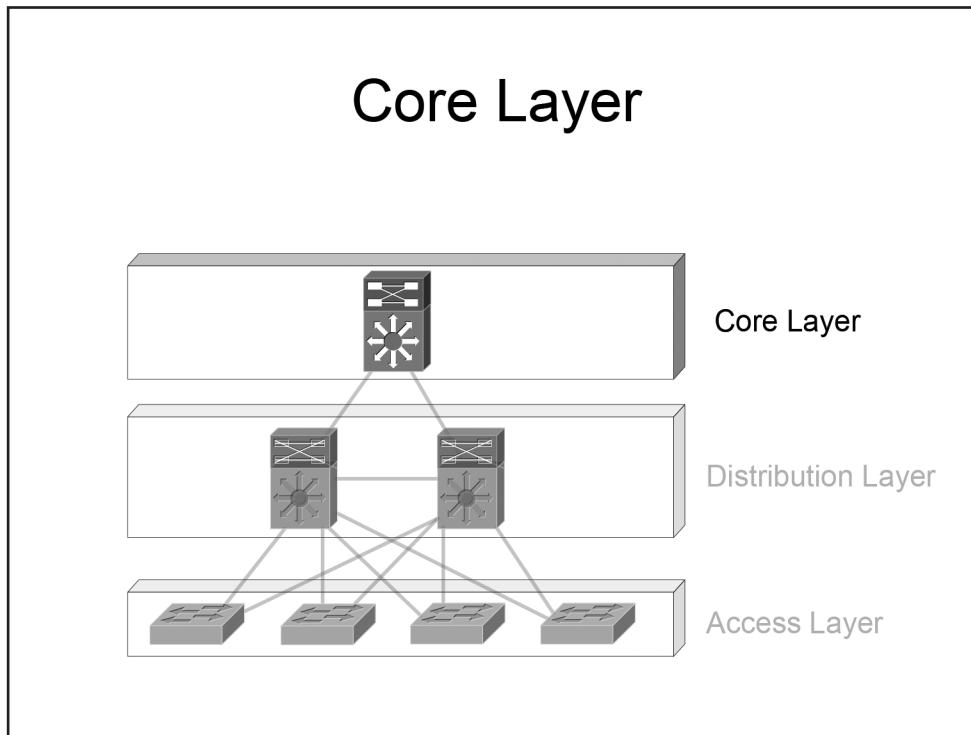


Cisco Three-Tier Network Design Model

The three-tier network design model is a Cisco hierarchical model that divides a network into three distinct components:

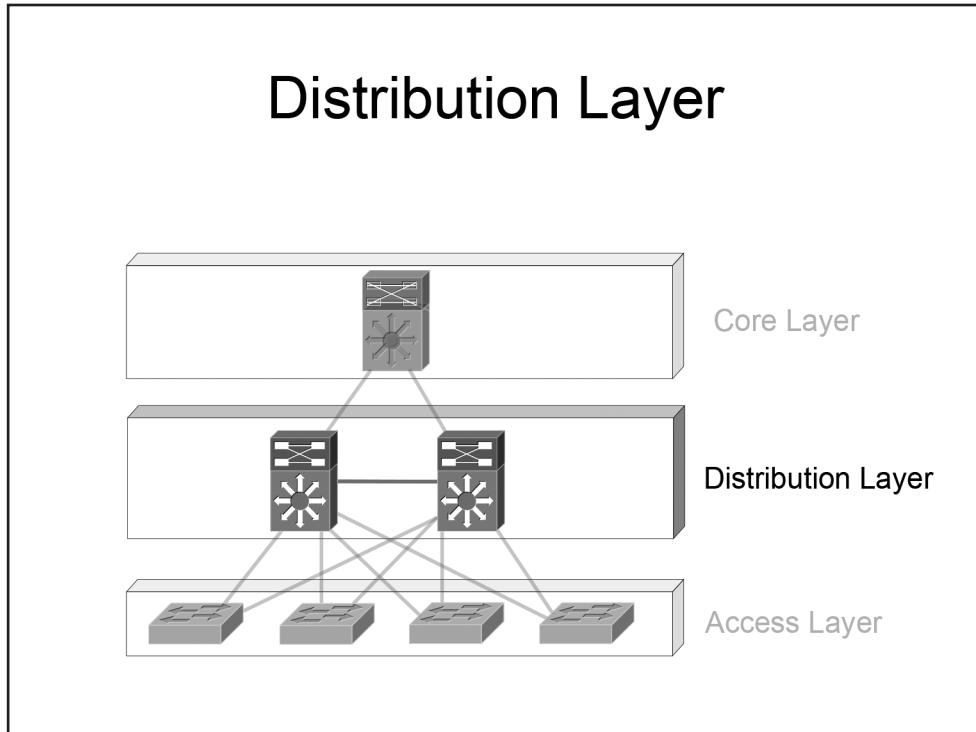
- Core layer
- Distribution layer
- Access layer

Dividing a network design into the layers above simplifies the scalability and troubleshooting of a network.



Core Layer

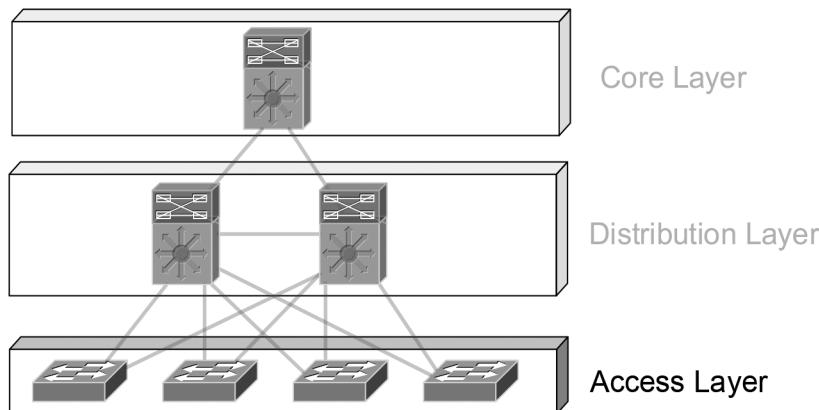
The core layer typically provides the fastest switching path in the network. As the network backbone, the core layer is primarily associated with low latency and high reliability.



Distribution Layer

The distribution layer, which is sometimes referred to as the aggregation layer, provides route filtering and interVLAN routing. Management ACLs and IPS filtering are typically implemented at the distribution layer. The distribution layer serves as an aggregation point for access layer network links. Because the distribution layer is the intermediary between the access layer and the core layer, the distribution layer is the ideal place to enforce security policies and to perform tasks that involve packet manipulation, such as routing. Summarization and next-hop redundancy are also performed in the distribution layer.

Access Layer



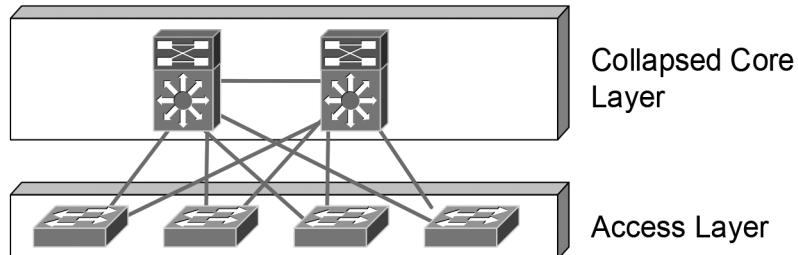
Access Layer

The access layer provides Network Admission Control (NAC). NAC is a Cisco feature that prevents hosts from accessing the network if they do not comply with organizational requirements, such as an updated antivirus definition file. NAC Profiler automates NAC by automatically discovering and inventorying devices attached to the LAN.

The access layer serves as a media termination point for servers and endpoints. Because access layer devices provide access to the network, the access layer is the ideal place to perform user authentication and port security.

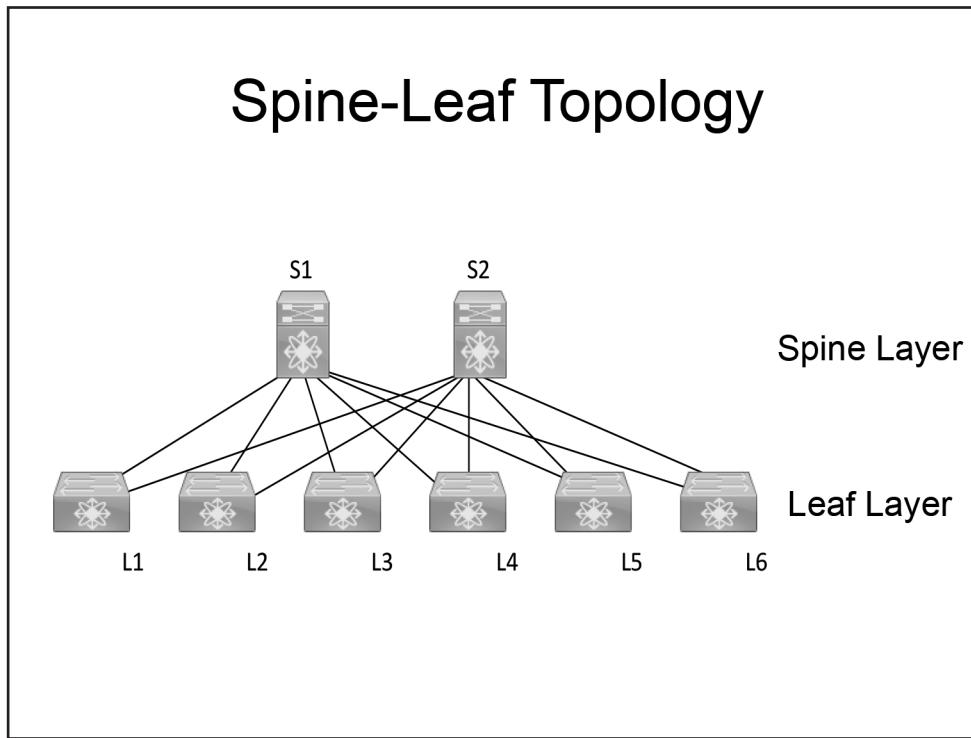
Traditionally the access layer consists of OSI Layer 2 switches only; when a packet must be routed to a separate network, the packet must first be sent to a Layer 3 device in the distribution layer before it can be routed to the correct destination. However, some designs employ Layer 3 switches in the access layer, which in effect moves the demarcation between Layer 2 and Layer 3 switching to the access layer.

Cisco Two-Tier Network Design Model



Cisco Two-Tier Network Design Model

The two-tier network design model is sometimes called the collapsed-core network design model. In the two-tier network design model, the functionality of the core layer is collapsed into the distribution layer. The functionality of the core layer is provided by the distribution layer and a distinct core layer does not exist. However, the distribution layer infrastructure must be sufficient to meet the design requirements.



Spine-Leaf Topology

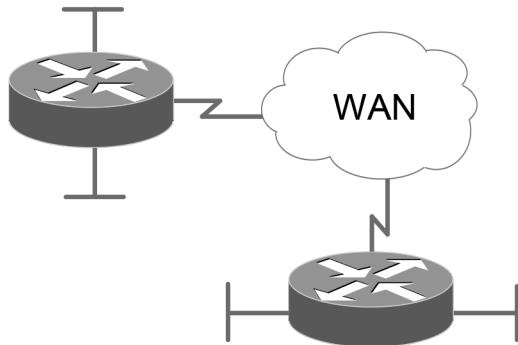
Spine-leaf topologies are generally seen in data centers. A spine-leaf topology is a two-tier, partial-mesh network architecture in which every lower-tier leaf switch connects to every top-tier spine switch. However, the leafs and spines are not connected to one another.

Spine switches connect to the network backbone. If link oversubscription occurs, a new spine switch can be added and connections to every leaf switch can be established. Leaf switches connect to nodes, such as servers. When port capacity becomes a problem with the addition of new servers, a new leaf can be added and connections to every spine switch can be established.

Because a spine node has a connection to every leaf node, the scalability of the fabric is limited by the number of ports on the spine node, not by the number of ports on the leaf node. In addition, redundant connections between a spine and leaf pair are unnecessary because the nature of the topology ensures that each leaf has multiple connections to the network fabric. Therefore, each spine node requires only a single connection to each leaf node.

The spine and leaf nodes create a scalable network fabric that is optimized for east-west data transfer, which in a data center is typically traffic between an application server and its supporting data services, such as database or file servers. This topology enables nonlocal traffic to pass from any ingress leaf interface to any egress leaf interface through a single, dynamically selected spine node. Because every traffic flow must pass through no more than two network hops, throughput and latency become much more even and predictable.

