TestOut®

TestOut Routing and Switching Pro - English 7.0.x

LESSON PLAN

Modified: 2020-06-15

Powered by LABSIM

Table of Contents

1.1: Introduction

Summary

This course is designed to prepare you to pass the TestOut Routing and Switching Pro and the Cisco CCNA 200-301 certifications. This course is designed for anyone interested in managing and deploying Cisco products in a business environment. This section introduction covers the following topics:

- Course purpose
- Course prerequisites
- Certifications

Course Purpose

The purpose of this course is to prepare you for an associate-level job role in the IT industry. This course covers the knowledge and skills related to:

- Switch setup and configuration
- Switch interface configuration
- VLAN configuration
- TCP/IP configuration
- Spanning tree configuration
- InterVLAN routing
- EtherChannel configuration
- Routers and IP routing implementation with OSPF and EIGRP routing configuration
- Access control lists
- DHCP
- DNS
- NAT
- Security and malware fundamentals
- Automation and programmability

Course Prerequisites

There are no formal prerequisites for CCNA certification, but CCNA candidates often have:

- At least a year of experience implementing and administering Cisco solutions
- A basic understanding of IP addressing and network fundamentals

Certifications

This course meets the specifications for two industry certification programs:

- TestOut Routing and Switching Pro
- Cisco CCNA 200-301

Video/Demo	Time
1.1.1 Routing and Switching Pro Overview	3:55
1.1.2 Use the Simulator	14:51
1.1.3 Explore the New Lab Features	10:19
Total Video Time	**29:05**

Fact Sheets

1.1.4 Cisco Device Icons

Total Time

About 35 minutes

2.1: TCP/IP Networking Model

Lecture Focus Questions:

- What is the purpose of a network model?
- How does the TCP protocol differ from the UDP protocol?
- What functions are performed by Application layer protocols?
- How does TCP negotiate a connection with a remote host?
- What role does port assignments play in application-to-application communications?
- What functions are provided by the Internet layer?
- What are MAC addresses? How are they used by the Link layer?

Key terms for this section include the following:

Term	Definition
TCP/IP model	The TCP/IP model consists of four separate layers, each defining certain protocols and actions that allow successful communications between two systems over a network
Media Access Control (MAC) address	A MAC address is a unique, physical address on the network port in your workstation.
File Transfer Protocol (FTP)	FTP is an Application layer protocol.
Simple Mail Transport protocol (SMTP)	SMTP is an Application layer protocol.
Transmission Control Protocol (TCP)	TCP is a Transport layer protocol.
User Datagram Protocol (UDP)	UDP is a Transport layer protocol.
Internet Work Protocol (IP)	IP is an Internet layer protocol.
Broadcast domain	A broadcast domain is a smaller region of a larger network.
Virtual LAN	A virtual LAN is a smaller region of a larger network.
Data Link	Data Link is a sublayer of the Link layer.
Physical	Physical is a sublayer of the Link layer.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.5 Compare TCP to UDP 4.8 Configure network devices for remote access using SSH

	4.9 Describe the capabilities and function of TFTP/FTP in the network

Video/Demo	Time
2.1.1 Network Models Overview	3:30
2.1.2 TCP/IP Model	6:03
2.1.4 Application Layer	2:37
2.1.5 Transport Layer	4:51
2.1.6 Internet Layer	4:41
2.1.7 Link Layer	1:59
Total Video Time	**23:41**

Fact Sheets

- 2.1.3 TCP/IP Model Overview Facts
- 2.1.8 TCP/IP Model Facts
- 2.1.9 TCP and UDP Port Numbers

Number of Exam Questions

10 questions

Total Time

About 49 minutes

2.2: OSI Networking Model

Lecture Focus Questions:

- How does the OSI model differ from the TCP/IP model? How are they similar?
- What is the function of the Physical layer of the OSI model? What is the corresponding layer in the TCP/IP model?
- How does the Presentation layer ensure that data presented to the Application layer is in a compatible form?
- Which protocols are used by the Data Link layer?
- How are host-to-host connections managed?
- Which protocols are used to determine the IP address of a known MAC address?

Key terms for this section include the following:

Term	Definition
Secure Sockets Layer (SSL)	SSL is a data encrypting technology
Simple Mail Transport Protocol (SMTP)	SMTP is an email relay protocol
Post Office Protocol Version 3 (POP3)	POP3 is an email relay protocol
File Transfer Protocol (FTP)	FTP is a file transferring protocol that uses TCP
Trivial File Transfer Protocol (TFTP)	TFTP is a file transferring protocol that uses UDP
Secure Shell (SSH)	SSH is a remote device connectivity protocol
Telnet	Telnet is a remote device connectivity protocol
Simple Network Management Protocol (SNMP)	SNMP is a management and troubleshooting protocol
Domain Name System (DNS)	DNS is a translating protocol
Dynamic Host Configuration Protocol (DHCP)	DHCP is an IP configuration delivery protocol

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.8 Configure network devices for remote access using SSH

Video/Demo	Time
2.2.1 OSI Layers	5:04
2.2.2 OSI Comparison to TCP/IP	2:18
2.2.5 Network Applications	4:15
Total Video Time	**11:37**

Fact Sheets

- 2.2.3 OSI Model Facts
- 2.2.4 OSI Layer Summary
- 2.2.6 TCP/IP Protocol Suite Facts

Number of Exam Questions
10 questions

Total Time
About 37 minutes

2.3: Networking Basics

Lecture Focus Questions:

- What are the two classifications of twisted pair cable?
- What are the characteristics of the Cat 5 unshielded twisted pair (UTP) cable type?
- How do the Cat 5 and Cat 5e types differ?
- What is the general rule for substituting UTP cable types?
- What is the purpose of cladding in fiber optic cabling?
- What are the advantages of fiber optic cabling?
- How do single-mode fiber cables differ from multi-mode?
- What connector types are used with fiber optic cable?

Key terms for this section include the following:

Term	Definition
Internet Service Providers (ISPs)	ISPs are organizations that provide access to the internet as well as providing other internet related services.
Unshielded Twisted Pair (UTP)	UTP is the most commonly used type of Ethernet cable. It consists of two or more twisted pairs of copper wire surrounded by an outer cover.
Fiber Optic	Fiber Optic is a type of cable consisting of glass fibers that transmit data using light.
RJ-45 Connector	RJ-45 is a UTP cable connector typically used in telecommunications or data equipment.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.3 Compare physical interface and cabling types • 1.3.a Single-mode fiber, multimode fiber, copper

Video/Demo	Time
2.3.1 Network Design Overview	2:48
2.3.2 Cables and Connectors	6:11
Total Video Time	**8:59**

Fact Sheets

- 2.3.3 Twisted Pair Facts
- 2.3.4 Fiber Optic Facts

Number of Exam Questions

10 questions

Total Time
About 29 minutes

2.4: Data Encapsulation and Communications

Lecture Focus Questions:

- Which destination address and source address are identified in a frame header?
- When are ARP requests used?
- What information is contained in the unicast response to an ARP broadcast?
- What action does a router perform when it receives frames?
- What happens if there are missing or damaged packets?
- How does data encapsulation facilitate data transmission?
- What are the TCP/IP encapsulation process steps on a sending host?
- What are the TCP/IP de-encapsulation process steps?
- What information does the Transport layer add to data being transmitted?
- What is a PDU? How do PDUs relate to TCP/IP layers?

Key terms for this section include the following:

Term	Definition
Address Resolution Protocol (ARP)	ARP is a system MAC address discovery protocol

Video/Demo	Time
2.4.1 Data Encapsulation and PDUs	5:21
2.4.3 Address Resolution Protocol (ARP)	4:26
2.4.4 Packets and Frames	5:58
Total Video Time	**15:45**

Fact Sheets

- 2.4.2 Data Encapsulation Facts
- 2.4.5 Network Communication Process Facts

Number of Exam Questions

10 questions

Total Time

About 36 minutes

2.5: Ethernet

Lecture Focus Questions:

- What functions do network access technologies provide?
- What are the three most common topology types used by Ethernet?
- What are the components of a chassis-based switch? What function does each component perform?
- What is switch layering? How does it work?
- How does the CSMA/CD network access method help to ensure data delivery?
- What are the components of an Ethernet frame?
- What hardware is required to use full-duplex mode?

Key terms for this section include the following:

Term	Definition
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	CSMA/CD is an Ethernet technology

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.3 Compare physical interface and cabling types • 1.3.a Single-mode fiber, multimode fiber, copper • 1.3.b Connections (Ethernet shared media and point-to-point) • 1.3.c Concepts of PoE 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

Video/Demo	Time
2.5.1 Network Topologies	3:42
2.5.2 Network Access (CSMA/Cx)	7:08
2.5.5 Frame Format	3:58
2.5.7 Ethernet Standards	1:54
Total Video Time	**16:42**

Fact Sheets

- 2.5.3 Ethernet Architecture Facts
- 2.5.4 Half and Full Duplex Facts
- 2.5.6 Ethernet Frame Format Facts
- 2.5.8 Ethernet Standards Facts

Number of Exam Questions

10 questions

Total Time
About 47 minutes

2.6: Network Devices

Lecture Focus Questions:

- What is the function of a switch?
- How does a unicast transmission differ from a broadcast transmission?
- How do routers handle broadcast transmissions?
- What is convergence?
- Why would you use a router instead of a switch?
- How do different network appliances affect network communications?