WAN Topologies



- Leased lines
- Frame relay
- ATM
- MPLS
- Metro ethernet

WAN Topologies

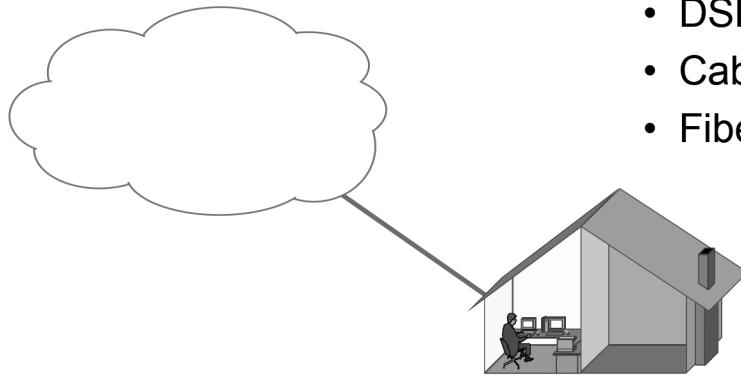
A wide area network (WAN) is a network that covers a large geographical area. Often, a WAN is spread across multiple cities or countries. The largest example of a WAN is the Internet.

Geographically dispersed LANs are typically connected together by a WAN. WAN connectivity is generally supplied by a service provider. Customers can connect LANs by tunneling traffic securely over the WAN, often by using a site-to-site VPN. The service provider's routers and switches are invisible to the customer's LAN. Therefore, a WAN is often represented on a topology diagram as a cloud.

Older WAN technologies include T1 and T3 leased lines, which provide point-to-point connectivity, and Frame Relay and Asynchronous Transfer Mode (ATM), which provide point-to-multipoint connectivity. Newer WAN technologies include Multiprotocol Label Switching (MPLS) and Metro Ethernet.

SOHO Topologies

- Satellite
- DSL
- Cable
- Fiber



SOHO Topologies

As telecommuting becomes more prevalent, small office/home office (SOHO) topologies are becoming commonplace. A SOHO topology is typically a small LAN or WLAN with one or more computers. The LAN or WLAN is connected to a service provider network, typically over satellite, Digital Subscriber Line (DSL), cable, and fiber to the Internet. Satellite and DSL are older and slower technologies, whereas cable and fiber are faster technologies.

On-Premises and Cloud Deployments

- On-Premises
 - Gives an organization the most customization and control
 - Has higher up-front cost
 - Requires staff
- Cloud
 - Gives the service provider full control
 - Has lower up-front cost
 - Includes monthly fee
 - Does not require staff

On-Premises and Cloud Deployments

On-premises deployments, which are also known as traditional deployments, involve the purchasing, configuration, and maintenance of the deployment at the local level. This means that an organization has full control over the network. For example, a company that deploys an on-premises badge access solution will have complete control of the system and its data. However, the company must pay for the hardware and software. In addition, the company must hire staff to maintain the deployment, thereby increasing costs.

A cloud deployment is owned and maintained by the cloud hosting provider, meaning the provider has control over both the hardware and software. A cloud deployment typically requires a monthly usage fee and therefore might have a lower up-front cost than an on-premises deployment. In addition, the customer does not have to hire, train, and employ technical staff to maintain the deployment. However, a cloud-based deployment is less likely to offer an organization more customization and control than an on-premises deployment.

Although cloud deployments can decrease operational costs, they can increase risks. When Internet service is interrupted, access to those resources is also interrupted. Also, a company's confidential data might be stored on a third-party server for which the company does not have full administrative control; if security is not adequate, data breaches can occur.

The National Institute of Standards and Technology (NIST) defines three service models in its definition of cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These service modules will be discussed in the following sections.



- Provides consumer with access to licensed applications but no management control
- Is least likely to require change to the consumer's network
- Includes applications such as Office 365, Google Drive, and iCloud

SaaS

The SaaS model enables a consumer to access applications that are running in the cloud infrastructure but does not enable the consumer to manage the cloud infrastructure or to configure the provided applications. Of the three models, SaaS exposes the least amount of the consumer's network to the cloud and is the least likely to require changes to the consumer's network design. A company uses SaaS when it licenses a service provider's office suite and email service and delivers it to end users through a web browser. SaaS providers use an Internet-enabled licensing function, a streaming service, or a web application to provide end users with software that might otherwise be installed and activated locally. Web-based email clients are examples of SaaS. Other examples include Microsoft Office 365, Google Drive, and iCloud, all of which enable the user to create or manipulate data by using the provider's tools.

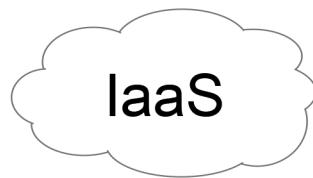


PaaS

- Provides consumer with access to the provider's infrastructure and development tools to serve cloud-based applications or services
 - An example is using MySQL and Apache services to build a CRM platform

PaaS

The PaaS model provides a consumer with a bit more freedom than the SaaS model by enabling the consumer to install and possibly configure provider-supported applications in the cloud infrastructure. A company that uses a provider's development tools or API to deploy specific cloud-based applications or services is using PaaS. For example, by using the PaaS model, an organization could use a third party's MySQL database and Apache services to build a cloud-based customer relationship management (CRM) platform.



- Consumer can provision hardware and network resources
- Consumer can install OSs and applications
- Servers can be physical or virtual
- Examples include SQL, web, DNS, and DHCP hosting solutions

IaaS

The IaaS model provides the greatest degree of freedom by enabling a consumer to provision processing, memory, storage, and network resources within the cloud infrastructure. IaaS also enables a consumer to install operating systems (OSs) and applications. However, with IaaS, the cloud infrastructure remains under the control of the service provider. A company uses IaaS when it hires a service provider to deliver cloud-based processing and storage that will house multiple physical or virtual hosts that can be configured in a variety of ways.

For example, suppose a company wants to establish a web server farm by configuring multiple Linux Apache MySQL PHP (LAMP) servers. The company could save hardware costs by virtualizing the farm and using a provider's cloud service to deliver the physical infrastructure and bandwidth for the virtual farm. Control over the OS, software, and server configuration would remain the responsibility of the organization, whereas the physical infrastructure and bandwidth would be the responsibility of the service provider. Another example of IaaS is using a third party's infrastructure to host corporate DNS and DHCP servers.

Interfaces and Cabling

- Ethernet
- Serial
- Fiber-optic
- PoE

Interfaces and Cabling

Cisco routers support a wide variety of physical interfaces. Because the needs of network implementations vary from design to design, Cisco offers both fixed-configuration routers and modular routers. Fixed-configuration routers have a limited number of integrated interfaces and do not support the addition or replacement of interfaces. This style of router is well suited for SOHO implementations, which typically do not require very many interfaces and do not tend to experience considerable changes to their infrastructure. Cisco's modular routers generally come with a small number of integrated LAN interfaces, but they also offer expansion slots that can support additional types and numbers of interfaces.

This section covers Ethernet, serial, and fiber-optic cabling. In addition, this section covers Power over Ethernet (PoE) interfaces.

Copper Cables



Copper Cables

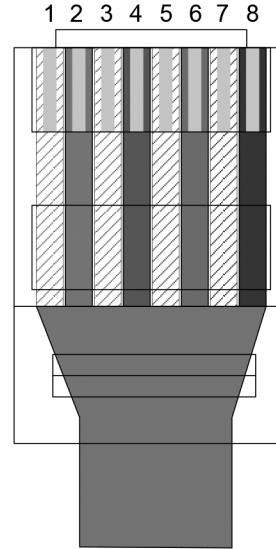
Copper is a soft metal that is an excellent conductor of both heat and electricity. Copper wires are used to transmit data as electrical signals. For example, Ethernet, Token Ring, and Copper Distributed Data Interface (CDDI) networks all use copper cabling to transmit data. Most modern Ethernet networks use copper unshielded twisted-pair (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 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



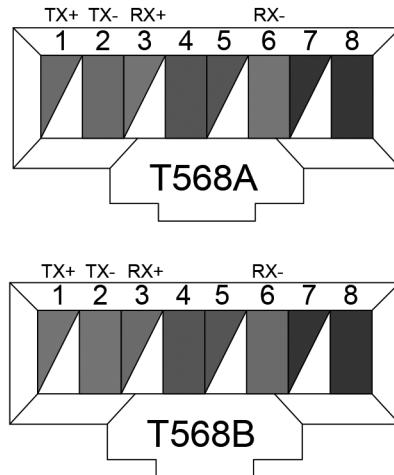
Connecting UTP With RJ-45

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.

Connecting UTP With RJ-45

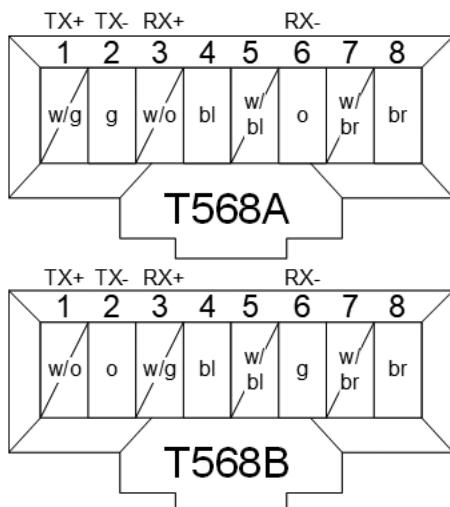
- Wires connect to pins based on one of two color-coded standards
- The transmit and receive wires in the T568A standard are inverse in the T568B standard



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, whereas the T568B standard is compatible with a standard established by AT&T.

It is important to note 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.

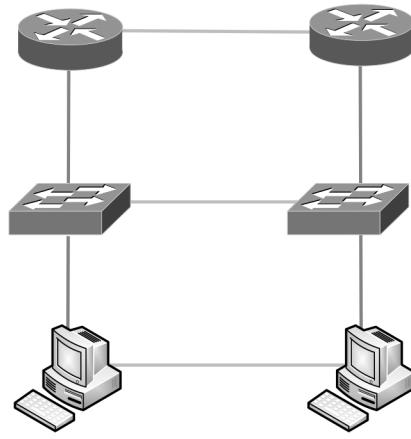


The T568B standard uses the white/orange and orange wires for Pins 1 and 2, respectively and uses the white/green and green wires for Pins 3 and 6, respectively. Therefore, the T568B standard transmits over white/orange and orange and receives over white/green and green.

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



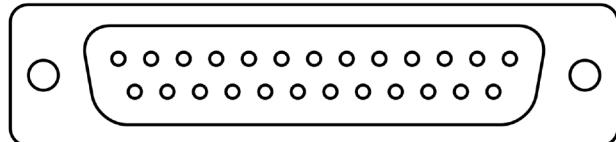
Understanding Straight-Through and Crossover Cables

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 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 T568-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.

Serial Cables



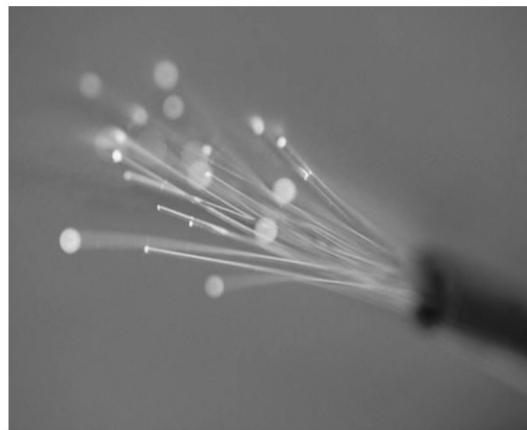
Serial Cables

Serial cables are also copper cables. However, serial cables are not as commonly used as they once were. Most service provider equipment has transitioned to Ethernet and fiber-optic cables.

Cisco devices support five types of serial cables. However, the most commonly used serial cable is a 25-pin EIA/TIA-232 cable with a DB-25 connector at either end.

One end of a serial cable is the data communications equipment (DCE) end and the other end is the data terminal equipment (DTE) end. The most important thing to remember about serial cables is that the DCE end provides clocking to the DTE end. If the correct clock rate is not configured on the DTE end, physical connectivity between the devices cannot be established.

Fiber-Optic Cables



Fiber-Optic Cables

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.

Fiber-Optic Cable Types

- Multimode fiber
 - Can use a 62.5-micron core
 - Typically uses 850-nm wavelength frequency range
 - Used for distances of less than 2 km
- Single-mode fiber
 - Can use a 9-micron core
 - Typically uses 1,310-nm or 1,550-nm wavelength frequency range
 - Used for distances of more than 80 km

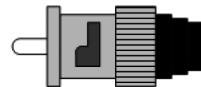
Fiber-Optic Cable Types

Multimode fiber (MMF) can use a 62.5-micron core and a wavelength of 850 nanometers (nm). Additionally, MMF is typically used for distances less than 2 kilometers (km). When light is transmitted through a fiber-optic cable, the light is only propagated by the fiber core at certain angles, or modes. The light transmitted into the core of an MMF cable is typically in the 850-nm or 1,300-nm frequency range. Because MMF has a relatively large core (50 micron or 62.5 micron) that permits many different angles of light, the signal becomes dispersed over great distances. This dispersion effectively limits the usable distance of MMF to 2 km. MMF is typically used in campus designs that require at least 1 Gbps of bandwidth and network runs that are less than 2 km.

Single-mode fiber (SMF) typically uses a 9-micron core. The light transmitted into the core of an SMF cable is typically in the 1,310-nm or 1,550-nm frequency range. Because SMF has a relatively small core that permits very few angles of light, the signal does not become very dispersed over great distances. The limited dispersion of SMF enables network runs of 80 km or more. SMF is typically used in campus designs that require at least 10 Gbps of bandwidth and network runs that are greater than 2 km.

Fiber-Optic Cable Connectors

- ST



- SC



- LC



- MT-RJ (miniature RJ-45)

Fiber-Optic Cable Connectors

Older fiber-optic cables use ST and SC connectors. The older ST connector is a round, spring-loaded connector. The SC connector is typically a square-shaped connector that snaps into its receptacle; it is available in both single and duplex varieties.

Newer fiber-optic cables can also use LC or MT-RJ connectors. LC connectors are small form factor connectors that are available in both single and duplex varieties. Similar to the SC connector, the LC connector snaps into its receptacle. However, LC connectors are half the size of SC connectors. MT-RJ connectors look like miniature RJ-45 Ethernet copper connectors. Like the LC connector, the MT-RJ connector can provide a duplex interface in a single connector.

PoE

- IEEE 802.3af
 - Class 0: 0.44 W to 12.94 W
 - Class 1: 0.44 W to 3.84 W
 - Class 2: 3.84 W to 6.49 W
 - Class 3: 6.49 W to 12.95 W
- IEEE 802.3at (PoE Plus)
 - Class 4: 12.95 to 25.50 W

PoE

PoE provides in-line power for connected IP phones and WAPs over the same cable that carries voice and data traffic. As a result, PoE eases Voice over IP (VoIP) and WLAN implementations because you are not limited to installing devices next to existing power sources. As long as there is a network jack available, the device can draw its power from the network cable, allowing placement where the device will be most accessible.

A Cisco Catalyst switch can provide power to both Cisco and non-Cisco devices that support either the IEEE 802.3af standard, the IEEE 802.3at standard, or the Cisco prestandard method. For a Catalyst switch to successfully provide power, both the switch and the device must support the same PoE method. After a common PoE method is determined, CDP messages sent between Catalyst switches and Cisco devices can further refine the amount of allocated power.

The 802.3af standard divides power requirements into the following classes:

- Class 0: 0.44 – 12.94 watts (W)
- Class 1: 0.44 – 3.84 W
- Class 2: 3.84 – 6.49 W
- Class 3: 6.49 – 12.95 W

Class 0 is the default PoE level. Devices that are classified as Class 0 will draw as much power as they need, up to the maximum amount.

The 802.3at PoE Plus standard adds a fourth class, Class 4, which is used for high-power PoE devices. Class 4 provides 12.95 W to 25.50 W of power.

Cisco Catalyst switches monitor and police PoE ports. If a device attempts to draw more power than a port is configured to provide, a syslog message will be issued and the port will be shut down and enter the error-disabled state.

Troubleshooting Interfaces and Cabling

- Excessive noise
- Collisions
- Late collisions
- Duplex mismatch
- Speed mismatch

Troubleshooting Interfaces and Cabling

This section covers several common interface and cabling issues that occur and how to troubleshoot those issues. Specifically, it includes the following issues:

- Excessive noise
- Collisions
- Late collisions
- Duplex mismatch
- Speed mismatch
- Broadcast storms

Excessive Noise

- Results in transmission errors
- Is caused by
 - Damaged cables
 - Improper cable types
- Can be verified by issuing the **show interfaces** command

Excessive Noise

Excessive noise is a problem that can cause transmission errors. Noise errors are typically caused by a physical media problem. For example, a damaged cable could cause excessive noise errors to occur. Using the wrong cable type could also cause excessive noise errors. If you determine that a device is experiencing excessive noise problems, you should check the physical media attached to the device.

Excessive noise errors are detectable by viewing output from the **show interfaces** command. A high number of cyclic redundancy check (CRC) errors along with a low number of collisions could indicate an excessive noise issue.

The following output of the **show interfaces** command provides an example of a possible excessive noise issue:

```
SwitchA#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is X2345, address is 00c0.1234.5678
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto-speed
  Last input 0:00:05, output 0:00:03, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
119641 packets input, 21282118 bytes, 0 no buffer
Received 92561 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 12345 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
149712 packets output, 14562789 bytes, 0 underruns
0 output errors, 47 collisions, 5 interface resets
0 babbles, 0 late collision, 7 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

The relevant entries in the output have been emphasized. In this example, 12,345 CRC errors have been reported, while only 47 collisions have been detected. In such a scenario, you should verify that the cables are not damaged and that they have been correctly installed.

Collisions

- Result in network congestion and could result in dropped packets
- Are caused by
 - Too many nodes on a network segment
 - Malfunctioning NICs in host computers
 - Duplex mismatch errors
- Can be verified by issuing the **show interfaces** command

Collisions

Too many collisions can cause network congestion due to packets being retransmitted as a result of the collisions. Collisions can be caused by several factors. Malfunctioning NICs in host computers can cause jabber on the network, which can cause collisions to occur. Too many devices transmitting on one network segment could also cause collisions. Another potential cause for collisions is duplex mismatch errors between devices. For example, if a switch port is configured for full duplex and a hub is connected to the port, it is possible that collisions could occur; a hub can operate only in half-duplex mode. Resolving collision errors may involve replacing NICs in client computers, creating additional network segments, or reconfiguring duplex settings, depending on what is identified as the cause of the excessive collision issues.

The number of collisions that occur on an interface can be viewed by issuing the **show interfaces** command. A high number of collisions could indicate transmission problems on the network.

The following output of the **show interfaces** command indicates that a problem could be causing too many collisions to occur on the network:

```
SwitchA#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is X2345, address is 00c0.1234.5678
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto-speed
  Last input 0:00:05, output 0:00:03, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
```

```
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    119641 packets input, 21282118 bytes, 0 no buffer
    Received 92561 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    149712 packets output, 14562789 bytes, 0 underruns
    0 output errors, 12345 collisions, 5 interface resets
    0 babbles, 0 late collision, 7 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

The relevant entry in the output has been emphasized. In this output, 12,345 collisions have occurred on the FastEthernet 0/1 interface.

Late Collisions

- Result in network congestion because frames have to be re-sent
- Are caused by
 - Duplex mismatch errors
 - Network segment is too long
- Can be verified by issuing the **show interfaces** command

Late Collisions

A late collision is a collision that occurs after the 512th bit (64th byte) of a frame has been transmitted by a device. A device detects such a collision if it begins sending a frame and a collision occurs after 512 bits of the outgoing frame have been sent. The amount of time it takes to send the first 512 bits of a frame is dependent on the network technology in use. For example, it takes 51.2 microseconds to send 512 bits over a 10-Mbps Ethernet segment, whereas it only takes 5.12 microseconds to send 512 bits over a 100-Mbps FastEthernet segment. Similar to other collision errors, late collisions can occur as a result of duplex mismatch errors or a network segment that extends farther than the cable length supports. If you notice late collisions occurring on an interface, you should ensure that the duplex settings are configured correctly and that the network segments are not too long.

The number of late collisions that occur on an interface can be viewed by issuing the **show interfaces** command. The number of late collisions detected on an interface are shown in the late collision counter, as shown in the following sample output:

```
SwitchA#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is X2345, address is 00c0.1234.5678
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto-speed
  Last input 0:00:05, output 0:00:03, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Last clearing of "show interface" counters never
```

```
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 119641 packets input, 21282118 bytes, 0 no buffer
  Received 92561 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 input packets with dribble condition detected
 149712 packets output, 14562789 bytes, 0 underruns
  0 output errors, 1 collisions, 5 interface resets
  0 babbles, 100 late collision, 7 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

The relevant entry in the output has been emphasized. In this sample output, 100 late collisions have been detected on the FastEthernet 0/1 interface.

Duplex Mismatch

- Duplex mismatch results in connectivity and performance problems
- Duplex mismatch is indicated by a high number of collisions and late collisions
- Duplex settings can be verified by issuing the **show interfaces status** command

Duplex Mismatch

Duplex mismatch errors can cause a number of problems, including intermittent connectivity, performance problems, a high number of collisions, and late collisions. A duplex mismatch error occurs when the ends of a network link are configured with different duplex settings. Cisco devices support half-duplex mode and full-duplex mode, but both ends of the link should be configured to use the same duplex setting. If they are configured with different duplex settings, network performance could be adversely affected due to collisions being detected. One symptom of a duplex mismatch is that the half-duplex side of the connection will report late collisions. The full-duplex side, on the other hand, will report runts, Frame Check Sequence (FCS) errors, and alignment errors. You can configure the duplex settings explicitly, or you can configure the link to autonegotiate the duplex settings.

Duplex mismatches can sometimes be difficult to diagnose because the problems might be intermittent and the interface will report an up/up state. If you suspect that a duplex mismatch error is causing network problems, you can use the **status** parameter of the **show interfaces** command to verify the duplex settings for all the interfaces on a device. The following displays sample output from the **show interfaces status** command:

```
SwitchA#show interfaces status
Port      Name          Status       Vlan     Duplex    Speed Type
Fa0/1           connected    1         a-full   a-100  10/100BaseTX
Fa0/2           connected    1         a-full   a-100  10/100BaseTX
Fa0/3           connected    1         a-full   a-100  10/100BaseTX
Fa0/4           connected    1         a-full   a-100  10/100BaseTX
Fa0/5           notconnect   1         auto    auto   10/100BaseTX
Fa0/6           notconnect   1         auto    auto   10/100BaseTX
```

Fa0/7	notconnect	1	auto	auto	10/100BaseTX
Fa0/8	notconnect	1	auto	auto	10/100BaseTX
Fa0/9	notconnect	1	auto	auto	10/100BaseTX
Fa0/10	notconnect	1	auto	auto	10/100BaseTX
Fa0/11	connected	1	a-full	a-100	10/100BaseTX
Fa0/12	connected	1	a-full	a-100	10/100BaseTX
Gi0/1	notconnect	1	auto	auto	10/100BaseTX
Gi0/2	notconnect	1	auto	auto	10/100BaseTX

In this sample output, the interfaces have been configured to autonegotiate the duplex settings, as depicted by the a- prefix before the duplex setting in the output. For example, interface Fa0/1 autonegotiated full-duplex mode.

Autonegotiation is a method of electrical signaling between interfaces to enable the automatic configuration of speed and duplex settings on an interface. Cisco recommends that autonegotiation be enabled on both sides of a link if it is supported. If one side of the link is statically configured, the autonegotiation-enabled side of the link will attempt to operate at the fastest speed that is supported by the remote side of the link. In such a case, the Speed field for the autonegotiation-enabled port will display the word auto. However, setting autonegotiation on only one side of a link can cause configuration problems on the link, such as mismatched duplex settings, because it is not possible to statically configure the duplex settings of a port unless the port speed is statically configured first.

Speed Mismatch

- Speed mismatch prevents the interface from sending traffic
- Speed mismatch is sometimes indicated by a link being in the down state
- Speed settings can be verified by using the **show interfaces status** command

Speed Mismatch

Speed mismatch errors can prevent an interface from sending or receiving traffic. A speed mismatch error occurs when one end of a network link is configured to use a different speed than the other end of the link, such as when one end of a link is configured to transmit at 10 Mbps while the other end of the link is configured to transmit at 100 Mbps. In such a scenario, a link between the two interfaces would not be able to be established and the links would remain in the down state.

Similar to configuring interface duplex, you can explicitly configure the speed setting on an interface or you can configure the link to autonegotiate the speed setting. You can even explicitly configure one end and configure the other end to autonegotiate. In such a scenario, the autonegotiating port can identify the other port's link speed by the electrical signal sent by the port. You can prevent a speed mismatch from occurring by ensuring that at least one end of a link is configured to autonegotiate the speed settings.

You can use the **show interfaces status** command to view the speed settings for the interfaces on a device. The following example displays sample output from the **show interfaces status** command:

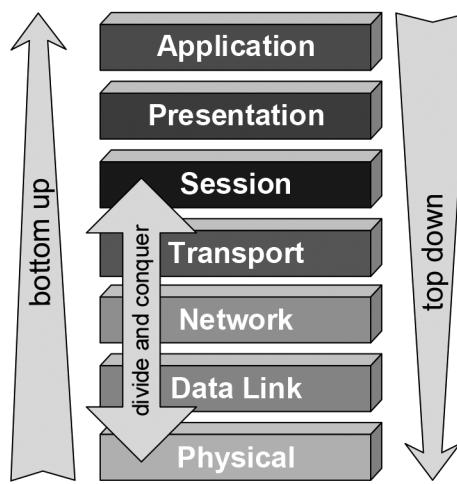
```
SwitchA#show interfaces status
Port      Name          Status       Vlan     Duplex    Speed   Type
Fa0/1                connected    1         a-full   a-100  10/100BaseTX
Fa0/2                connected    1         a-full   a-100  10/100BaseTX
Fa0/3                connected    1         a-full   a-100  10/100BaseTX
Fa0/4                connected    1         a-full   a-100  10/100BaseTX
Fa0/5                notconnect  1         auto    auto   10/100BaseTX
Fa0/6                notconnect  1         auto    auto   10/100BaseTX
Fa0/7                notconnect  1         auto    auto   10/100BaseTX
```

Fa0/8	notconnect	1	auto	auto	10/100BaseTX
Fa0/9	notconnect	1	auto	auto	10/100BaseTX
Fa0/10	notconnect	1	auto	auto	10/100BaseTX
Fa0/11	connected	1	a-full	a-100	10/100BaseTX
Fa0/12	connected	1	a-full	a-100	10/100BaseTX
Gi0/1	notconnect	1	auto	auto	10/100BaseTX
Gi0/2	notconnect	1	auto	auto	10/100BaseTX

In this sample output, the interfaces have been configured to autonegotiate the speed settings, as depicted by the `a-` prefix before the speed setting in the output. For example, interface Fa0/1 autonegociated a 100-Mbps transmission speed.

Using the OSI Model to Troubleshoot Networks

- The bottom up method starts at Layer 1 and moves up the OSI model
- The top down method starts at Layer 7 and moves down the OSI model
- The divide and conquer method starts at Layer 3 and goes up or down depending on tests



Using the OSI Model to Troubleshoot Networks

You can also use the OSI reference model as a basis for troubleshooting a network. Each of the troubleshooting techniques below uses the logical structure of the OSI model to discover the cause of network problems.

Understanding the Bottom Up Troubleshooting Technique

The bottom up method of network troubleshooting begins at the Physical layer of the OSI reference model and then works through each layer toward the Application layer until the problem is isolated. For example, an administrator who is troubleshooting a workstation that can no longer connect to the network might choose to first check the workstation's physical connection to the network, such as checking for a loose cable. If the cable is not loose, the administrator might decide to proceed to the Data Link layer of the OSI reference model and verify the network card, then the IP address at the Network Layer, and so on.

Understanding the Top Down Troubleshooting Technique

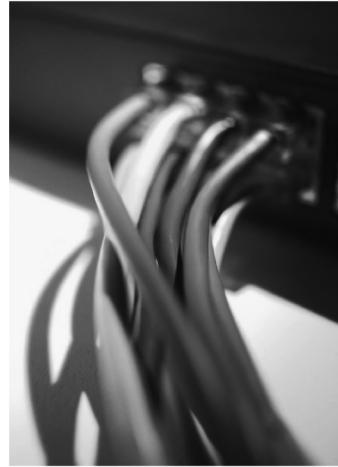
The top down troubleshooting technique starts at the Application layer and works toward the Physical layer of the OSI reference model. An administrator using the top down method of network troubleshooting might begin the process by examining or restarting the network applications on a workstation that has lost connectivity to the network.

Understanding the Divide and Conquer Troubleshooting Technique

The divide and conquer troubleshooting technique starts at the Network layer and works either up or down the OSI model depending on the outcome of network tests. For example, an administrator who is using the divide and conquer method to troubleshoot a workstation that has lost connectivity to the network might successfully test connectivity at the Network layer and, based on that result, might decide to move on to the Transport layer of the OSI model. However, an administrator who determines that connectivity does not exist at the Network layer might choose to check for a valid IP address on an interface, then check for the Data Link layer problems, and then check for a cable-connection problem at the Physical layer.

Troubleshooting Connectivity

- Verify Physical layer connectivity
- Verify Data Link layer connectivity
- Verify Network layer connectivity



Troubleshooting Connectivity

Using the bottom up method of troubleshooting is generally best for isolating interface configuration issues. Therefore, you should begin by troubleshooting Layer 1, or Physical layer, connectivity. Once you have verified physical connectivity, you can then test Layer 2, or Data Link layer, and Layer 3, or Network layer, interface configuration issues.

Troubleshooting Physical Layer Connectivity

Verifying physical connectivity to the ISP from RouterA

```
RouterA#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
    Hardware is M4T
    Internet address is 192.0.2.2/27
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation PPP, LCP Open
    Open: IPCP, CDP/CP, crc 16, loopback not set
    Keepalive set (10 sec)
    Restart-Delay is 0 secs
    Last input 00:00:10, output 00:00:02, output hang never
    Last clearing of "show interface" counters 00:00:20
<output omitted>
```

Troubleshooting Physical Layer Connectivity

Layer 1 of the OSI model is the Physical layer. Therefore, you should begin the troubleshooting process by verifying that physical connectivity exists between the router and the ISP. There are several ways to verify physical connectivity, the first of which is simply examining the cable that directly connects the router to the ISP link. Next, you should connect to the router and issue the **show interfaces** command in privileged EXEC mode. When issued without parameters, the **show interfaces** command displays information about each of the router's network interfaces. You can also display information about a specific interface by issuing the **show interfaces type number** command, where type is the name and number is the number of the interface you want to examine.

In the output above, the Serial 0/0 interface on RouterA is in the up state. In addition, the line protocol is in the up state. An interface status of up indicates that the physical interface is working properly. An interface status of down indicates the presence of a Layer 1 problem. Examples of Layer 1, or Physical layer, problems include a faulty interface, a broken cable, or an incorrect cable. You should use a crossover cable to connect the Ethernet interfaces of two similar devices, such as two computers, two switches, or two routers. You should use a straight-through cable to connect two dissimilar devices, such as a computer to a switch or a switch to a router. If the interface status is in the administratively down state, the **shutdown** command is configured on the interface.

The **show interfaces** command also provides statistics that might be helpful in diagnosing other Layer 1 problems. For example, many CRC errors on an interface could be indicative of a bad cable. A high number of input queue drops or output queue drops could indicate that the router hardware is unable to efficiently process the volume of traffic that is being sent to the router.

Although problems at the Physical layer might indicate hardware issues with network interfaces or cables, there are some Cisco configuration mistakes that can create Physical layer problems. For example, the DCE end of a serial connection provides clocking information to the DTE end. If the correct clock rate is not configured on the DTE interface, physical connectivity between the devices cannot be established. You can issue the **show controllers serial** command to determine which end of the cable is connected to the router.

Similarly, Ethernet interfaces require that the duplex configuration match on each end of the link. There are two different duplex modes: full duplex and half duplex. When full-duplex mode is configured, data is sent from one pair of wires and received by using a different pair of wires, which prevents collisions from occurring. Full duplex enables both ends of a link to transmit and receive information simultaneously. By contrast, hubs support only half-duplex operation; a device connected to a hub cannot send and receive data simultaneously.

Most modern devices automatically negotiate the duplex settings for Ethernet, FastEthernet, and GigabitEthernet interfaces. However, duplex mismatches can still occur if the **duplex {full | half | auto}** command is manually configured with different modes on each end of a link or if something interferes with the automatic negotiation process. If a high number of collisions is displayed in the output of the **show interfaces** command, a duplex mismatch might be the cause.

The speed of an interface is also automatically negotiated on modern devices. Therefore, a full-duplex GigabitEthernet interface that is connected to a full-duplex FastEthernet interface will negotiate a speed of 100 megabits per second (Mbps). However, if the **speed {10 | 100 | 1000 | auto}** command is issued on each side of the link and the speeds do not match, a link will not be established. For example, a FastEthernet interface that is manually configured to a speed of 100 Mbps will not be able to establish a link with a GigabitEthernet interface that is manually configured to a speed of 1,000 Mbps.

Cisco recommends manually configuring speed and duplex settings on links to devices that are not likely to change or be moved, such as file servers. However, for most devices, automatic negotiation of speed and duplex should be allowed to occur.

Troubleshooting Data Link Layer Connectivity

Verifying the Layer 2 configuration of the interface on RouterA