Key terms for this section include the following:

Term	Definition
Hub	A hub is a networking device that functions as a central connection for networking equipment.
Switch	Switch is a networking device that receives data packets and directs those packets to the intended destination on the local area network.
Router	Router is a networking device that connects a local area network to the internet.
Unicast transmission	A one-to-one transmission in which a device is trying to reach one particular host on the network.
Broadcast transmission	A one-to-many transmission in which a device is trying to reach all hosts on the network.
Multicast transmission	A transmission in which one or more devices send a communication to specific set of devices.
Redundant Array of Inexpensive Disks (RAID)	RAID is a data storage system made up of several disk drives configured to act as one or more units for providing improved performance, data redundancy, or both.
Next generation firewall (NGFW)	NGFW is a more advanced version of the traditional firewall.
Intrusion Prevention System (IPS)	IPS is a network protection and troubleshooting system

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.1 Explain the role and function of network components • 1.1.a Routers • 1.1.b L2 and L3 switches • 1.1.c Next-generation firewalls and IPS • 1.1.d Access points

	• 1.1.e Controllers (Cisco DNA Center and WLC) • 1.1.g Servers 1.13 Describe switching concepts 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG) 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS) 2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

Video/Demo	**Time**
2.6.1 Switches	5:32
2.6.3 Routers	6:51
2.6.5 Internetworks	4:07
2.6.6 Network Appliances	9:12
Total Video Time	**25:42**

Fact Sheets

- 2.6.2 LAN Connectivity Device Facts
- 2.6.4 Router Facts
- 2.6.7 Network Appliance Facts

Number of Exam Questions

10 questions

Total Time

About 51 minutes

3.1: Cisco Device Connection

Lecture Focus Questions:

- How do you connect to a Cisco switch?
- What are the storage methods available on a Cisco device?
- What is the boot sequence for a Cisco device?
- Where is the startup-config file stored?
- Where is the running-config file stored?
- What is stored in read-only memory (ROM)?
- In which locations does the system check for the Internetwork Operation System (IOS) image if the startup-config file is missing?

In this section, you will learn to:

- Boot a router
- Modify configuration files

Key terms for this section include the following:

Term	Definition
Boot loader software	A small program located in ROM that runs after the power-on self-test (POST) completes. The boot loader software is used to locate and launch the operating system.
Central processing unit (CPU) subsystem	The CPU subsystem is made up of the CPU, the dynamic random-access memory (DRAM), and the flash file system. POST checks the CPU subsystem at device bootup.
Non-volatile	Memory that does not lose content when the device is powered down.
Power-on-self-test	A series of tests that a device performs when booting.
Random access memory (RAM)	Volatile memory that is used in routers to provide temporary storage. It is used for running config files, IP routing tables, ARP tables, and the IOS.
Read-only memory	Nonvolatile memory that is used to provide storage for diagnostic software, boot instructions, and some IOS files.
Volatile memory	Memory that loses content when the device is powered down.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.8 Configure network devices for remote access using SSH

Video/Demo	Time
3.1.1 Device Access	2:41
3.1.3 IOS Boot Process	3:43

3.1.4 Boot a Router	6:01
3.1.5 Router Configuration Files	3:14
3.1.6 Modify Configuration Files	3:38
Total Video Time	**19:17**

Fact Sheets

- 3.1.2 Device Connection Facts
- 3.1.7 Manage IOS Files Facts

Number of Exam Questions

10 questions

Total Time

About 40 minutes

3.2: Command Line Interface (CLI)

Lecture Focus Questions:

- Which commands can be used to show information about a router?
- Which commands can be used to copy from one location to another?
- Which commands can be used to get help within the command line?
- How are device interfaces named?

In this section, you will learn to:

- Use the Command Line Interface (CLI)
- Find device information
- Use Command History, Editing, and Help

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	1.1 Setup and configure a router • View router configuration information

Video/Demo	Time
3.2.1 Command Modes	2:31
3.2.2 Use the Command Line Interface (CLI)	8:35
3.2.8 Use Command History, Editing, and Help	6:18
Total Video Time	**17:24**

Lab/Activity

- 3.2.7 Find Device Information

Fact Sheets

- 3.2.3 Command Line Interface Facts
- 3.2.4 Show Command List
- 3.2.5 Copy Command List
- 3.2.6 Interface Naming Facts
- 3.2.9 Command Help Facts
- 3.2.10 Command History Facts
- 3.2.11 Command Editing Facts

Number of Exam Questions

10 questions

Total Time

About 75 minutes

3.3: IOS Licensing

Lecture Focus Questions:

- What is package licensing?
- How can you activate a Cisco Internetwork Operating System (IOS) package?
- What does a Cisco IOS filename indicate?
- How do you backup an Cisco IOS?
- How do you upgrade a Cisco IOS?

In this section, you will learn to:

- View the current license status

Video/Demo	Time
3.3.1 IOS Universal Image Model	3:44
3.3.2 Package Licensing and Activation	2:36
3.3.3 View the Current License Status	3:28
Total Video Time	**9:48**

Fact Sheets

3.3.4 IOS Licensing Facts

Number of Exam Questions

10 questions

Total Time

About 25 minutes

3.4: Device Settings

Lecture Focus Questions:

- What command do you use to set a description for a specific interface?
- How do you remove the interface description?
- What does the no logging console command accomplish?
- How can you change the disconnect time?
- If you enter a banner command without a keyword, which type of banner is created?
- How do you create multiple-line banners?

In this section, you will learn to:

- Configure hostnames and descriptions
- Configure banners
- Modify banners

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	1.1 Setup and configure a router • Configure router hostnames and interface descriptions • Configure router banners 1.2 Setup and configure a switch • Configure switch hostnames and interface descriptions

Video/Demo	Time
3.4.1 Configure Device Settings	11:36
Total Video Time	**11:36**

Lab/Activity

- 3.4.3 Configure Hostnames and Descriptions
- 3.4.6 Configure Banners
- 3.4.7 Modify Banners

Fact Sheets

- 3.4.2 Hostname and Description Command List
- 3.4.4 Screen Output Management Facts
- 3.4.5 Banner Command List

Number of Exam Questions
10 questions

Total Time
About 73 minutes

3.5: Device Passwords

Lecture Focus Questions:

- What is the difference between enable and enable secret passwords?
- How would you require a password to log in through the console?
- What must you do to disable virtual teletype (VTY) login?
- Why is the login command in line mode important?

In this section, you will learn to:

- Set console and VTY passwords
- Configure enable mode passwords
- Modify system passwords

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.1 Configure router security • Configure router passwords 6.2 Configure switch security • Configure switch passwords
Cisco CCNA 200-301	5.3 Configure device access control using local passwords

Video/Demo	Time
3.5.1 Password Levels	1:48
3.5.2 Configure Line Level Passwords	2:03
3.5.5 Configure Enable Mode Passwords	4:51
3.5.8 Router Password Recovery	2:27
3.5.9 Recover a Forgotten Password	3:15
Total Video Time	**14:24**

Lab/Activity

- 3.5.3 Set Console and VTY Passwords
- 3.5.6 Explore Enable Passwords
- 3.5.7 Modify System Passwords

Fact Sheets

- 3.5.4 Device Password Facts
- 3.5.10 Password Recovery Facts

Number of Exam Questions
10 questions

Total Time
About 71 minutes

3.6: Cisco Discovery Protocol (CDP)

Lecture Focus Questions:

- What is the default state of Cisco Discovery Protocol (CDP) on supported interfaces?
- How do you view information about CDP configuration?
- How can you access information about all CDP neighbor devices?
- What command specifies how often CDP packets are exchanged?
- What is the requirement for CDP? What types of devices does it discover information about?

In this section you will learn to:

- Explore CDP
- Configure CDP
- Modify the CDP configuration
- Find CDP information

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	2.1 Configure a router interface • View directly-connected devices using CDP • Manage the CDP Configuration 2.2 Configure a switch interface • Manage the CDP configuration
Cisco CCNA 200-301	2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

Video/Demo	Time
3.6.1 Cisco Discovery Protocol (CDP)	1:39
3.6.2 Set Up CDP	9:15
Total Video Time	**10:54**

Lab/Activity

- 3.6.4 Explore CDP
- 3.6.5 Configure CDP
- 3.6.6 Modify the CDP Configuration
- 3.6.7 Find CDP Information

Fact Sheets

- 3.6.3 CDP Command List
- 3.6.8 Support Non-Cisco Devices with LLDP

Number of Exam Questions

10 questions

Total Time

About 79 minutes

4.1: IPv4 Addressing Overview

Lecture Focus Questions:

- What information do IP addresses provide?
- What is the binary form of the IPv4 address 192.168.46.20?
- What is the role of a subnet mask?
- What is the purpose of the IP address default class?
- What is the default address class of the IP address 132.11.166.5?
- Which three address ranges are used for private IP addresses?
- Using IPv4, how is the host portion of a network address expressed?
- Which network address is used by routers to specify the default route?
- What are commonly used broadcast address formats?
- What is a commonly used loopback address?

Key terms for this section include the following:

Term	Definition
Private IP address	Private addresses aren't routed to the internet.
Public IP address	Public IP addresses are available and accessible on the internet.
Network Address Translation (NAT)	NAT converts private IP address to public IP addresses.
Decimal notation	Decimal notation is a base 10 numbering system. It uses integers 0 – 9.
Binary notation	Binary notation is a numbering system that uses only two integers, 0 and 1.
IP address range class	The class identifies the range and default subnet mask for the address.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing

Video/Demo	Time
4.1.1 Numbering Systems	8:41
4.1.3 IP Addresses	5:07
4.1.4 IP Address Format	6:07
4.1.5 IP Address Classes	6:37
4.1.7 Public vs. Private IP Addresses	5:35
Total Video Time	**32:07**

Fact Sheets

- 4.1.2 Numbering System Facts
- 4.1.6 IP Address Class Facts
- 4.1.8 Public and Private IP Address Facts

Number of Exam Questions

10 questions

Total Time

About 58 minutes

4.2: Subnets

Lecture Focus Questions:

- Which formula is used to determine the decimal value of a binary number?
- What is the purpose of a subnet? How do subnets enable network implementation?
- What does a subnet mask identify?
- Given IP addresses and subnet masks, how do you determine if two workstations are on the same subnet?
- What is the relationship between the number of subnets on a network and the number of hosts on each subnet?
- How are classful addresses different from classless addresses?
- What information do Classless Interdomain Routing (CIDR) routers use to identify networks?
- What is route aggregation?