```
RouterA#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
    Hardware is M4T
    Internet address is 192.0.2.2/27
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation PPP, LCP Open
    Open: IPCP, CDP/CP, crc 16, loopback not set
    Keepalive set (10 sec)
    Restart-Delay is 0 secs
    Last input 00:00:10, output 00:00:02, output hang never
    Last clearing of "show interface" counters 00:00:20
    <output omitted>
```

Troubleshooting Data Link Layer Connectivity

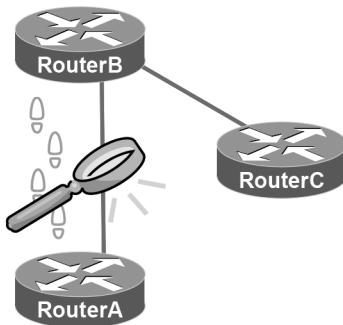
The **show interfaces** command is also useful for verifying the Data Link layer components of the interface configuration on a router or a switch. A Layer 2 protocol is required to transmit information from one interface to another across a link. Protocols that operate at the Data Link layer include Ethernet, PPP, High-level Data Link Control (HDLC), and Frame Relay. In the output above, the Serial 0/0 interface is in the up state. In addition, the line protocol, which is the Data Link layer protocol, is in the up state. An interface status of up combined with a line protocol status of up indicates that the interface and line protocol are working properly. The Layer 2 protocol must match on each end of a link for connectivity to be established.

An interface status of up combined with a line protocol status of down indicates the presence of a Data Link layer problem. Examples of Data Link layer problems include mismatched encapsulation between linked serial interfaces, clocking errors, or a lack of keepalive messages. You can verify the Layer 2 encapsulation method that is being used on the interface by examining the output of the **show interfaces** command. In the output above, the encapsulation is configured to PPP. By default, a Cisco serial interface is configured to use HDLC encapsulation.

The **show interfaces** command is also useful for verifying maximum transmission unit (MTU) configured on an interface. The MTU is the largest frame that a device can transmit. MTU typically refers to the largest frame that can be transmitted along a path. However, MTU is sometimes also used to describe the largest packet that a router can forward. The default MTU for an Ethernet frame is 1,500 bytes. Because an IP packet has a 20-byte header, the largest IP payload that can be carried in an Ethernet frame is 1,480 bytes. If a frame exceeds the MTU of a link, the frame will be fragmented if possible or discarded if the do-not-fragment, or DF, bit is set.

Troubleshooting Network Layer Connectivity

- Verify network addressing scheme, including subnet masks
- Verify that the path exists in the routing table
- Verify routing protocol configuration
- Verify default gateway configuration



Troubleshooting Network Layer Connectivity

Troubleshooting the Network layer, or Layer 3, of the OSI model is potentially the most involved task in troubleshooting router connectivity. Network layer troubleshooting requires the verification of correct IPv4 and IPv6 network addressing and therefore an understanding of IPv4 subnetting and variable-length subnet masking (VLSM) as well as IPv6 addressing. These concepts will be covered in the **Network Addressing and Transport** module. In addition, Network layer troubleshooting might involve the examination of routing tables and routing protocol configuration or default gateway configuration.

Summary

- The OSI model
 - Network devices and protocols
- Devices form topologies
- On-premises versus cloud
- Cables connect to interfaces
 - Ethernet
 - Serial
 - Fiber-optic
- Troubleshooting methodologies
- The **show interfaces** command

Summary

The fundamentals of networking begin with an understanding of the OSI model as well as the devices and protocols that operate at each layer. Devices are connected together to form network topologies, and each topology has a specific function. Each company must decide how to connect its devices as well as whether to implement solutions that are on-premises, cloud-based, or a combination of both.

Individual devices can communicate over the network by connecting Ethernet, serial, or fiber-optic cables to their corresponding interfaces. When communication fails, troubleshooting methodologies can help to isolate problems quickly. Understanding the output of the **show interfaces** command is vital in order to efficiently troubleshoot and administer Cisco devices.

Module Notes

Review Question 1

How do spines and leafs connect in a spine-leaf topology?

- A. Each leaf must connect to every spine.
- B. Each leaf must connect to at least two spines.
- C. Each spine must connect to every other spine.
- D. Each leaf must connect to every other leaf.

Review Question 1

How do spines and leafs connect in a spine-leaf topology?

- A. Each leaf must connect to every spine.
- B. Each leaf must connect to at least two spines.
- C. Each spine must connect to every other spine.
- D. Each leaf must connect to every other leaf.

In a spine-leaf topology, each leaf must connect to every spine. In addition, each spine must connect to every leaf. A spine-leaf topology is a two-tier network architecture in which every lower-tier leaf switch connects to every top-tier spine switch. However, the leafs and spines are not connected to one another.

Spine switches connect to the network backbone. If link oversubscription occurs, a new spine switch can be added and connections to every leaf switch can be established.

Leaf switches connect to nodes, such as servers. When port capacity becomes a problem with the addition of new servers, a new leaf can be added and connections to every spine switch can be established.

When traffic is sent through a spine-leaf topology, the path is randomly chosen so that the traffic is evenly distributed among the spines. Because every traffic flow must pass through no more than two network hops, throughput and latency become much more even and predictable.

Review Question 2

Which of the following cloud computing service models provides the least management control to the consumer?

- A. IaaS
- B. PaaS
- C. SaaS

Review Question 2

Which of the following cloud computing service models provides the least management control to the consumer?

- A. IaaS
- B. PaaS
- C. SaaS

Software as a Service (SaaS) is the cloud computing service model that provides the least management control to the consumer. The National Institute of Standards and Technology (NIST) defines three service models in its definition of cloud computing: SaaS, Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

The SaaS model enables a consumer to access applications that are running in the cloud infrastructure but does not enable the consumer to manage the cloud infrastructure or to configure the provided applications. Of the three models, SaaS exposes the least amount of the consumer's network to the cloud and is the least likely to require changes to the consumer's network design.

The PaaS model provides a consumer with somewhat more freedom than the SaaS model by enabling the consumer to install and possibly configure provider-supported applications in the cloud infrastructure. A company that uses a provider's development tools or Application Programming Interface (API) to deploy specific cloud-based applications or services is using PaaS.

The IaaS model provides the greatest degree of freedom by enabling a consumer to provision processing, memory, storage, and network resources within the cloud infrastructure. IaaS also enables a consumer to install operating systems (OSs) and applications. However, with IaaS, the cloud infrastructure remains under the control of the service provider. A company uses IaaS when it hires a service provider to deliver cloud-based processing and storage that will house multiple physical or virtual hosts that can be configured in a variety of ways.

Review Question 3

An interface has a status of up combined with a line protocol status of down. At which of the following layers does the problem most likely exist?

- A. at the Physical layer
- B. at the Data Link layer
- C. at the Network layer
- D. at the Transport layer

Review Question 3

An interface has a status of up combined with a line protocol status of down. At which of the following layers does the problem most likely exist?

- A. at the Physical layer
- B. at the Data Link layer
- C. at the Network layer
- D. at the Transport layer

An interface status of up combined with a line protocol status of down most likely indicates the presence of a Data Link layer problem. Examples of Data Link layer problems include mismatched encapsulation between linked serial interfaces, clocking errors, or a lack of keepalive messages. You can verify the Layer 2 encapsulation method that is being used on the interface by examining the output of the **show interfaces** command.

An interface status of down most likely indicates the presence of a Physical layer problem. Examples of Physical layer problems include a faulty interface, a broken cable, or an incorrect cable. You should use a crossover cable to connect the Ethernet interfaces of two similar devices, such as two computers, two switches, or two routers. You should use a straight-through cable to connect two dissimilar devices, such as a computer to a switch, or a switch to a router. If the interface status is in the administratively down state, the **shutdown** command will be configured on the interface.

A Network layer problem or a Transport layer problem might not affect the interface status or the line protocol status. Network layer troubleshooting requires the verification of correct Internet Protocol version 4 (IPv4) and IP version 6 (IPv6) network addressing as well as the examination of routing protocol and default gateway configurations. Transport layer troubleshooting involves the verification of access control lists (ACLs) and firewall rules to determine whether any Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports have been blocked.

Index

Symbols

- 3DES (Triple Data Encryption Standard), 513, 516, 635**
- A**
- AAA (Authentication, Authorization, and Accounting), 139, 170, 552, 620, 621, 622, 623, 624, 625, 626, 649**
 - ABR (area border router), 400, 401, 410, 411, 413, 415**
 - ACLs (access control lists), 33, 41, 88, 213, 246, 493, 495, 501, 517, 530, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 663**
 - AD (administrative distance), 271, 344, 356, 360, 361, 367, 368, 369, 413, 420, 456, 464**
 - ADD1 (Address 1), 171**
 - ADD2 (Address 2), 171**
 - ADD3 (Address 3), 171**
 - ADD4 (Address 4), 171**
 - ADSL (Asynchronous Digital Subscriber Line), 28**
 - AES (Advanced Encryption Standard), 168, 169, 180, 516, 517, 616, 617, 635, 654**
 - AES-CCMP (Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 168, 169, 180**
 - AES-GCMP (Advanced Encryption Standard-Galois/Counter Mode Protocol), 169, 180**
 - AF (assured forwarding), 531**
 - AH (Authentication Header), 634**
 - AID (association identity), 171**
 - AP (access point), 38, 154, 157, 158, 159, 165, 169, 170, 171, 173**
 - API (Application Programming Interface), 38, 49, 86, 658, 659, 663, 665, 667, 668, 672, 673, 674, 675, 676, 677, 679, 681, 682, 689, 696**
 - APIPA (Automatic Private Internet Protocol Addresses), 98, 113, 472**
 - ARP (Address Resolution Protocol), 333, 348, 349, 352, 354, 371, 424, 445, 446, 447, 448, 449, 450, 453, 600, 604**
 - ASA (Adaptive Security Appliance), 36, 630**
 - AS (autonomous system), 373, 374, 397, 400, 407, 408, 413**
 - ATM (Asynchronous Transfer Mode), 45**
 - AUI (Attachment Unit Interface), 329**