Key terms for this section include the following:

Term	Definition
Subnet	A subnet is a division in the network.
Variable Length Subnet Mask (VLSM)	VLSM varies the number of bits in the subnet mask to accommodate fewer, larger networks or more, smaller networks.
Supernet	A supernet is a combination of multiple networks.
Classful Address	A classful address uses the default subnet mask.
Classless Address	A classless address uses a custom mask value.
Classless Interdomain Routing	CIDR is an official standard that includes VLSM.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing

Video/Demo	Time
4.2.1 Subnets	6:28
4.2.3 Subnet Math	9:56
4.2.5 Variable Length Subnet Masking (VLSM)	12:03
Total Video Time	**28:27**

Fact Sheets

4.2.2 Subnet Facts

- 4.2.4 Subnet Math Facts
- 4.2.6 VLSM Facts
- 4.2.7 Subnet Operations Facts

Number of Exam Questions
10 questions

Total Time
About 59 minutes

4.3: Subnet Planning and Design

Lecture Focus Questions:

- If you use 8 bits for host addressing, how many hosts can you have on each subnet?
- How do you determine the number of subnets you will need for the network?
- If you want to increase the number of hosts on each subnet, how do you change the subnet mask? What is this process called?

In this section, you will learn to:

- Configure subnet masks.

Key terms for this section include the following:

Term	Definition
IP address design	The IP address design is a document detailing a subnetting plan.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.1 Configure device IP settings • Configure router TCP/IP settings
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting 1.7 Describe the need for private IPv4 addressing

Video/Demo	Time
4.3.1 Subnet Design	6:36
4.3.2 Configure Subnets	1:36
Total Video Time	**8:12**

Lab/Activity

- 4.3.4 Configure Subnet Masks 1
- 4.3.5 Configure Subnet Masks 2

Fact Sheets

- 4.3.3 Subnet Design Facts

Number of Exam Questions

10 questions

Total Time
About 48 minutes

4.4: Route Summarization

Lecture Focus Questions:

- What benefits are provided by route summarization?
- If automatic route summarization is used, how does the router determine which routes to summarize?
- What route becomes the summarized network?
- Which routing protocol does not support automatic route summarization?
- Why do discontiguous networks pose a problem for route summarization?

In this section, you will learn to:

- Configure route summarization.

Key terms for this section include the following:

Term	Definition
Route Summarization	Route summarization is a process that combines routes to subnetted networks.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting

Video/Demo	Time
4.4.1 Route Summarization Overview	3:13
4.4.2 Route Summarization Network Design	3:23
4.4.4 Configure Route Summarization	3:22
Total Video Time	**9:58**

Fact Sheets

- 4.4.3 Route Summarization Facts
- 4.4.5 Route Summarization Command List

Number of Exam Questions

10 questions

Total Time

About 30 minutes

4.5: IPv6 Addressing Overview

Lecture Focus Questions:

- Why was it necessary to implement IPv6?
- How many bits of data does each quartet represent in an IPv6 address?
- How do you properly abbreviate an IPv6 address?
- What two 64-bit parts are contained in an IPv6 address? What does each part represent?
- What is the difference between an anycast address and a unicast address?
- What is the function of the local loopback address?
- How can you easily identify IPv6 multicast addresses?
- What does the special address FF02::2 mean? When is address ::1 used?
- How is the Extended Unique Identifier (EUI-64) format applied?
- When would you use dual stack?
- Which tunneling methods use NAT?
- How does 6 to 4 tunneling differ from the Intra-site Automatic Tunnel Addressing Protocol (ISATAP) method of tunneling? Which is easier to implement?
- How does Teredo tunneling enable host-to-host communication between IPv6 devices through an IPv4 network?
- How are IPv6 addresses created using static partial assignment?
- What is the next step to configure an IPv6 address if the host receives a neighbor advertisement (NA) message?

In this section, you will learn to:

- Configure IPv6

Key terms for this section include the following:

Term	Definition
Native Internet Protocol Security (IPsec)	IPsec is a protocol that can encrypt any traffic supported by the IP protocol.
Flow label	The flow label is a field in the IPv6 packet header.
Prefix	The prefix is the first 64 bits of the IPv6 address.
Interface ID	The interface ID is the last 64 bits of the IPv6 address.
Unicast	Unicast is a type of IPv6 communication involving a single sender and a single recipient.
Link-local	Link-local is a type of IPv6 address that is valid only within the segment or the broadcast domain of the host.
Unique local	Unique local is a private IPv6 address.
Global unicast	Global unicast is a type of IPv6 communication that can be routed globally.
Multicast	Multicast is a type of IPv6 communication sent to multiple IP addresses.

Anycast	Anycast is a type of IPv6 address assigned to a set of interfaces.
Loopback	Loopback is a type of IPv6 address that is the address of the device.
Unspecified	Unspecified is a type of IPv6 address that is represented as (::).
Extended Unique Identifier	EUI-64 is a method that generates the host portion of an endpoint's IP address

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.1 Explain the role and function of network components • 1.1.f Endpoints 1.8 Configure and verify IPv6 addressing and prefix 1.9 Compare IPv6 address types • 1.9.a Global unicast • 1.9.b Unique local • 1.9.c Link local • 1.9.d Anycast • 1.9.e Multicast • 1.9.f Modified EUI 64

Video/Demo	Time
4.5.1 IPv6 Overview	5:08
4.5.3 IPv6 Addressing	5:22
4.5.6 EUI-64 and Auto-Configuration	3:18
4.5.8 Configure IPv6	1:32
Total Video Time	**15:20**

Fact Sheets

- 4.5.2 IPv6 Benefits Facts
- 4.5.4 IPv6 Address Facts
- 4.5.5 IPv6 Address Type Facts
- 4.5.7 EUI-64 Addressing Facts
- 4.5.9 IPv6 Implementation Strategy Facts
- 4.5.10 IPv6 Configuration Facts

Number of Exam Questions

10 questions

Total Time
About 56 minutes

4.6: Dynamic Host Configuration Protocol (DHCP)

Lecture Focus Questions:

- What is the difference between the Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) protocols?
- What is the difference between the Bootstrap Protocol (BootP) and Dynamic Host Configuration Protocol (DHCP) protocols?
- What type of information is delivered by DHCP options?
- How can you make sure a specific host gets the same IP address from the DHCP server each time it boots?
- How does the router determine which interfaces will respond to DHCP requests?
- How can you enable DHCP messages to work across subnets?

In this section, you will learn to:

- Configure a DHCP server
- Configure DHCP manual bindings
- Configure a DHCP relay agent

Key terms for this section include the following:

Term	Definition
Address pool	The address pool is the range of addresses that can be assigned to hosts.
Lease	The lease is the length of time for which the assignment is valid.
Binding	A binding is an association of a MAC address with a specific IP address.
Address Resolution Protocol	ARP discovers the MAC address of a computer from its IP address.
Reverse Address Resolution Protocol	RARP discovers the IP address of a computer from its MAC address.
Bootstrap Protocol	BOOTP queries a bootstrap computer and receives an IP address assignment.
Dynamic Host Configuration Protocol	DHCP dynamically assigns IP address and other TCP/IP configuration parameters.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	5.2 Configure DHCP • Configure the DHCP service on a router • Configure DHCP bindings

Cisco CCNA 200-301	• Configure a DHCP relay agent 4.3 Explain the role of DHCP and DNS within the network 4.6 Configure and verify DHCP client and relay

Video/Demo	Time
4.6.1 DHCP Overview	8:33
4.6.3 Set Up DHCP	3:14
Total Video Time	**11:47**

Lab/Activity

- 4.6.5 Configure a DHCP Server
- 4.6.6 Configure DHCP Manual Bindings
- 4.6.7 Configure a DHCP Relay Agent

Fact Sheets

- 4.6.2 DHCP Facts
- 4.6.4 DHCP Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 68 minutes

4.7: The Domain Name System (DNS)

Lecture Focus Questions:

- How are host names organized in Domain Name System (DNS)?
- What is the difference between a forward lookup zone and a reverse lookup?
- What is the role of the root servers in DNS?
- In DNS, what is the difference between a zone and a domain?
- What is the difference between an A record and a pointer (PTR) record?

In this section, you will learn to:

- Configure DNS addresses
- Create standard DNS zones
- Create host records
- Create CNAME records
- Troubleshoot DNS records

Key terms for this section include the following:

Term	Definition
Domain Name System	DNS is a hierarchical distributed database that links domain names with IP addresses.
. (dot) domain	The . (dot) domain, or root domain, denotes a fully qualified, unambiguous domain name.
Top-Level Domain (TDL)	A TDL is the last part of a domain name.
Fully Qualified Domain Name (FQDN)	The FQDN includes the host name and all domain names separated by periods.
Additional domains	Additional domains are second-level domains with names registered to an individual or organization.
Host name	The host name is the part of a domain name that represents a specific host.
Authoritative server	An authoritative server is a type of DNS server that answers requests for domain names that are within its system. The DNS server does provide answers obtained from another DNS server.
Dynamic DNS (DDNS)	DDNS enables clients or the DHCP server to update records in the zone database.
Recursion	Recursion is a DNS server process for name resolution in which the DNS server communicates with other DNS servers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	5.3 Configure DNS

	• Configure DNS • Create DNS zones • Create DNS records • Troubleshoot DNS
Cisco CCNA 200-301	4.3 Explain the role of DHCP and DNS within the network

Video/Demo	Time
4.7.1 DNS	12:54
4.7.2 Configure DNS	11:32
4.7.4 Configure DNS on a Router	2:14
Total Video Time	**26:40**

Lab/Activity

- 4.7.6 Configure DNS Addresses
- 4.7.7 Create Standard DNS Zones
- 4.7.8 Create Host Records
- 4.7.9 Create CNAME Records
- 4.7.10 Troubleshoot DNS Records

Fact Sheets

- 4.7.3 DNS Facts
- 4.7.5 DNS Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 107 minutes

5.1: Layer 2 Switching Overview

Lecture Focus Questions:

- What is the function of a content addressable memory (CAM) table?
- How does a switch learn information to populate the CAM table?
- When is a CAM table complete?
- When does a switch use flooding? What happens when a switch floods the frame?
- How does the two-tier architecture differ from the three-tier architecture?
- When would you use the spine-and-leaf architecture?
- How does the store and forward method of switching differ from the fragment-free method?
- What conditions can lead to a broadcast storm?