 - AUX (Auxiliary), 329, 571, 572**
- B**
- BDR (backup designated router), 395, 396, 403, 404, 405, 406, 408**
- BE (best effort), 531**
- BGP (Border Gateway Protocol), 351, 356, 358, 362, 372, 374**
- BIAs (burned-in addresses), 91**
- BID (bridge ID), 273, 274, 275, 276, 290, 320**
- BPDU (bridge protocol data unit), 273, 280, 281, 282, 284, 285, 286, 287, 289, 293, 294, 295, 296, 313, 320**
- BRI (Basic Rate Interface), 329**
- Bridge, 31**
 - broadcast domain, 31, 32, 33
- BSS (Basic Service Set), 156, 158, 173**
- BSSID (Basic Service Set Identifier), 171**

C

- CAM (Content Addressable Memory), 32, 33**
- CAR (committed access rate), 538**
- CBWFQ (class-based weighted fair queuing), 534, 535, 548**
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 168, 169, 180, 616, 617, 654**
- CCNA (Cisco Certified Network Associate), 697, 698, 699, 700, 709, 710, 711, 712, 714, 716**
- CCTV (closed-circuit television), 699**
- CDDI (Copper Distributed Data Interface), 52**
- CDP (Cisco Discovery Protocol), 27, 61, 238, 250, 252, 262, 263, 264, 265, 266, 268, 269, 270, 271, 313**
- CEF (Cisco Express Forwarding), 345, 348, 350, 352, 354**
- CF (Compact Flash), 329**
- CHAP (Challenge Handshake Authentication Protocol), 337**
- CIDR (Classless Inter-Domain Routing), 108**
- CIR (committed information rate), 538**
- Cisco Three-Tier Network Design Model, 39**
 - Access layer, 39, 41, 42
 - Core layer, 39, 40, 41, 43
 - Distribution layer, 39, 41, 42, 43
- Cisco Two-Tier Network Design Model, 43**
- Cisco Unified Wireless Networks, 38**
- CKIP (Cisco Key Integrity Protocol), 618**
- CLI (command-line interface), 134, 136, 329, 508**
- Commands**
 - aaa authentication, 622, 624, 626
 - aaa authentication login, 624, 626
 - aaa group server radius, 624
 - aaa group server tacacs+, 626
 - aaa new-model, 622
 - access-class, 595, 598
 - access-list, 493, 495, 517, 586, 588, 589, 591, 592, 593, 595, 598, 599
 - access-list permit, 493, 495
 - address ipv4, 623, 625

address prefix, 427, 479
bandwidth, 30, 50, 58, 59, 92, 98, 112, 204, 205, 289, 292, 298, 313, 339, 344, 365, 366, 386, 391, 392, 393, 394, 406, 420, 422, 524, 534, 538, 548, 590
cdp enable, 264
cdp run, 264
channel-group, 303, 304, 305, 309, 316
channel-group mode, 303
clear adjacency, 352, 354
clear cef table, 354
clear ip arp, 352, 354
clear ip cache, 354
clear ip dhcp binding, 481
clear ip route, 354
clear ipv6 dhcp binding, 481
clock rate, 57, 78, 339
clock timezone, 498
copy, 208, 244, 378, 379, 407, 505, 507, 569, 610, 635, 680, 708
 copy flash:myios.bin ftp://198.51.100.1/ios/myios.bin, 505
 copy flash:myios.bin tftp://198.51.100.1/myios.bin, 507
 copy ftp://198.51.100.1/ios/myios.bin flash:myios.bin, 505
 copy running-config startup-config, 610
 copy tftp://198.51.100.1/myios.bin flash:myios.bin, 507
crypto key generate rsa, 513
debug, 271, 343, 419, 520, 522
 debug cdp, 271
 debug cdp packets, 271
 debug ip ospf adj, 419
 debug ipv6 ospf adj, 419
 debug lldp, 271
 debug lldp packets, 271
 debug ppp negotiation, 343
default-information originate, 411
default-router, 480
description, 330, 515
distance, 59, 324, 325, 344, 360, 369, 375, 377, 378, 379, 380, 381, 382, 383, 386, 388, 391, 413, 420, 464
dns-server, 480
domain-name, 480, 483, 513
do show vlan, 249
duplex, 30, 60, 64, 66, 68, 70, 71, 72, 78, 92, 93, 205, 223, 224, 225, 226, 228, 230, 231, 284, 302, 331, 333
enable password, 573, 574
enable secret, 573, 574, 575
encapsulation, 79, 88, 196, 230, 237, 238, 239, 240, 261, 266, 311, 333, 336, 338, 340, 342, 343, 349, 608, 638, 640, 643, 644, 663
encapsulation hdlc, 338
errdisable recovery cause bpduguard, 295
errdisable recovery interval, 295, 611
glbp, 451, 452, 453, 454, 455
hostname, 135, 513, 515
interface range, 302, 303, 304, 305, 316
interface tunnel, 640, 642, 643
interface vlan, 248
ip, 135, 230, 231, 332, 339, 347, 348, 350, 351, 352, 353, 354, 355, 356, 358, 360, 361, 362, 366, 369, 371, 372, 376, 402, 403, 405, 406, 408, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 430, 439, 451, 476, 479, 480, 481, 483, 484, 491, 492, 493, 494, 495, 498, 500, 504, 505, 508, 513, 515, 521, 586, 588, 589, 591, 592, 593, 596, 597, 602, 603, 605, 623, 625, 640, 641, 642, 643, 644, 648
 ip access-group, 596, 597
 ip access-list, 586, 588, 589, 592, 593
 ip address, 231, 332, 339, 411, 476, 640, 641, 642, 643
 ip address dhcp, 476
 ip arp inspection trust, 605
 ip arp inspection vlan, 605
 ip cef, 348, 350, 352
 ip default-gateway, 230, 371
 ip default-network, 371
 ip dhcp client lease, 476
 ip dhcp excluded-address, 479
 ip dhcp pool, 479
 ip dhcp snooping, 602, 603
 ip dhcp snooping trust, 602
 ip dhcp snooping vlan, 602
 ip dns server, 484
 ip domain lookup, 483
 ip domain name, 483
 ip ftp password, 504, 505
 ip ftp username, 504, 505
 ip helper-address, 476
 ip host, 484
 ip mtu, 419
 ip name-server, 483
 ip nat inside, 491, 492, 493, 495
 ip nat outside, 491, 495
 ip nat pool, 493
 ip nhrp redirect, 648
 ip nhrp shortcut, 648
 ip ospf, 366, 402, 403, 405, 406, 408, 410, 414, 415, 416, 417, 418, 419, 420, 422
 ip ospf cost, 366, 422
 ip ospf dead-interval, 403

ip ospf hello-interval, 403
ip ospf mtu-ignore, 405, 418
ip ospf priority, 405, 406
ip route, 347, 351, 354, 355, 356, 358, 360, 361, 362, 369, 371, 372, 411, 413, 420, 421, 643
ip route-cache, 347
ip ssh version 1, 513
ip ssh version 2, 513
ipv6, 332, 333, 361, 364, 391, 402, 409, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 476, 477, 478, 479, 480, 481, 484, 517, 598, 599, 641, 642
ipv6 access-class, 598
ipv6 access-list, 598, 599
ipv6 address, 332, 411, 477, 478, 641
ipv6 address autoconfig, 477, 478
ipv6 dhcp client lease, 476
ipv6 dhcp pool, 479
ipv6 host-name, 484
ipv6 mtu, 419
ipv6 nd other-config-flag, 480
ipv6 ospf, 402, 411, 414, 415, 416, 417, 418, 419, 420, 422
ipv6 route, 361, 364, 413, 420, 421
ipv6 router ospf, 391, 409, 412
ipv6 traffic-filter, 599
ipv6 unicast-routing, 361, 409
keepalive, 64, 66, 68, 79, 88, 228, 342
key, 102, 166, 167, 168, 173, 180, 311, 498, 500, 501, 512, 513, 581, 615, 616, 618, 623, 625, 635, 637, 654, 677, 678
line vty, 509, 595
lldp enable, 265
lldp run, 265
logging console, 523
logging host, 521
login, 509, 564, 571, 572, 624, 626, 710
login local, 509, 572
mac-address-table aging-time, 211
maximum-paths, 422
name, 24, 77, 116, 127, 134, 165, 230, 248, 249, 254, 256, 257, 260, 302, 416, 417, 432, 433, 441, 470, 476, 478, 479, 480, 482, 483, 484, 486, 493, 495, 501, 503, 504, 505, 507, 510, 512, 513, 515, 516, 517, 518, 521, 522, 546, 572, 581, 583, 584, 588, 592, 594, 595, 596, 598, 599, 613, 619, 622, 623, 624, 625, 626, 652, 706, 714
neighbor, 122, 127, 148, 262, 269, 375, 378, 379, 381, 385, 387, 388, 391, 395, 403, 404, 405, 406, 407, 408, 416, 417, 418, 460, 522, 669
network, 410, 411
ntp access-group, 501
ntp authenticate, 500, 501
ntp authentication-key, 500
ntp master, 499
ntp server, 498, 499, 500, 501
ntp trusted-key, 500, 501
passive-interface, 418
password, 24, 165, 166, 253, 254, 257, 403, 419, 460, 504, 505, 509, 510, 517, 564, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 618, 619, 620, 621, 622, 623, 625, 649, 652
ping, 98, 248, 561, 643
port, 625
radius server, 623, 624
resume, 510
router-id, 402, 417
router ospf, 391, 409, 411, 412
service dhcp, 479
service password-encryption, 571, 574, 575
service timestamps log datetime msec, 520
show, 64, 66, 67, 68, 70, 72, 77, 78, 79, 81, 88, 211, 212, 227, 228, 229, 230, 234, 235, 241, 248, 249, 260, 261, 266, 267, 268, 269, 270, 271, 276, 277, 278, 289, 291, 292, 306, 307, 308, 309, 310, 311, 333, 334, 335, 338, 339, 340, 341, 342, 343, 350, 351, 352, 353, 355, 356, 358, 362, 364, 369, 372, 402, 408, 412, 413, 414, 415, 416, 417, 418, 420, 421, 432, 433, 440, 441, 454, 455, 480, 481, 492, 493, 494, 495, 501, 502, 513, 516, 521, 572, 573, 574, 594, 602, 603, 607, 613, 643, 644, 645
show access-lists, 493, 495
show adjacency, 352
show cdp, 266, 267, 268, 269, 270, 271
show cdp entry, 269
show cdp entry device-id protocol, 269
show cdp interface, 266, 267
show cdp neighbors, 268, 269
show cdp neighbors detail, 268, 269
show cdp traffic, 270, 271
show controllers, 78, 338, 339
show controllers serial, 78, 338, 339
show etherchannel, 308, 309, 310, 311
show glbp, 454, 455
show interfaces, 64, 66, 68, 70, 72, 77, 78, 79, 81, 88, 227, 228, 229, 234, 241, 248, 261, 308, 333, 334, 335, 340, 341, 342, 343, 607, 644, 645
show interfaces interface switchport, 234
show interfaces [interface] trunk, 241
show interfaces port-channel, 308
show interfaces status, 70, 72
show interfaces switchport, 241, 261
show interfaces trunk, 241, 261
show interfaces tunnel, 644
show interfaces vlan, 248
show ip arp, 352

*show ip cache, 352, 353
show ip cef, 350, 352
show ip dhcp binding, 481
show ip dhcp conflict, 480
show ip dhcp snooping, 602, 603
show ip dhcp snooping binding, 603
show ip interface brief, 358, 362, 644
show ip nat translations, 492, 494, 495
show ip ospf, 402, 408, 414, 415, 416, 417, 418, 420
show ip ospf database, 408, 414
show ip ospf interface, 416, 418, 420
show ip ospf neighbor, 417, 418
show ip protocols, 412, 418
show ip route, 351, 355, 356, 358, 362, 369, 372, 413, 420, 421, 643
show ip route ospf, 413
show ip ssh, 513
show ipv6 dhcp binding, 481
show ipv6 interface, 333, 364
show ipv6 interface brief, 364
show ipv6 ospf, 402, 414, 415, 416, 417, 418, 420
show ipv6 ospf database, 414
show ipv6 ospf interface, 416, 418, 420
show ipv6 ospf neighbor, 417, 418
show ipv6 protocols, 412, 418
show ipv6 route, 364, 413, 420, 421
show ipv6 route static, 364
show lldp entry, 269
show lldp interface, 267
show lldp neighbors, 268, 269
show lldp neighbors detail, 268, 269
show lldp traffic, 270, 271
show logging, 521
show mac-address-table, 211, 212, 261
show mac-address-table address, 212
show mac-address-table aging-time, 211
show mac-address-table interface, 212
show mac-address-table vlan, 212
show ntp associations, 502
show ntp authentication keys, 501
show ntp authentication-status, 501
show ntp status, 502
show ntp trusted-keys, 501
show port-security interface, 613
show running-config, 227, 230, 289, 291, 292, 310, 343, 412, 418, 572, 573, 574
show snmp community, 516
show snmp contact, 516
show snmp host, 516
show snmp location, 516
show spanning-tree, 276, 277, 278, 289, 291, 292, 306, 307
show spanning-tree interface, 278
show spanning-tree mst, 292
show spanning-tree root, 277
show spanning-tree vlan, 277, 306, 307
show standby, 432, 433
show time-range, 594
show vlan, 235, 249, 261
show vlan brief, 235, 249
show vlan id, 249
show vlan name, 249
show vrrp, 440, 441
show vtp status, 260
shutdown, 77, 88, 303, 308, 332, 335, 339, 342, 607, 611
snmp-server community, 515
snmp-server contact, 515
snmp-server enable traps, 518, 519
snmp-server engineID, 516
snmp-server group, 517
snmp-server host, 515, 516, 518
snmp-server location, 515
snmp-server user, 517
snmp-server view, 517
spanning-tree, 275, 276, 277, 278, 282, 284, 285, 289, 291, 292, 294, 295, 296, 297, 306, 307
spanning-tree bpdu guard enable, 295
spanning-tree guard loop, 296
spanning-tree guard root, 297
spanning-tree link-type point-to-point, 284
spanning-tree loopguard default, 296
spanning-tree mode mst, 292
spanning-tree mode pvst, 289
spanning-tree mode rapid-pvst, 285, 291
spanning-tree portfast, 294, 295
spanning-tree portfast bpdu guard default, 295
spanning-tree vlan forward-time, 282
spanning-tree vlan hello-time, 282
spanning-tree vlan max-age, 282
spanning-tree vlan root primary, 275
spanning-tree vlan root secondary, 275
speed, 33, 58, 64, 66, 68, 71, 72, 73, 78, 194, 200, 223, 224, 226, 228, 230, 279, 302, 331, 338, 339, 429, 528, 628
ssh, 510, 512, 513
standby, 424, 426, 428, 430, 431, 432, 433, 435, 442
switchport, 230, 233, 234, 239, 241, 242, 243, 252, 259, 261, 302, 318, 602, 608, 609, 610, 611, 612
switchport access vlan, 230, 233
switchport access vlan dynamic, 233
switchport mode, 230, 233, 239, 242, 252, 302, 318, 608
switchport mode access, 233, 242, 252, 608
switchport mode trunk, 230, 239, 242, 608
switchport nonegotiate, 243, 608*

- switchport port-security*, 609, 610, 611, 612
- switchport port-security mac-address*, 609, 610
- switchport port-security violation*, 609, 611
- switchport trunk allowed vlan*, 259
- switchport trunk encapsulation*, 230, 239, 608
- switchport trunk native vlan*, 239, 261
- switchport voice vlan*, 252
- switchport voice vlan dot1p*, 252
- switchport voice vlan none*, 252
- switchport voice vlan untagged*, 252
- tacacs server, 625, 626
- telnet, 508, 510, 595, 598
- time-range, 594
- transport input, 510, 512, 595
- trust device cisco-phone, 250
- tunnel destination, 627, 642, 643, 645
- tunnel mode gre ip, 640, 641, 642, 643
- tunnel mode gre ipv6, 641
- tunnel source, 627, 642, 643, 645
- username, 504, 505, 509, 572, 574, 622
- username password, 509
- vlan, 211, 212, 230, 233, 235, 239, 248, 249, 252, 258, 259, 261, 275, 277, 282, 306, 307, 602, 605
- vrpp, 439, 440, 441
- vtp, 254, 255, 256, 259, 260
 - vtp domain*, 254
 - vtp mode*, 256
 - vtp password*, 254
 - vtp pruning*, 259
 - vtp version*, 255
- Controllers**, 38
 - Cisco DNA Controller, 38
 - Software-Defined Networking, 38
 - wireless LAN controllers, 38
- CQ (custom queuing)**, 534, 535, 548
- CRC (cyclic redundancy check)**, 64, 65, 67, 69, 77, 93, 172, 216, 228, 229, 237, 334, 341
- CRM (customer relationship management)**, 49
- CRUD (create, read, update, delete)**, 674, 675, 696
- CS (class selector)**, 531
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**, 30, 92, 93
- CSR 1000V (Cisco Cloud Services Router 1000V)**, 191
- CST (Common Spanning Tree)**, 290
- CSU/DSU (channel service unit/data service unit)**, 341
- D**
 - DAI (Dynamic ARP Inspection)**, 600, 604, 605, 649
 - DBD (Database Descriptor)**, 408, 418
 - DCE (data communications equipment)**, 57, 78, 338, 339
- DES (Data Encryption Standard)**, 513, 516, 635
- DHCP (Dynamic Host Configuration Protocol)**, 22, 34, 50, 113, 114, 127, 138, 150, 468, 470, 471, 472, 473, 474, 475, 476, 479, 480, 481, 539, 544, 600, 601, 602, 603, 604, 649
- DHCP process**, 471
 - DHCP Acknowledgment, 471, 475
 - DHCP Discover, 471, 472
 - DHCP Offer, 471, 473
 - DHCP Request, 471, 474
- DHCPv6 (Dynamic Host Configuration Protocol version 6)**, 114
- DH (Diffie-Hellman)**, 635
- Dijkstra algorithm**, 392, 394
- Distance-vector protocols**, 324
- DMVPN (Dynamic Multipoint virtual private network)**, 630, 646, 647, 648
- DNA (Digital Network Architecture)**, 659, 683, 689
- DNS (Domain Name System)**, 22, 50, 127, 468, 473, 478, 480, 482, 483, 484, 486, 508, 539, 546
- DoD (Department of Defense)**, 578
- DR (designated router)**, 395, 396, 403, 404, 405, 406, 407, 408
- DSCP (Differentiated Services Code Point)**, 530, 531, 532
- DSL (Digital Subscriber Line)**, 46, 630
- DSP (digital signal processor)**, 519
- DTE (data terminal equipment)**, 57, 78, 338
- DTP (Dynamic Trunking Protocol)**, 242, 243, 261, 318, 608
- Duplex mode**, 324
 - Full-duplex, 70, 71, 78, 93, 205, 224, 225, 284
 - Half-duplex mode, 30, 66, 70, 93, 224, 225, 284
- DUR (Duration)**, 171
- E**
 - EAP (Extensible Authentication Protocol)**, 167, 168, 169, 170, 618, 621
 - EF (expedited forwarding)**, 531
 - EGPs (exterior gateway protocols)**, 351, 356, 358, 362, 372, 374
 - EIDs (endpoint identifiers)**, 671
 - EIGRP (Enhanced Interior Gateway Routing Protocol)**, 26, 121, 247, 351, 352, 355, 356, 358, 362, 365, 366, 367, 372, 374, 375, 387, 390, 393, 423, 456, 464, 639, 669
 - EMI (electromagnetic interference)**, 58
 - Endpoints**, 31, 32, 35
 - ESP (Encapsulating Security Payload)**, 634
 - ESS (Extended Service Set)**, 156, 159, 173
 - Ethernet**, 27, 28, 30, 32, 45, 51, 52, 53, 54, 56, 57, 60, 68, 77, 78, 79, 81, 88

ETSI (European Telecommunications Standards Institute), 191

F

FAQ (Frequently Asked Questions), 703
FC (Frame Control), 171
FCS (Frame Check Sequence), 70, 93, 172, 207
FDDI (Fiber Distributed Data Interface), 58, 248
FHRP (First-Hop Redundancy Protocol), 324, 423, 457, 462
Fiber-optic cables, 28, 57, 58, 59, 60, 81
 LC connectors, 60
 MT-RJ connectors, 60
 SC connectors, 60
 ST connectors, 60
FIB (Forwarding Information Base), 348, 350, 352, 354
FIFO (first-in-first-out), 527, 528, 534, 535
Firewall, 36, 88
Frame Relay, 27, 45, 79
FTP (File Transfer Protocol), 22, 141, 150, 468, 469, 503, 504, 505, 506, 507, 539, 592, 664, 666

G

GCMP (Galois/Counter Mode Protocol), 169, 180, 617, 654
GIF (Graphics Interchange Format), 23
GLBP (Gateway Load Balancing Protocol), 324, 325, 423, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 457, 462
GMAC (Galois Message Authentication Code), 617, 654
GPS (global positioning system), 497, 502, 583
GRE (Generic Routing Encapsulation), 627, 630, 638, 639, 640, 641, 643, 644, 645, 646, 647
GUI (graphical user interface), 38, 134, 135, 136, 618, 619, 683, 689

H

HDLC (High-level Data Link Control), 79, 336, 338, 340, 342, 343, 396
HIPS (Host-based IPS), 565
HMAC (Hash-based Message Authentication Code), 516, 636
HMAC-SHA (Hash-based Message Authentication Code-SHA), 516
HSRP (Hot Standby Router Protocol), 324, 325, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 438, 439, 442, 443, 445, 451, 452, 453, 457, 462
HSRPv1 (HSRP version 1), 425, 426, 427, 428, 430

HSRPv2 (HSRP version 2), 425, 426, 427, 428, 429, 430
HTDB (host tracking database), 671
HTML (Hypertext Markup Language), 676
HTTP (Hypertext Transfer Protocol), 22, 141, 150, 508, 592, 673, 675, 681, 689, 696
Hub, 30, 31, 66, 78
 collision domain, 30, 31, 32
 Collision domains, 30

I

IaaS (Infrastructure as a Service), 47, 50, 86
IANA (Internet Assigned Numbers Authority), 96, 146
IBSS (Independent Basic Service Set), 156, 157, 173
ICMP (Internet Control Message Protocol), 33, 370, 520, 561, 591
ICMPv6 (Internet Control Message Protocol version 6), 114
ICV (Integrity Check Value), 166
IEEE (Institute of Electrical and Electronics Engineers), 37, 61, 91, 92, 94, 95, 144, 154, 156, 157, 158, 159, 163, 167, 168, 170, 171, 173, 178, 224, 237, 240, 250, 263, 283, 288, 292, 299, 462, 530
 802.1Q, 237, 239, 240, 250, 252, 253, 289, 313, 530
 802.1s, 288, 292
 802.3, 92, 93
 802.3ad, 299
 802.3u, 224
 802.3z, 224
 802.11, 154, 157, 158, 159, 163, 164, 166, 171, 172, 173
IETF (Internet Engineering Task Force), 123, 423, 435, 457, 462, 621, 680
IGP (Interior Gateway Protocol), 324, 374, 375, 376, 390, 456
IHL (IP Header Length), 97, 115
IO (system input/output), 526, 527
IP addresses, *See also IPv4 (Internet Protocol version 4); See also IPv6 (Internet Protocol version 6)*
IP (Internet Protocol), 22, 26, 30, 33, 34, 61, 74, 75, 79, 88, 96, 97, 98, 100, 101, 106, 107, 108, 109, 110, 112, 113, 114, 115, 116, 129, 134, 135, 136, 137, 138, 146, 193, 194, 200, 207, 220, 221, 228, 232, 247, 248, 250, 251, 252, 260, 263, 313, 323, 326, 328, 331, 332, 339, 346, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 360, 362, 370, 371, 399, 402, 403, 405, 406, 410, 411, 416, 417, 419, 423, 424, 430, 432, 433, 435, 436, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 450, 451, 454, 455, 456, 467, 470, 472, 473, 474, 475, 476, 479, 480, 481, 482, 483, 485, 486, 488, 489, 490, 492, 493, 494, 495, 496, 497, 498, 500, 502,

- 508, 510, 512, 515, 516, 521, 530, 531, 532, 534, 535, 537, 539, 542, 546, 548, 561, 586, 587, 588, 590, 591, 592, 595, 596, 597, 598, 601, 603, 604, 623, 625, 628, 633, 634, 638, 640, 642, 644, 646, 647, 648, 663, 666, 669**
- IPP (Internet Protocol Precedence), 530, 531**
- IPSec (Internet Protocol Security), 114, 194, 200, 512, 614, 619, 627, 628, 630, 632, 633, 634, 635, 636, 637, 638, 639, 646, 648**
- IPS (Intrusion Prevention System), 29, 36, 41, 562, 565**
- IPv4 (Internet Protocol version 4), 26, 80, 88, 96, 97, 113, 114, 115, 116, 120, 121, 122, 123, 124, 126, 128, 129, 130, 131, 132, 133, 142, 146, 148, 324, 351, 364, 390, 411, 413, 425, 428, 435, 470, 472, 476, 479, 480, 483, 484, 485, 530, 539, 595, 596, 598, 599, 623, 625, 640, 642**
- IPv6 (Internet Protocol version 6), 26, 80, 88, 96, 97, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 126, 127, 128, 129, 130, 131, 132, 133, 142, 148, 324, 332, 333, 361, 364, 390, 403, 409, 411, 412, 413, 419, 425, 470, 477, 478, 479, 480, 481, 483, 484, 485, 530, 598, 599, 641, 642**
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 131**
- ISDN (Integrated Services Digital Network), 54, 329, 632**
- IS-IS (Intermediate System-to-Intermediate System), 669**
- ISL (Inter-Switch Link), 237, 239, 240, 253, 289**
- ISP (Internet service provider), 77, 96, 124, 125, 146, 359, 373, 400, 628**
- IV (initialization vector), 166, 167, 180, 615, 654**
- J**
- JPEG (Joint Photographic Experts Group), 23**
- JSON (JavaScript Object Notation), 659, 673, 677, 678, 680, 681, 689**
- K**
- KPI (Key Performance Indicator), 683**
- L**
- LACP (Link Aggregation Control Protocol), 299, 300, 301, 305, 309, 310, 311, 316**
- LAMP (Linux Apache MySQL PHP), 50**
- LANs (local area networks), 37, 38, 42, 45, 46, 51, 58, 92, 93, 155, 188, 200, 244, 245, 247, 250, 311, 327, 330, 331, 337, 338, 462, 476, 596, 605, 606, 614, 619, 660, 668, 670, 671, 692**
- LAP (lightweight access point), 38**
- LCP (Link Control Protocol), 337**
- LFI (Link Fragmentation and Interleaving), 535**
- LLDP (Link-Layer Discovery Protocol), 262, 263, 265, 266, 267, 268, 269, 270, 271, 313**
- LLQ (low latency queuing), 534, 535, 548**
- LSAck (Link State Acknowledgment), 408**
- LSAs (link-state advertisements), 388, 389, 391, 397, 399, 406, 407, 408, 414**
- LSDB (link-state database), 388, 400, 401, 406, 407, 408**
- LSR (Link State Request), 408**
- LSU (Link State Update), 408**
- LWAPP (Lightweight Access Point Protocol), 38, 155**
- M**
- MAC (Media Access Control), 27, 30, 31, 32, 91, 92, 93, 94, 95, 126, 142, 144, 154, 171, 206, 207, 208, 209, 210, 212, 220, 221, 233, 251, 261, 267, 274, 275, 281, 284, 290, 313, 320, 326, 333, 340, 352, 353, 424, 427, 432, 440, 443, 444, 445, 446, 447, 448, 449, 450, 452, 453, 454, 530, 598, 601, 603, 604, 609, 610, 611, 612, 613, 663**
- MD5 (Message Digest 5), 260, 500, 514, 516, 572, 573, 574, 636, 637**
- mGRE (multipoint Generic Routing Encapsulation, 646, 647**
- MIB (management information base), 514, 515, 518, 680**
- MICs (message integrity checks), 615, 617, 654**
- MIMO (Multiple Input, Multiple Output), 163**
- MMF (multimode fiber), 59**
- MPEG (Motion Picture Experts Group), 23**
- MPLS (Multiprotocol Label Switching), 45, 628**
- MST (Multiple Spanning Tree), 288**
- MTU (maximum transmission unit), 64, 66, 68, 79, 228, 308, 333, 340, 405, 408, 418, 419, 643, 644**
- MU-MIMO (multi-user Multiple Input, Multiple Output), 163**
- mVPN (Multicast Virtual Private Networking), 670**
- N**
- NAC (Network Admission Control), 42**
- NAT (Network Address Translation), 98, 107, 114, 128, 130, 132, 146, 346, 468, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 539, 542, 663**
- NAT-PT (Network Address Translation-Protocol Translation), 128**
- NBAR2 (Next Generation NBAR), 531**
- NBAR (Network-Based Application Recognition), 531**
- NBIs (northbound interfaces), 672**

NBMA (nonbroadcast multiaccess), 395, 396, 403, 405
NCP (Network Control Protocol), 337