Key terms for this section include the following:

Term	Definition
Access switch	A switch that gives end users access to the local area network.
Distribution switch	A switch that resides in the distribution layer and connects to the access and core switches.
Core switch	A switch that resides in the core layer of a two-tier architecture and connects to distribution switches.
Two-tier	A switch architecture designed with an access layer that contains access switches, and a distribution layer that contains distribution switches.
Three-tier	A switch architecture designed with an access layer, a distribution layer, and a core layer.
Two-tier spine-and-leaf	A switch architecture used in data centers, designed with a leaf layer and a spine layer.
Three-tier spine-and-leaf	A switch architecture used in data centers, designed with a leaf layer, a spine layer, and a core layer.
Unicast frame	A frame sent to a single recipient.
Broadcast frame	A frame sent to all interfaces on the same physical network segment.
Multicast frame	A frame sent to multiple recipients.
Content addressable memory table	A table that contains MAC addresses and the ports used to reach the devices.
Learning	The process a switch uses to determine MAC addresses from frames it receives.
Forwarding	The process a switch uses to send frames to the destination MAC address.

Filtering	The process a switch uses to restrict frames from an IP address.
Flooding	The process a switch uses to find the MAC address of an incoming frame by sending a unicast frame to all ports in the VLAN.
LAN segmentation	The process of dividing the network to overcome problems.
Collision domain	A network or subnetwork where devices share the same transmission medium and where packets can collide.
Broadcast domain	A network or subnetwork where computers receive frame-level broadcasts from their neighbors.
Jitter	A variation in delay as data is transferred between the sending and receiving phones.
Packet loss	When packets do not arrive at the destination.
Echo	Hearing your own voice in the telephone receiver while you are talking.
Cut-through	A switching method where the switch reads the frame until it gets to the destination MAC address and begins forwarding the packet without verifying frame integrity.
Fragment-free	A switching method where the switch reads the first 64 bytes of the data field in a frame before it begins forwarding the packet.
Store-and-forward	A switching method where the switch reads the entire frame and verifies the frame's integrity with the frame check sequence (FCS) before it forwards the frame to the destination device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.1 Explain the role and function of network components • 1.1.f Endpoints 1.2 Describe characteristics of network topology architectures • 1.2.a 2 tier • 1.2.b 3 tier • 1.2.c Spine-leaf 1.3 Compare physical interface and cabling types • 1.3.c Concepts of PoE 1.13 Describe switching concepts • 1.13.a MAC learning and aging

- 1.13.b Frame switching
- 1.13.c Frame flooding
- 1.13.d MAC address table

Video/Demo	Time
5.1.1 Switch Architecture	7:16
5.1.3 Switch Operations	5:30
5.1.4 Unicast, Broadcast, and Multicast Frames	6:08
5.1.6 Collision and Broadcast Domains	5:01
5.1.8 Switching Methods	5:22
Total Video Time	**29:17**

Fact Sheets

- 5.1.2 Switch Architecture Facts
- 5.1.5 Switch Operations Facts
- 5.1.7 Broadcast and Collision Domain Facts
- 5.1.9 Switching Method Facts

Number of Exam Questions

10 questions

Total Time

About 60 minutes

5.2: Switch Interface Configuration

Lecture Focus Questions:

- How does VLAN interface configuration mode differ from Ethernet, Fast Ethernet and Gigabit Ethernet interface configuration modes?
- What must you consider if you manually configure the speed or duplex setting?
- What happens when autonegotiation fails on the Ethernet interface on a Cisco device?
- What is the default setting for a switch?
- How does port numbering differ from switch numbering?
- What is the minimum amount of information a workstation needs in order to communicate on a single subnet? What additional configuration values are required for internetwork communications?
- What address range indicates an APIPA address assignment?
- Why does a switch have an IP address? Which interface is assigned the IP address?

In this section, you will learn to:

- Configure a switch port.
- Configure management VLAN settings.
- Configure switch IP settings.
- Configure device IP settings.
- Explore switch port status.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	2.2 Configure a switch interface • View the status of switch interfaces 3.1 Configure device IP settings • Configure router TCP/IP settings • Configure switch TCP/IP settings 4.1 Configure switch VLANs • Configure VLANs on a switch

Video/Demo	Time
5.2.1 Switch Configuration Overview	3:22
5.2.2 Configure Switch Interfaces	4:00

5.2.6 IP Address and Default Gateway Configuration	2:42
5.2.7 Verify Switch Configuration and Operation	2:54
Total Video Time	**12:58**

Lab/Activity

- 5.2.5 Configure Switch Ports
- 5.2.9 Configure IP Settings on a Switch
- 5.2.10 Configure the Host and Interface on a Switch
- 5.2.11 Configure Device IP Settings
- 5.2.12 Explore Switch Port Status

Fact Sheets

- 5.2.3 Switch Configuration Facts
- 5.2.4 Switch Configuration Mode Facts
- 5.2.8 Switch IP Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 98 minutes

6.1: IPv4 Routing

Lecture Focus Questions:

- What are the primary functions of a router?
- How does a router determine the best path?
- What is the packet forwarding decision process?
- How are administrative distance values used to populate the routing table?

Key terms for this section include the following:

Term	Definition
Administrative distance	The metric that routers use to determine the best path when two or more routes are available to the same destination.
Dynamic route	A route to a network that has been learned using EIGRP, OSPF, or another dynamic routing. protocol.
Metric	A measurable value used to quantify properties of a communication path.
Routing table	A data table that includes information about direct and remote connections.
Static routes	A route to a network that has been manually entered into the routing table.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	3.1 Interpret the components of routing table • 3.1.a Routing protocol code • 3.1.b Prefix • 3.1.c Network mask • 3.1.d Next hop • 3.1.e Administrative distance • 3.1.f Metric • 3.1.g Gateway of last resort 3.2 Determine how a router makes a forwarding decision by default • 3.2.a Longest match • 3.2.b Administrative distance • 3.2.c Routing protocol metric 3.3 Configure and verify IPv4 and IPv6 static routing • 3.3.a Default route

- 3.3.b Network route
- 3.3.c Host route
- 3.3.d Floating static

Video/Demo	Time
6.1.1 Routing Overview	6:29
6.1.3 Routing Metrics	4:36
6.1.4 Administrative Distance (AD)	3:44
Total Video Time	**14:49**

Fact Sheets

- 6.1.2 Routing Table Facts
- 6.1.5 Administrative Distance Facts

Number of Exam Questions

10 questions

Total Time

About 35 minutes

6.2: Static Routing

Lecture Focus Questions:

- What are the advantages and disadvantages of static routing?
- When would you configure static routes?
- When would you configure a default static route?
- When would you configure a floating static route?

In this section, you will learn to:

- Configure static routes

Key terms for this section include the following:

Term	Definition
Stub network	A stub network has a router with only one neighbor and can be reached using only a single route.
Floating static route	A floating static route provides a backup option to a primary route in the event of a link failure. This route is used only if the preferred route is unavailable.
Next-hop static route	A next-hop static route directs traffic only to the next-hop address.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.2 Implement IP routing • Configure static routes on a router 1.3 Compare physical interface and cabling types • 1.3.b Connections (Ethernet shared media and point-to-point)
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting 3.3 Configure and verify IPv4 and IPv6 static routing • 3.3.a Default route • 3.3.b Network route • 3.3.c Host route • 3.3.d Floating static

Video/Demo	Time
6.2.1 Static vs. Dynamic Routing	3:45
6.2.3 Set Up Static Routing	3:23
Total Video Time	**7:08**

Lab/Activity

- 6.2.5 Configure Static Routes

Fact Sheets

- 6.2.2 Static vs. Dynamic Routing Comparison
- 6.2.4 Static and Default Route Command List

Number of Exam Questions

10 questions

Total Time

About 40 minutes

6.3: Dynamic Routing

Lecture Focus Questions:

- What is the difference between internal and external routing?
- What is the purpose of dynamic routing protocols?
- How does a router determine which route will be used to forward a packet?
- What is the difference between distance vector routing and link-state routing?

In this section, you will learn to:

- Find routing table information

Key terms for this section include the following:

Term	Definition
Algorithm	A list of steps to complete a task.
Convergence	All routers have provided each other with updates and the routing tables have the same information.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.2 Implement IP routing • View the routing table on a router

Video/Demo	Time
6.3.1 Dynamic Routing Overview	5:19
6.3.3 Best Path Determination	3:53
6.3.4 Distance Vector Routing Operation	2:45
6.3.6 Link State Routing Operation	3:35
Total Video Time	**15:32**

Lab/Activity

- 6.3.9 Find Routing Table Information

Fact Sheets

- 6.3.2 Dynamic Routing Facts
- 6.3.5 Distance Vector Facts
- 6.3.7 Link State Routing Facts
- 6.3.8 Routing Protocol Comparison Facts

Number of Exam Questions

10 questions

Total Time

About 58 minutes

6.4: IPv4 Routing Troubleshooting

Lecture Focus Questions:

- What does a successful ping verify?
- How does the ping command differ from the traceroute command?
- What are common problems that occur between hosts and routers?
- What causes a port to be in an err-disabled state?
- What are overlapping routes?

In this section, you will learn to:

- Use ping and traceroute
- Use show commands on the router

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux) 3.3 Configure and verify IPv4 and IPv6 static routing • 3.3.a Default route • 3.3.b Network route • 3.3.c Host route • 3.3.d Floating static

Video/Demo	Time
6.4.1 IPv4 Routing Overview	3:34
6.4.2 Routing Troubleshooting Tools	7:56
6.4.3 Use Ping and Traceroute	1:23
6.4.4 Host Configuration Issues	5:35
6.4.5 Router Configuration Issues	6:02
6.4.6 Use Show Commands on the Router	3:25
Total Video Time	**27:55**

Fact Sheets

6.4.7 Troubleshooting IPv4 Routing Facts

Number of Exam Questions

10 questions

Total Time

About 43 minutes

6.5: Network Communications Troubleshooting

Lecture Focus Questions:

- What are common errors that can cause communication problems within a Cisco network?
- Which tools can be used to diagnose network connectivity problems?

In this section, you will learn to:

- Troubleshoot network communications
- Explore TCP/IP communications

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.1 Configure device IP settings • Configure router TCP/IP settings • Configure switch TCP/IP settings
Cisco CCNA 200-301	1.6 Configure and verify IPv4 addressing and subnetting

Video/Demo	Time
6.5.1 Network Communications Troubleshooting	4:53
6.5.3 Troubleshoot Network Communications	3:33
Total Video Time	**8:26**

Lab/Activity

- 6.5.7 Explore TCP/IP Communications

Fact Sheets

- 6.5.2 Network Communications Troubleshooting Facts
- 6.5.4 ICMP Facts
- 6.5.5 IP Troubleshooting Utility Facts
- 6.5.6 IP Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 51 minutes

7.1: Open Shortest Path First (OSPF) Overview

Lecture Focus Questions:

- How do the DR and the BDR reduce network traffic?
- When is the DR not used?
- How is the DR elected? How can you ensure that a specific device becomes the DR?
- What conditions must be met before two routers running OSPF will share information?

In this section, you will learn to:

- Explore OSPF areas

Key terms for this section include the following:

Term	Definition
Area	A sub-domain of an OSPF network which consists of routers, links, and networks that share the same area ID.
Area border router (ABR)	A router that has interfaces in both the backbone area (Area 0) and in a subordinate area.
Link-state advertisement (LSA)	A communication that is sent to neighboring routers which includes the router's topology.
Link-state database (LSDB)	A map of the network which contains active links and network segments. It is built from the information obtained from LSAs.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	3.4 Configure and verify single area OSPFv2 • 3.4.a Neighbor adjacencies • 3.4.b Point-to-point • 3.4.c Broadcast (DR/BDR selection) • 3.4.d Router ID

Video/Demo	Time
7.1.1 OSPF Concepts and Terminology	7:31
7.1.2 OSPF Areas and Border Routers	3:58
7.1.3 Explore OSPF Areas	4:17
7.1.4 OSPF Passive Interfaces and Default Routes	5:24
Total Video Time	**21:10**

Fact Sheets

7.1.5 OSPF Facts

Number of Exam Questions
10 questions

Total Time
About 37 minutes

7.2: OSPF for IPv4

Lecture Focus Questions:

- Must the process ID numbers used on different OSPF routers match?
- What is area 0 in an OSPF implementation?
- How many areas can a single subnet be in?
- What conditions must be met before two routers running OSPF will share information?

In this section, you will learn to:

- Configure OSPF routing for IPv4
- Verify OSPF

Key terms for this section include the following:

Term	Definition
Designated router (DR)	A router that all the internal routers in an area use as the only path for exchange. This minimizes traffic on the network since internal routers do not exchange information with each other. This router has the highest OSPF priority.
Backup designated router (BDR)	The router that will take over the designated router function should the designated router go down. This router has the second highest priority.
Router ID	An assigned IPv4 address made up of a 32-bit binary number which is unique to each router and is used for identification.
Hello interval	A timer that designates how often a hello packet is sent out.
Dead interval	The length of time to wait for a response to the hello packet sent to a neighbor router. If the time expires without a response, that router is considered dead.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	3.4 Configure and verify single area OSPFv2 • 3.4.a Neighbor adjacencies • 3.4.b Point-to-point • 3.4.c Broadcast (DR/BDR selection) • 3.4.d Router ID

Video/Demo	Time
7.2.1 Advanced OSPF Concepts	5:13
7.2.2 Configure OSPF Routing for IPv4	9:08

Total Video Time **14:21**

Fact Sheets

- 7.2.3 OSPF for IPv4 Facts

Number of Exam Questions

10 questions

Total Time

About 30 minutes

7.3: OSPF Configuration

Lecture Focus Questions:

- What is the significance of the router ID?
- What is area 0 in an OSPF implementation?
- How many areas can a single subnet be in?

In this section, you will learn to:

- Configure passive interfaces and default routes
- Enable OSPF
- Explore OSPF
- Configure OSPF

Key terms for this section include the following:

Term	Definition
Point-to-point connection	Two routers connected with a single link. The simplest network.
Passive interface	An OSPF interface that will not send or receive hello packets, will not form adjacencies, and will not send or receive LSAs.
Default route	The default route, also known as the gateway of last resort, is the route used to forward information when the destination address is not in any routing table in the network.
Adjacencies	Routers establish adjacencies with neighbors to exchange link state updates and data description packets.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.3 Configure OSPFv2 routing • Enable OSPF routing • Configure and manage OSPF routing
Cisco CCNA 200-301	3.4 Configure and verify single area OSPFv2 • 3.4.a Neighbor adjacencies • 3.4.b Point-to-point • 3.4.c Broadcast (DR/BDR selection) • 3.4.d Router ID

Video/Demo	Time
7.3.1 Set Up OSPF	6:09

7.3.2 Configure Passive Interfaces and Default Routes	6:52
7.3.3 Verify OSPF	5:06
Total Video Time	**18:07**

Lab/Activity

- 7.3.5 Enable OSPF
- 7.3.6 Explore OSPF
- 7.3.7 Configure OSPF Routing

Fact Sheets

- 7.3.4 OSPF Command List

Number of Exam Questions

10 questions

Total Time

About 70 minutes

7.4: OSPF LSA Types and Databases

Lecture Focus Questions:

- What are the different types of LSAs?
- What is the role of an area border router (ABR)?
- How does a router choose between competing connected and static OSPF routes?
- What are the three databases that OSPF uses?
- When would you use an OSPF multi-area configuration?
- What are backbone routers? What are internal routers?
- What are common interface subcommand configuration problems?
- What is the function of a type 3 inter-area prefix LSA?

In this section, you will learn to:

- Explore LSA types
- Explore OSPF databases

Key terms for this section include the following:

Term	Definition
Link-state advertisement (LSA)	A communication packet that contains topology data for an area of an OSPF network.
Cost	A metric used to calculate the cumulative speed of a route in which the reference bandwidth of 100 Mbps is divided by the interface bandwidth.
Administrative distance (AD)	The process based on reliability that is used by routers to select the best path when there are multiple route possibilities from different routing protocols.
Network topology	A description of the arrangement of routers in a network or area.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	3.4 Configure and verify single area OSPFv2 • 3.4.a Neighbor adjacencies • 3.4.b Point-to-point • 3.4.c Broadcast (DR/BDR selection) • 3.4.d Router ID

Video/Demo	Time
7.4.1 OSPF LSA Types	7:38
7.4.2 Explore LSA Types	4:49

7.4.3 Explore OSPF Databases	3:21
Total Video Time	**15:48**

Fact Sheets

7.4.4 OSPF LSA Types and Databases Facts

Number of Exam Questions

10 questions

Total Time

About 31 minutes

7.5: Adjacency Troubleshooting

Lecture Focus Questions:

- What are the neighbor requirements for adjacency?
- Why is it important to analyze neighbor relationships when troubleshooting IPv4 routing protocols?
- What should you look for when analyzing neighbor relationships?
- What is the E bit? If you get a message that indicates a mismatched E bit, what is the problem?

In this section, you will learn to:

- Explore adjacency issues
- Troubleshoot OSPF

Key terms for this section include the following:

Term	Definition
Subnet (Subnetwork)	A subdivided portion of a large IP network.
Subnet mask	A subnet mask defines the part of the IP address that identifies the network portion and the host portion of the IP address.
Autonomous system	The networks that are within a single administration.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	3.3 Configure OSPFv2 routing • Troubleshoot OSPF routing
Cisco CCNA 200-301	3.4 Configure and verify single area OSPFv2 • 3.4.a Neighbor adjacencies • 3.4.b Point-to-point • 3.4.c Broadcast (DR/BDR selection) • 3.4.d Router ID

Video/Demo	Time
7.5.1 Adjacency Issues	3:56
7.5.2 Explore Adjacency Issues	7:54
Total Video Time	**11:50**

Lab/Activity

- 7.5.4 Troubleshoot OSPF 1
- 7.5.5 Troubleshoot OSPF 2

Fact Sheets

- 7.5.3 Adjacency Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 51 minutes

7.6: EIGRP for IPv4 Routing

Lecture Focus Questions:

- What type of routing protocol is EIGRP?
- What metric is used with EIGRP?
- How does the router calculate the feasible distance?
- What condition must be met for a route to become a feasible successor route?
- What is the difference between a feasible successor and a successor?
- How does EIGRP determine how many paths to keep in its topology database?

In this section, you will learn to:

- Explore EIGRP convergence

Key terms for this section include the following:

Term	Definition
Routing loop	A problem caused in the network when a packet is continuously passed through the same routers.
Convergence	The point at which all routers in an internetwork have the same information in their routing tables.
Feasible distance	The lowest known computed distance value to a destination.
Reported distance	The distance to a destination, as reported by a neighbor.
Computed distance	The total distance to a destination through a specific neighbor router.

Video/Demo	Time
7.6.1 EIGRP Routing Overview	4:45
7.6.2 EIGRP Routing Processes	5:07
7.6.3 EIGRP Convergence	4:46
7.6.4 Explore EIGRP Convergence	6:12
Total Video Time	**20:50**

Fact Sheets

7.6.5 EIGRP Facts

Number of Exam Questions

10 questions

Total Time

About 36 minutes

7.7: EIGRP for IPv4 Configuration

Lecture Focus Questions:

- What are the core steps for configuring EIGRP?
- What is the importance of the autonomous system (AS) number?
- How is EIGRP different from OSPF?
- What are the differences between a contiguous network and a discontiguous network?
- How does EIGRP choose the bandwidth metrics for the optimal route calculation?
- How many paths does load balancing support by default? What is the maximum number of supported paths?

In this section, you will learn to:

- Enable EIGRP.
- Explore auto summary, load balancing, and passive interfaces.

Key terms for this section include the following:

Term	Definition
Discontiguous network	A classful network with two subnets that are connected by another network.
Classful network	A network addressing approach that has a three-part perspective on the subnetted IP address structure that includes an 8-, 16-, or 24-bit network field.
Equal-cost route	A routing process in which next-hop forwarding can go through multiple best paths that are equivalent to the best rank in routing metric calculations to a single destination.
Autonomous system number	A unique identifier that is required for EIGRP named configurations.