NF (network function), 191
NFV (Network Function Virtualization), 188, 191
NGFWv (Cisco NextGen Firewall Virtual Appliance), 191
NHRP (Next-Hop Resolution Protocol), 630, 646, 647, 648
NIC (network interface card), 28, 66, 92, 226
NIST (National Institute of Standards and Technology), 47, 86
NMS (network management system), 183, 518
NMs (network modules), 328, 329
NTP (Network Time Protocol), 139
NVGRE (Network Virtualization using Generic Routing Encapsulation), 670
NVRAM (non-volatile random-access memory), 209, 256, 258

O

OIDs (object IDs), 514
OSGi (Open Services Gateway initiative), 672
OSI Model, 21, 22, 23, 24, 25, 26, 27, 28, 38, 74, 75, 77, 80, 81
Access layer, 39, 207, 423, 457
Application layer, 21, 22, 23, 74, 137, 138, 141, 470
Data Link layer, 21, 26, 27, 28, 74, 75, 76, 79, 88, 207, 263, 328, 336
Layer 1, 21, 27, 28, 76, 77, 335, 342, 418
Layer 2, 21, 27, 32, 33, 38, 42, 76, 79, 88, 90, 91, 96, 142, 155, 189, 192, 200, 207, 208, 209, 210, 220, 221, 253, 263, 272, 326, 335, 342, 348, 349, 350, 418, 442, 529, 530, 532, 533, 552, 596, 600, 614, 615, 618, 619, 628, 649, 654, 663, 692
Layer 3, 21, 26, 32, 33, 38, 42, 76, 80, 90, 96, 133, 134, 135, 136, 142, 155, 193, 200, 220, 221, 222, 246, 247, 250, 263, 268, 324, 326, 331, 338, 345, 346, 349, 350, 423, 424, 425, 430, 456, 457, 529, 531, 532, 533, 596, 599, 614, 619, 628, 638, 640, 662, 663, 671, 692
Layer 4, 21, 25, 90, 137, 142, 326, 490, 530, 531
Layer 5, 21, 24
Layer 6, 21, 23
Layer 7, 21, 22, 530, 531
Network layer, 21, 25, 26, 27, 75, 76, 80, 88, 97, 216, 329, 634
Physical layer, 21, 27, 28, 74, 75, 76, 77, 78, 88, 207
Presentation layer, 21, 22, 23, 24
Session layer, 21, 23, 24, 25
Transport layer, 21, 24, 25, 26, 75, 88, 114, 137, 138, 140, 150

OSI (Open Systems Interconnection), 20, 21, 22, 23, 24, 25, 26, 27, 28, 38, 42, 74, 75, 77, 80, 81, 90, 97, 142, 155, 207, 326, 336, 529, 530, 600, 628, 634, 640, 649

OSI model, 97, 142
Application layer, 137, 138, 141
Network layer, 97
Transport layer, 114, 137, 138, 140, 150

OS (operating system), 50, 86, 136, 137, 184, 185, 186, 187, 196, 198, 202, 482

OSPF (Open Shortest Path First), 26, 247, 324, 325, 351, 356, 358, 362, 365, 366, 367, 368, 369, 372, 374, 375, 387, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 420, 421, 422, 456, 460, 464, 662, 669

OSPFv2 (OSPF version 2), 324, 390, 391, 394, 409, 410, 411, 412, 413, 418, 422

OSPFv3 (OSPF version 3), 324, 390, 391, 402, 403, 409, 411, 412, 413, 414, 416, 417, 418, 419, 422

OTV (Overlay Transport Virtualization), 670

OUI (Organizationally Unique Identifier), 94, 95, 126, 144

OVS (Open vSwitch), 189

P

PaaS (Platform as a Service), 47, 49, 86

PAgP (Port Aggregation Protocol), 299, 300, 304, 309, 316

PAP (Password Authentication Protocol), 24, 337

PAT (Port Address Translation), 114

PC (personal computer), 35

PCP (priority code point), 530

PDA (personal digital assistant), 35

PDLMs (Protocol Description Language Modules), 531

PDU (protocol data unit), 21

PHB (Per-Hop Behavior), 531

PHI (protected health information), 582

PIN (personal identification number), 582, 585

PKI (Public Key Infrastructure), 580, 581

PMF (Protected Management Frames), 169

pNIC (physical NIC), 190

PoE (Power over Ethernet), 51, 61, 62, 263, 313

POP3 (Post Office Protocol 3), 22, 141

PPP (Point-to-Point Protocol), 27, 79, 336, 337, 338, 342, 343, 396, 630

PQ (priority queuing), 534, 535, 548

PSK (Pre-Shared Key), 618, 636, 637

PS (Power Save), 171

PVRST+ (Per-VLAN Rapid Spanning Tree Plus), 288, 291, 292

PVST+ (Per-VLAN Spanning Tree Plus), 288, 289, 290, 291, 292
PVST (Per-VLAN Spanning Tree), 288, 289, 290, 291, 292
PyDSL (Python Domain Specific Language), 688

Q

QoS (Quality of Service), 33, 38, 213, 246, 250, 252, 468, 469, 524, 528, 529, 530, 531, 532, 538, 539, 683
QuickTime, 23

R

RADIUS (Remote Authentication Dial-In User Service), 139, 170, 572, 620, 621, 622, 623, 624, 625, 649
RED (random early detection), 537
REST (Representational State Transfer), 659, 672, 673, 674, 675, 676, 677, 681, 689, 696
RFC (Request for Comments), 98, 107, 122, 146, 434, 437, 472, 486, 680, 681
RFI (radio frequency interference), 58
RF (radio frequency), 37, 155, 173
RIB (Routing Information Base), 220
RIP (Routing Information Protocol), 121, 351, 355, 356, 358, 362, 367, 368, 369, 372, 375, 383, 391, 394, 464
RIPv2 (Routing Information Protocol version 2), 324, 365, 366, 374, 378, 379
Routers, 33, 51, 56, 77, 78, 79, 80, 88, 98, 109, 112, 120, 121, 122, 127, 129, 130, 131, 148, 192, 193, 200, 222, 236, 244, 246, 247, 264, 324, 325, 326, 327, 328, 329, 330, 331, 333, 334, 338, 340, 341, 343, 344, 346, 347, 349, 351, 355, 356, 358, 359, 360, 361, 362, 365, 366, 367, 369, 370, 371, 374, 375, 376, 377, 378, 379, 381, 383, 385, 386, 387, 388, 389, 391, 393, 395, 396, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 424, 425, 428, 429, 431, 432, 433, 434, 435, 436, 438, 439, 440, 441, 442, 443, 444, 445, 448, 449, 450, 451, 452, 453, 454, 455, 456, 460, 476, 477, 479, 480, 483, 484, 486, 488, 489, 492, 493, 494, 495, 496, 498, 500, 501, 504, 515, 524, 525, 526, 527, 528, 530, 532, 587, 588, 589, 590, 591, 593, 594, 596, 597, 622, 633, 640, 642, 643, 644, 647, 648, 660, 692
RPC (Remote Procedure Call), 24, 680
RSTP (Rapid Spanning Tree Protocol), 206, 277, 283, 284, 285, 286, 287, 288, 291, 292, 313
Rx-Ring (receive ring), 526, 527

S

SaaS (Software as a Service), 47, 48, 49, 86

SAE (Simultaneous Authentication of Equals), 169
SBIs (southbound interfaces), 679
SCP (Secure Copy), 503
SDA (Software-Defined Access), 38, 659, 668, 669, 670, 671, 672, 679, 683, 689
SDN (Software-Defined Networking), 38, 659, 667, 668, 669, 670, 671, 672, 679, 682, 683, 689
SEQ (Sequence), 171
SFTP (Secure File Transfer Protocol), 503
SHA (Secure Hash Algorithm), 514, 516, 517, 636, 637
SMF (single-mode fiber), 59
SMTP (Simple Mail Transfer Protocol), 22, 141, 150, 508
SNMP (Simple Network Management Protocol), 138, 150, 260, 468, 469, 514, 515, 516, 517, 518, 519, 539, 611, 664, 666, 680, 681, 684, 689, 694
SNMPv1 (Simple Network Management Protocol version 1), 514, 516
SNMPv2c (Simple Network Management Protocol version 2c), 514, 516, 518
SNMPv3 (Simple Network Management Protocol version 3), 222, 514, 516, 517, 518
SOF (start-of-frame), 93
SOHO (small office/home office), 46, 51
SPAN (Switched Port Analyzer), 606
SPF (shortest path first), 389, 392, 394, 415
Spine-Leaf Topology, 44, 84
 Leaf Node, 44
 Spine Node, 44
SSH (Secure Shell), 22, 222, 248, 329, 468, 469, 503, 510, 511, 512, 513, 539, 570, 581, 664, 666, 680, 687, 688, 694
SSH v1 (Secure Shell version 1), 513
SSH v2 (Secure Shell version 2), 513
SSID (Service Set Identifier), 165, 166, 173
SSL (Secure Sockets Layer), 194, 200, 627, 628, 629, 632, 633, 639, 682
SSO (single sign-on), 570
STA (Spanning Tree Algorithm), 272, 279
STP (Spanning Tree Protocol), 204, 206, 222, 272, 273, 276, 277, 278, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 306, 307, 311, 312, 313, 320
Switches, 27, 29, 32, 33, 42, 44, 45, 56, 58, 61, 62, 66, 77, 79, 84, 88, 93, 170, 189, 192, 200, 204, 205, 206, 207, 208, 209, 210, 211, 214, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 233, 236, 237, 238, 239, 240, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 260, 261, 263, 264, 272, 273, 274, 275, 276, 277, 279, 280, 282, 284, 285, 287, 289, 291, 292, 293, 294, 295, 296, 297, 298, 299, 303, 311, 312, 313, 318, 320, 326, 327, 330, 331, 349, 423, 498, 524, 525, 526, 527, 528,

530, 532, 594, 595, 601, 602, 604, 605, 606, 607, 608, 609, 610, 611, 613, 660, 692
Broadcast storms, 63
Collisions, 30, 32, 63, 64, 65, 66, 67, 68, 69, 70, 78, 92, 93, 204, 205, 229, 334, 341
Duplex mismatch, 63, 66, 68, 70, 78
Excessive noise, 63, 64
Late collisions, 63, 65, 67, 68, 69, 229, 335
Microsegmentation, 32
Speed mismatch, 63, 72
Switching modes, 204, 215
Adaptive cut-through switching, 215
Cut-through switching, 215
FragmentFree switching, 215, 219
Store-and-forward switching, 215

T

TACACS+ (Terminal Access Controller Access-Control System Plus), 620, 621, 622, 625, 626, 649
TCAM (Ternary Content Addressable Memory), 33
TCP/IP (Transmission Control Protocol/Internet Protocol), 98, 207
TCP (Transmission Control Protocol), 25, 88, 90, 98, 140, 141, 142, 150, 207, 326, 482, 496, 503, 508, 531, 536, 537, 538, 546, 562, 591, 593, 596, 621, 625, 685, 686, 687, 694
Telnet, 22, 141, 248, 329, 468, 469, 508, 509, 510, 511, 512, 520, 539, 570, 574, 595, 598, 664, 666
TFTP (Trivial File Transfer Protocol), 22, 139, 150, 468, 469, 480, 506, 507, 539, 571, 664, 666
TIA (Telecommunications Industry Association), 54, 57
TID (Traffic Identifier), 530
TKIP (Temporal Key Integrity Protocol), 167, 180, 615, 654
TLS (Transport Layer Security), 680, 682
Troubleshooting Networks
Bottom up method, 74, 76
Divide and conquer, 75
Top down method, 74
TTL (Time To Live), 97, 115, 221
Tx-Ring (transmit ring), 526, 527, 528, 533, 535

U

UDP (User Datagram Protocol), 25, 88, 90, 138, 139, 140, 142, 150, 326, 476, 482, 506, 516, 518, 531, 546, 562, 621, 623
UPS (uninterruptible power supply), 555
URL (uniform resource locator), 505, 507
USB (universal serial bus), 28
U.S. (United States), 578
UTC (Coordinated Universal Time), 498, 502, 520

UTP (unshielded twisted-pair), 52, 53, 56, 58

V

VLAN (virtual local area network), 32, 188, 192, 193, 200, 204, 209, 210, 211, 212, 230, 232, 233, 235, 236, 237, 238, 239, 241, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 256, 257, 258, 259, 260, 261, 268, 275, 277, 278, 288, 289, 290, 291, 292, 298, 302, 311, 313, 327, 423, 451, 476, 530, 596, 601, 602, 603, 605, 606
VLSMs (variable-length subnet masks), 80, 108, 109, 247, 376, 393
VMM (virtual machine manager), 185
VMPS (VLAN Management Policy Server), 233
VM (virtual machine), 184, 186, 187, 188, 189, 190, 191, 195, 196, 200, 202
vNIC (virtual network interface card), 190
VoIP (Voice over IP), 61, 263, 480
VPN (virtual private network), 36, 45, 188, 194, 200, 552, 619, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 646, 649
VRF (Virtual Routing and Forwarding), 188, 193, 200, 670
VRRP (Virtual Router Redundancy Protocol), 324, 325, 423, 434, 435, 436, 437, 438, 439, 440, 441, 442, 457, 462
vSwitches (virtual switches), 188, 189, 190, 196, 200
VTP (VLAN Trunking Protocol), 222, 253, 254, 255, 256, 257, 258, 259, 260, 268, 313
VTY (virtual terminal), 329, 509, 510, 512, 570, 571, 574, 575, 595, 598, 622, 624, 626
VXLAN (Virtual Extensible LAN), 670, 671

W

WAN (wide area network), 45, 191, 194, 200, 328, 329, 330, 336, 337, 338, 462, 628, 629, 630
WAP (wireless access point), 29, 37, 61, 616, 654
WEP (Wired Equivalent Privacy), 166, 167, 168, 180, 615, 616, 618, 654
WFQ (weighted fair queuing), 534, 535, 548
WICs (WAN interface cards), 328, 329
WinRM (Windows Remote Management), 688
WLAN (wireless local area network), 37, 38, 46, 61, 154, 155, 156, 157, 158, 159, 160, 163, 173, 552, 614, 618, 619
WLCs (wireless LAN controllers), 38, 155, 614, 618, 619, 671
WPA2 (Wi-Fi Protected Access 2), 168, 169, 180, 616, 617, 618, 654
WPA3 (Wi-Fi Protected Access 3), 169, 180
WPA (Wi-Fi Protected Access), 165, 167, 168, 169, 180, 614, 615, 616, 618, 654

WRED (weighted random early detection), 537

X

**XML (Extensible Markup Language), 659, 673, 676,
677, 680, 681, 689**

Y

**YAML (YAML Ain't Markup Language), 687, 688,
694**

YANG (Yet Another Next Generation), 679, 680, 681

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





B o s o n . c o m

8 7 7 . 3 3 3 . 3 9 2 6

support@boson.com

© Copyright 2020 Boson Software, LLC. All rights reserved.