Video/Demo	Time
7.7.1 EIGRP Design and Implementation	4:35
7.7.2 Set Up EIGRP Routing	5:00
7.7.3 Verify EIGRP Routing	3:49
7.7.5 EIGRP Load Balancing, Metrics, and Auto-Summarization	4:27
7.7.6 Explore Auto Summary, Load Balancing, and Passive Interfaces	6:14
Total Video Time	**24:05**

Lab/Activity

- 7.7.4 Enable EIGRP

Fact Sheets

7.7.7 EIGRP Implementation Facts

Number of Exam Questions
10 questions

Total Time
About 52 minutes

8.1: IPv6 Routing Overview

Lecture Focus Questions:

- What are the three types of unicast addressing?
- What is the difference between stateful and stateless address autoconfiguration?
- Which command is used to enable IPv6 on a router interface?
- Which utility can you use to verify that DNS is working?
- What are some possible causes of hosts not being able to communicate with a router?
- What can a failed ping from a host to a router indicate?

In this section, you will learn to:

- Explore IPv6 addressing on routers

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.8 Configure and verify IPv6 addressing and prefix 1.9 Compare IPv6 address types • 1.9.a Global unicast • 1.9.b Unique local • 1.9.c Link local • 1.9.d Anycast • 1.9.e Multicast • 1.9.f Modified EUI 64

Video/Demo	Time
8.1.1 IPv6 Routing	6:12
8.1.3 Explore IPv6 Addressing on Routers	6:09
8.1.4 Common IPv6 Troubleshooting Issues	6:25
Total Video Time	**18:46**

Fact Sheets

- 8.1.2 IPv6 Routing Facts
- 8.1.5 IPv6 Routing Facts

Number of Exam Questions

10 questions

Total Time

About 39 minutes

8.2: OSPFv3

Lecture Focus Questions:

- What is the difference between OSPFv2 and OSPFv3?
- Which command is used to enable OSPFv3 routing?
- What are common interface subcommand configuration problems?
- Which command can be used to enable OSPF for IPv6?

In this section, you will learn to:

- Configure OSPFv3 routing
- Verify OSPFv3 routing functionality

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.8 Configure and verify IPv6 addressing and prefix 1.9 Compare IPv6 address types • 1.9.a Global unicast • 1.9.b Unique local • 1.9.c Link local • 1.9.d Anycast • 1.9.e Multicast • 1.9.f Modified EUI 64

Video/Demo	Time
8.2.1 OSPFv3 Routing Overview	3:31
8.2.2 Configure OSPFv3 Routing	5:52
8.2.3 Verify OSPFv3 Routing Functionality	2:31
Total Video Time	**11:54**

Fact Sheets

8.2.4 OSPFv3 Routing Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

8.3: EIGRPv6

Lecture Focus Questions:

- How does EIGRPv6 differ from EIGRPv4?
- How does EIGRP choose the bandwidth metrics for the optimal route calculation?
- What are common EIGRPv6 configuration errors?

In this section, you will learn to:

- Configure EIGRPv6 routing
- Verify EIGRPv6 routing functionality

Video/Demo	Time
8.3.1 EIGRPv6 Routing Overview	5:32
8.3.2 Configure EIGRPv6 Routing	3:25
8.3.3 Verify EIGRPv6 Routing Functionality	3:38
Total Video Time	**12:35**

Fact Sheets

8.3.4 EIGRPv6 Routing Facts

Number of Exam Questions

10 questions

Total Time

About 28 minutes

9.1: Wireless Concepts

Lecture Focus Questions:

- Under what circumstances might you choose an ad hoc wireless network?
- What device is used to create an infrastructure wireless network?
- How do wireless networks control media access?
- What is the difference between a BSS and an ESS?
- What do wireless clients use to identify a specific wireless access point?
- How do multiple access points identify themselves as part of the same network?

Key terms for this section include the following:

Term	Definition
Frequency Hopping Spread Spectrum (FHSS)	A signaling method that uses a narrow frequency band and hops data signals in a predictable sequence from frequency to frequency over a wide band of frequencies.
Direct-Sequence Spread Spectrum (DSSS)	A signaling method that breaks data into pieces and sends the pieces across multiple frequencies in a defined range.
Orthogonal Frequency-Division Multiplexing (OFDM)	A signaling method that breaks data into very small data streams to send the information across long distances where environmental obstacles may be an issue.
Ad hoc	A network topology that works in peer-to-peer mode without an access point.
Infrastructure	A network topology that uses an access point (AP) that functions like a hub on an Ethernet network.
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)	A network multiple access method used to control media access and avoid (rather than detect) collisions.
Station (STA)	A wireless NIC in an end device such as a laptop or wireless PDA.
Access point (AP)	A device that coordinates all communications between wireless devices, as well as the connection to the wired network.
Basic Service Set (BSS)	The smallest unit of a wireless network.
Independent Basic Service Set (IBSS)	A set of STAs configured in ad hoc mode.
Extended Service Set (ESS)	A set of multiple BSSs with a distribution system (DS).
Distribution System (DS)	The backbone or LAN that connects multiple APs (and BSSs) together.
Service Set Identifier (SSID)	A 32-character value that is inserted into each frame.

Basic Service Set Identifier (BSSID)	A 48-bit value that identifies an AP in an infrastructure network or an STA in an ad hoc network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.11 Describe wireless principles • 1.11.a Nonoverlapping Wi-Fi channels • 1.11.b SSID • 1.11.c RF 2.6 Compare Cisco Wireless Architectures and AP modes 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

Video/Demo	Time
9.1.1 Radio Frequency Wireless	8:07
9.1.2 Wireless Architecture	7:52
Total Video Time	**15:59**

Fact Sheets

- 9.1.3 Wireless Architecture Facts
- 9.1.4 Wireless Infrastructure Facts

Number of Exam Questions

10 questions

Total Time

About 36 minutes

9.2: Wireless Standards

Lecture Focus Questions:

- What are the differences between 802.11a and 802.11g specifications?
- Devices that support the 802.11g standards are typically compatible with which other wireless standard?
- How does MIMO differ from channel bonding?
- Why is channel bonding typically not used with the 2.4 GHz range?
- What happens when an 802.11a device connects to an access point that supports both 802.11n and 802.11a? What happens if the access point uses MIMO and supports dual band?
- What types of devices typically use Bluetooth wireless?

In this section, you will learn to:

- Configure Bluetooth connections.

Key terms for this section include the following:

Term	Definition
Multiple-Input, Multiple-Output (MIMO)	An antenna technology that increases bandwidth by using multiple antennas for both the transmitter and receiver.
Channel bonding	A practice that combines two non-overlapping channels into a single channel, resulting in slightly more than double the bandwidth.
Frame composition	The structure of the data frame which results in increased efficiency of data transmissions (less overhead).
Multi-user MIMO (MU-MIMO)	A wireless technology used by routers and endpoint devices that allows multiple users to use the same channel.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.11 Describe wireless principles • 1.11.a Nonoverlapping Wi-Fi channels

Video/Demo	Time
9.2.1 Wireless Standards	13:24
9.2.2 Infrared	3:34
9.2.3 Bluetooth	4:27
9.2.4 Configure Bluetooth Connections	5:26
Total Video Time	**26:51**

Fact Sheets

- 9.2.5 Wireless Standards Facts

Number of Exam Questions

10 questions

Total Time

About 42 minutes

9.3: Wireless Configuration

Lecture Focus Questions:

- What information does the wireless profile contain?
- What is the strongest encryption method?
- How does a MAC access list help keep a network secure?
- What is the purpose of a beacon?
- How are wireless networks listed in the notification area?

In this section, you will learn to:

- Create a wireless network for home use.
- Secure a wireless network for home use.

Key terms for this section include the following:

Term	Definition
Region	A physical area where the AP operates.
Advanced Encryption Standard (AES)	AES is an encryption method used with WPA2.
Temporal Key Integrity Protocol (TKIP)	TKIP is an encryption method used with WPA or WPA2.
Beacon	A frame that is sent out by the AP periodically.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Create a wireless network • Secure a wireless network 1.11 Describe wireless principles • 1.11.b SSID
Cisco CCNA 200-301	2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings 5.10 Configure WLAN using WPA2 PSK using the GUI

Video/Demo	Time
9.3.1 Wireless Network Configuration	9:31

9.3.3 Configure Wireless Networks	9:47
Total Video Time	**19:18**

Lab/Activity

- 9.3.4 Create a Home Wireless Network
- 9.3.5 Secure a Home Wireless Network

Fact Sheets

- 9.3.2 Wireless Configuration Tasks

Number of Exam Questions

10 questions

Total Time

About 59 minutes

9.4: Wireless Network Design

Lecture Focus Questions:

- What is device density?
- What is the difference between received signal length and signal to noise ratio?
- Which implementation automatically partitions a single broadcast domain into multiple VLANs?
- What information is specified in a logical network diagram?
- How do you measure the signal strength at a given distance from the access point?
- What is the Z-Wave protocol commonly used for?

In this section, you will learn to:

- Design an indoor wireless network.
- Design an outdoor wireless network.

Key terms for this section include the following:

Term	Definition
Z-Wave	A wireless communication protocol that's broadly used in home security and home automation.
ANT+	A protocol for monitoring sensor data.
Near-Field Communication (NFC)	A set of communication protocols that allows devices to communicate and share data with each other.
Goodput	The number of useful bits delivered from the sender to the receiver over the wireless network connection.
Site survey	A component of planning and designing a wireless network. It assesses the physical features of the location of a wireless network.
Spectrum analysis	The process of gathering the frequencies or other related quantities in a specific area.
Spectrum analyzer	A tool used to determine the noise floor in the desired frequency range, allowing you to select the best available wireless channel.
Received Signal Level (RSL)	A measurement that identifies how strong the radio signal is at the receiver. The closer you are to the transmitter, the stronger the RSL. The farther away you are, the lower the RSL.
Signal-to-noise ratio (SNR)	A measurement that compares the level of the wireless network signal (RSL) to the level of background noise (measured in decibels).
Channel plan	A plan that identifies which AP will use which channel.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Design a wireless network
Cisco CCNA 200-301	1.11 Describe wireless principles • 1.11.b SSID

Video/Demo	Time
9.4.1 Wireless Network Design	7:03
9.4.2 Site Survey	7:17
9.4.3 Wireless Antenna Types	6:11
9.4.5 Conduct a Wireless Survey	4:40
Total Video Time	**25:11**

Lab/Activity

- 9.4.7 Design an Indoor Wireless Network
- 9.4.8 Design an Outdoor Wireless Network

Fact Sheets

- 9.4.4 Wireless Network Design Facts
- 9.4.6 Wireless Site Survey Facts

Number of Exam Questions

10 questions

Total Time

About 70 minutes

9.5: Wireless Network Implementation

Lecture Focus Questions:

- What is the difference between a hub-and-spoke infrastructure and a distributed wireless mesh infrastructure?
- What is a lightweight access point used for?
- Which protocol is used to route frames back and forth between the wireless network and the wired LAN?
- Which enterprise deployment has limited mobility and is difficult to manage?

In this section, you will learn to:

- Implement an enterprise wireless network.

Key terms for this section include the following:

Term	Definition
Independent access points	A deployment model implemented by large organizations through their facilities. Each AP stood alone, providing separate wireless networks by using its own independent configuration.
Hub-and-spoke infrastructure	A deployment model where a wireless controller is connected to all APs through wired links.
Distributed wireless mesh infrastructure	A deployment model that moves some of the network intelligence from the controller out to the individual APs. In this configuration, the controller is no longer a bottleneck.
Lightweight Access Point Protocol (LWAPP)	A protocol used to route frames back and forth between the wireless network and the wired LAN.
Wireless bridge	A device used to connect wired or wireless networks together.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Implement and configure a wireless network
Cisco CCNA 200-301	2.6 Compare Cisco Wireless Architectures and AP modes 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)

Video/Demo	Time
9.5.1 Enterprise Wireless Equipment	7:47
9.5.2 Configure an Enterprise Wireless Network	8:09
Total Video Time	**15:56**

Lab/Activity

- 9.5.4 Implement an Enterprise Wireless Network

Fact Sheets

- 9.5.3 Enterprise Wireless Facts

Number of Exam Questions

10 questions

Total Time

About 43 minutes

9.6: SOHO Configuration

Lecture Focus Questions:

- In a small home/home office (SOHO) network, which types of devices are typically used to connect the location to the internet?
- What function does enabling NAT on the router provide for a SOHO network?
- What is the difference between a public IP address and a private IP address? What are the private IP address ranges?
- What are the advantages of turning off SSID broadcasting?
- What is the purpose of MAC address filtering?
- Once DHCP is disabled on a wireless access point, what three elements would an attacker have to configure to be able to connect?
- What guidelines should you consider when selecting the location of the access point to ensure the signal strength and network access?

In this section, you will learn to:

- Configure a wireless infrastructure

Key terms for this section include the following:

Term	Definition
Small home/home office network	A small network with typically 10 or fewer users.
SSID suppression	The act of disabling the SSID broadcast. This is also known as cloaking.
Network Address Translation (NAT)	A method for remapping one IP address space into another by modifying network address information in the headers of IP packets while they are in transit.
Wi-Fi Protected Setup (WPS)	A network security standard for wireless home networks.
Home network	A profile designed for networks in which you know and trust every device.
Work network	A profile designed to be used in a SOHO.
Public Network	A profile designed for use on unknown networks.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Implement and configure a wireless network

Cisco CCNA 200-301	1.2 Describe characteristics of network topology architectures • 1.2.e Small office/home office (SOHO)

Video/Demo	Time
9.6.1 SOHO Configuration	9:41
9.6.3 Configure a SOHO Router	13:10
9.6.4 Configure a Wireless Access Point	5:36
Total Video Time	**28:27**

Lab/Activity

- 9.6.7 Configure a Wireless Infrastructure

Fact Sheets

- 9.6.2 SOHO Configuration Facts
- 9.6.5 Access Point Configuration Facts
- 9.6.6 Windows Network Profile Facts

Number of Exam Questions

10 questions

Total Time

About 66 minutes

9.7: Wireless Security

Lecture Focus Questions:

- What does open authentication use to authenticate a device?
- Why is open authentication a non-secure solution?
- Which two additional components are required to implement 802.1x authentication?
- What is the difference between WPA Personal and WPA Enterprise?
- How can geofencing protect your network?
- Which default values should you always change on your wireless network?

In this section, you will learn to:

- Secure an Enterprise wireless network.

Key terms for this section include the following:

Term	Definition
Authentication	The process of proving identity.
Open System Authentication	An authentication method that requires clients to provide a MAC address in order to connect to the wireless network.
Pre-Shared Key	An authentication method that uses a secret or a passphrase previously shared between two parties using a secure channel before it can be used.
802.1x	An authentication method and standard that uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients.
Wi-Fi Protected Access (WPA)	A wireless security protocol based on initial 802.11i drafts that was deployed in 2003.
Wi-Fi Protected Access 2 (WPA2)	A wireless security protocol based on the 802.11i specifications and deployed in 2005.
Wi-Fi Protected Access 3 (WPA3)	A wireless security protocol based on the 802.11s specifications and deployed in 2018.
Geofencing	A virtual boundary of a physical location.
Rogue access point	An unauthorized access point added to a network.
Evil twin	A rogue AP configured to mimic a valid AP.
Data emanation	Wireless signals that extend beyond the intended area of coverage
Wardriving	A technique used to find wireless networks.
Warchalking	Symbols drawn, often using chalk, outside a building to indicate the presence of one or more wireless networks. The identification of the network may indicate it is targeted for attack.
Packet sniffing	The interception and decoding of wireless transmissions.

Interference	A signal that corrupts or destroys the wireless signal sent by APs and other wireless devices.
Electromagnetic interference (EMI)	A signal caused by motors, heavy machinery, and fluorescent lights.
Radio frequency interference (RFI)	A signal caused by radio signals using the same radio channel. It can be caused by nearby wireless devices, such as cordless phones or microwave ovens.
Jamming	Signal interference created intentionally by an attacker to make a wireless network impossible to use.
Spark jamming	A Wi-Fi interference attack repeatedly blasting equipment with high-intensity, short-duration RF bursts at a rapid pace.
Deauthentication	An attack that spoofs your MAC address and then tells your wireless network to disconnect you from the network.
Bluetooth	A standard for the short-range wireless interconnection designed to allow devices to communicate within a close proximity.
Personal area network (PAN)	A computer network for connecting devices around an individual's workspace.
Bluejacking	The practice of anonymously sending business cards to a Bluetooth recipient within a distance of 10–100 meters, depending on the class of the Bluetooth device. The business cards usually include a flirtatious message to elicit a visual reaction from the recipient.
Bluesnarfing	An attack where an attacker gains unauthorized access to an existing Bluetooth connection between phones, desktops, laptops, or PDAs.
Bluebugging	An attack that gives an attacker access to all mobile phone commands that use Bluetooth technology. Such commands include those that initiate phone calls, send and receive messages, listen to phone calls, and read and write phonebook contacts.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Secure a wireless network
Cisco CCNA 200-301	1.11 Describe wireless principles • 1.11.b SSID • 1.11.d Encryption

	2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS) 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

Video/Demo	Time
9.7.1 Wireless Security	10:23
9.7.3 Wireless Attacks	9:40
9.7.5 Secure a Wireless Network	13:26
Total Video Time	**33:29**

Lab/Activity

- 9.7.6 Secure an Enterprise Wireless Network

Fact Sheets

- 9.7.2 Wireless Security Facts
- 9.7.4 Wireless Attack Facts

Number of Exam Questions

10 questions

Total Time

About 66 minutes

9.8: Wireless Troubleshooting

Lecture Focus Questions:

- Where is the best place to situate your wireless access point?
- What types of objects might obstruct wireless radio frequency transmissions?
- How many channels should separate two wireless networks?
- Which types of wireless networks require line-of-sight connections?
- How do range and antenna placement affect wireless networks?
- How does refraction affect your RF signal?

In this section, you will learn to:

- Optimize a wireless network.
- Explore wireless network problems.
- Troubleshoot wireless network problems.

Key terms for this section include the following:

Term	Definition
Latency	The time it takes a device to receive a sent signal.
Bandwidth saturation	The point at which all available bandwidth on an internet connection has achieved maximum capacity and cannot pass any more data through the connection.
Device saturation	The point at which the percentage of CPU usage where I/O requests are issued to a device is at or close to 100%, or the bandwidth utilization for the device is close to 100%.
Untested updates	Updates that have not been tested in a network test environment before you apply them to your network.
Frequency mismatch	Devices on the network are not broadcasting on the same frequency.
Absorption	The rate at which a signal passes through objects and loses power or gets weaker.
Refraction	Radio waves that pass through objects of different densities which cause the signal to bend or change speeds.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.5 Configure wireless networking • Optimize a wireless network • Troubleshoot a wireless network
Cisco CCNA 200-301	1.11 Describe wireless principles

- 1.11.a Nonoverlapping Wi-Fi channels
- 1.11.b SSID

Video/Demo	Time
9.8.1 Wireless Communications Troubleshooting	11:35
9.8.2 Troubleshoot Wireless Connections	6:23
9.8.4 Optimize Wireless Networks	7:26
Total Video Time	**25:24**

Lab/Activity

- 9.8.5 Optimize a Wireless Network
- 9.8.6 Explore Wireless Network Problems
- 9.8.7 Troubleshoot Wireless Network Problems

Fact Sheets

- 9.8.3 Wireless Network Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 77 minutes

10.1: WAN Types

Lecture Focus Questions:

- How do private wide area networks (WANs) differ from public WANs?
- Which topologies are used by WANs?
- How does using leased lines for a WAN differ from using Multi-Protocol Label Switching (MPLS)?
- What are the advantages to using MPLS?
- What is an Ethernet handoff? What advantage does it have in WAN communication?
- How does a circuit switching WAN system differ from a packet switching implementation?
- What components are included in customer provided equipment (CPE)?
- What role does data communication equipment (DCE) play in WAN communications?

Key terms for this section include the following:

Term	Definition
Wide area network	Two or more local area networks (LANs) connected together, usually spanning a wide geographical area.
Private WAN	A private WAN uses communication channels that are not publically accessible to allow sites within the private network to communicate.
Public WAN	A public WAN allows access to any number of other sites, like the internet.
Multi-Protocol Label Switching	A high-performance method for forwarding packets through a network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.2 Describe characteristics of network topology architectures • 1.2.d WAN 1.3 Compare physical interface and cabling types • 1.3.b Connections (Ethernet shared media and point-to-point)

Video/Demo	Time
10.1.1 WAN Overview	3:41
10.1.3 Common WAN Technologies	4:57

Total Video Time **8:38**

Fact Sheets

- 10.1.2 WAN Type Facts
- 10.1.4 WAN Facts

Number of Exam Questions

10 questions

Total Time

About 29 minutes

10.2: Leased Line WAN Links

Lecture Focus Questions:

- What is a leased-line wide area network (WAN) link?
- What is High-level Data Link Control (HDLC) and what benefits does it provide?
- How do you configure routers to use HDLC over a leased line?
- What is the purpose of the frame check sequence (FCS) field used in the HDLC protocol?
- What are the roles of data communications equipment (DCE), data terminal equipment (DTE), and channel service units (CSUs) in a leased-line WAN link?
- What types of telecommunication lines are available for a leased-line WAN link?

In this section, you will learn to:

- Explore serial interface status
- Configure back-to-back routers

Key terms for this section include the following:

Term	Definition
Leased line	A dedicated, always-on circuit between two endpoints usually obtained through a service provider.
High-level Data Link Control	Often used as the data link protocol for WAN leased-line connections.
CPE	Customer Premise Equipment (CPE) is the equipment at the customer site.
Channel Service Unit Data Service Unit (DSU)	A digital-interface device used to connect DTE, such as a router, to a digital circuit, such as T1 line.
Data Communications Equipment	A device that sits between the DTE and a data transmission circuit, like a modem.
Data Terminal Equipment	An end instrument that converts user information into signals or converts received signals into user information, like a computer terminal.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	1.1 Setup and configure a router • View router configuration information 2.1 Configure a router interface

Cisco CCNA 200-301	• Configure Ethernet and serial router interfaces 3.1 Configure device IP settings • Configure router TCP/IP settings 1.2 Describe characteristics of network topology architectures • 1.2.d WAN

Video/Demo	Time
10.2.1 Leased Line Overview	8:10
10.2.2 Explore HDLC Links	3:55
10.2.5 Set Up Back-to-Back Routers	4:15
Total Video Time	**16:20**

Lab/Activity

- 10.2.4 Explore Serial Interface Status
- 10.2.7 Configure Back-to-Back Routers

Fact Sheets

- 10.2.3 Leased Line Facts
- 10.2.6 Serial Interface Command List

Number of Exam Questions

10 questions

Total Time

About 61 minutes

10.3: Network Address Translation (NAT)

Lecture Focus Questions:

- What are the benefits of using Network Address Translation (NAT)?
- What is the difference between an inside global address and an outside global address?
- What is overloading? Why is it important in a NAT configuration?
- How is an access list used in NAT configuration?
- How do you link a NAT address pool to an access list and an interface?
- Which parameter must you use in your NAT configuration if you have more private hosts than public IP addresses?
- Which NAT configuration method associates a specific outside IP address with an inside host?

In this section, you will learn to:

- Configure dynamic NAT
- Configure static NAT
- Configure Port Address Translation (PAT)

Key terms for this section include the following:

Term	Definition
Network Address Translation	Allows you to connect a private network to the internet without obtaining registered addresses for every host.
Port Address Translation	Is used to translate multiple inside addresses to a single public address using unique, dynamic ports. It is also known as NAT Overloading or Overloaded NAT.
Static NAT	Translates a single outside address to a single inside address
Dynamic NAT	Translates a range of outside addresses to a range of inside addresses.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	5.1 Configure NAT • Configure static NAT on a router • Configure dynamic NAT on a router • Configure PAT on a router
Cisco CCNA 200-301	4.1 Configure and verify inside source NAT using static and pools

Video/Demo **Time**

10.3.1 NAT Overview	8:03
10.3.3 Set Up Dynamic NAT	4:45
10.3.5 Set Up Static NAT	2:49
10.3.7 Set Up Port Address Translation (PAT)	3:31
Total Video Time	**19:08**

Lab/Activity

- 10.3.4 Configure Dynamic NAT
- 10.3.6 Configure Static NAT
- 10.3.8 Configure Port Address Translation (PAT)

Fact Sheets

- 10.3.2 NAT Facts

Number of Exam Questions

10 questions

Total Time

About 71 minutes

10.4: WAN Troubleshooting

Lecture Focus Questions:

- What are some possible causes of layer 1 problems?
- If a ping or traceroute fails, what can you examine to rule out layer 1 and layer 2 issues?
- At which layer is there a problem if a Telnet or SSH test fails?
- What does an interface status of down, down indicate? What does up, down indicate?
- What should you verify when troubleshooting TCP/IP connectivity?

In this section, you will learn to:

- View serial interface status
- Troubleshoot a serial connections

Key terms for this section include the following:

Term	Definition
show *[parameters]*	A router command used to show routing information, interface information, IP routing, configuration files, and serial interface configuration.
traceroute *[parameters]*	A router command used to verify Network layer connectivity between two points. It can also be used to test DNS address resolution.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	2.1 Configure a router interface • Configure Ethernet and serial router interfaces • Troubleshoot router connections
Cisco CCNA 200-301	1.2 Describe characteristics of network topology architectures • 1.2.d WAN

Video/Demo	Time
10.4.1 Serial WAN Link Troubleshooting	4:57
10.4.2 Troubleshoot WAN Issues	7:07
Total Video Time	**12:04**

Lab/Activity

- 10.4.4 View Serial Interface Status
- 10.4.5 Troubleshoot a Serial Connection 1
- 10.4.6 Troubleshoot a Serial Connection 2

Fact Sheets

- 10.4.3 WAN Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 64 minutes

11.1: Virtual LANs (VLANs)

Lecture Focus Questions:

- What are two advantages to creating virtual LANs (VLANs) on your network?
- You have two VLANs configured on a single switch. How many broadcast domains are there? How many collision domains are there?
- What happens if two devices on the same switch are assigned to different VLANs?

In this section, you will learn to:

- Create VLANs

Key terms for this section include the following:

Term	Definition
Broadcast domain	A logical network division in which all nodes can reach one another at the Data Link layer (layer 2).
Virtual LAN	A broadcast domain that is partitioned at the Data Link layer (layer 2).
Voice over IP (VoIP)	Hardware and software that uses the internet and data packets to transmit voice calls.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.1 Configure switch VLANs • Configure VLANs on a switch
Cisco CCNA 200-301	2.1 Configure and verify VLANs (normal range) spanning multiple switches • 2.1.a Access ports (data and voice) • 2.1.b Default VLAN • 2.1.c Connectivity 2.2 Configure and verify interswitch connectivity • 2.2.b 802.1Q

Video/Demo	Time
11.1.1 VLAN Overview	4:51
11.1.3 Configure VLANs	6:18

Total Video Time **11:09**

Lab/Activity

- 11.1.5 Create VLANs

Fact Sheets

- 11.1.2 VLAN Facts
- 11.1.4 VLAN Command List

Number of Exam Questions

10 questions

Total Time

About 44 minutes

11.2: Trunking

Lecture Focus Questions:

- Why is trunking important to virtual LAN (VLAN) configuration?
- Which trunking protocols are supported on a Cisco 2960 switch? Which protocol is an industry standard?
- What protocol does a Cisco switch use to automatically detect trunk ports?
- By default, traffic from which VLANs are allowed on trunk ports?
- What is the default configuration of most Cisco switches?
- A trunk port is set to dynamic desirable. Which configurations on other switches are allowed so the port enters a trunking state?
- What is the purpose of the VLAN Trunk Protocol (VTP)?
- What is the purpose of changing the default native VLAN?

In this section, you will learn to:

- Configure trunking
- Configure the native VLAN
- Configure allowed VLANs

Key terms for this section include the following:

Term	Definition
Trunking	The connection of two switches.
Trunking protocol	The format switches use for tagging frames with the VLAN ID.
Inter-Switch Link (ISL)	Cisco's proprietary trunking protocol.
802.1Q	An IEEE standard trunking protocol that is widely used on many devices.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.1 Configure switch VLANs • Configure VLANs on a switch • Use trunking to extend VLAN to multiple switches
Cisco CCNA 200-301	2.1 Configure and verify VLANs (normal range) spanning multiple switches • 2.1.a Access ports (data and voice) • 2.1.b Default VLAN • 2.1.c Connectivity

	2.2 Configure and verify interswitch connectivity • 2.2.a Trunk ports • 2.2.b 802.1Q • 2.2.c Native VLAN 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

Video/Demo	Time
11.2.1 Access and Trunk Ports	5:47
11.2.3 Set Up Trunking	3:23
11.2.7 Set Up the Native VLAN	6:02
Total Video Time	**15:12**

Lab/Activity

- 11.2.5 Configure Trunking
- 11.2.9 Configure the Native VLAN
- 11.2.10 Configure Allowed VLANs

Fact Sheets

- 11.2.2 Trunking Facts
- 11.2.4 Trunking Command List
- 11.2.6 Advanced Trunking Configuration
- 11.2.8 VLAN Trunking Protocol (VTP)

Number of Exam Questions

10 questions

Total Time

About 82 minutes

11.3: Spanning Tree

Lecture Focus Questions:

- What is a bridging loop? How does the Spanning Tree Protocol (STP) eliminate bridging loops?
- What advantages does STP provide?
- How is the root bridge determined?
- How do designated bridges differ from backup bridges?
- What is the function of Bridge Protocol Data Units (BPDUs)?
- How do bridges recover from the loss of a bridge on the network?
- Which ports become root ports?
- Which port state builds the bridge database with MAC addresses?
- A switch port is identified as a backup port. What state is it in?
- What advantages are added to spanning tree with the edge port type definition? How does this improve performance?
- What advantages does the EtherChannel feature provide?
- Why must EtherChannel be used to create multiple links that can be used at the same time between switches?
- How does EtherChannel interact with spanning tree?
- What function does BPDU guard provide?

In this section, you will learn to:

- Configure EtherChannel with Port Aggregation Protocol (PAGP)
- Configure EtherChannel with Link Aggregation Control Protocol (LACP)

Key terms for this section include the following:

Term	Definition
Spanning Tree Protocol	The protocol that assigns a designated bridge or switch for each route. It is also referred to as the Spanning Tree Algorithm (STA).
Bridge ID (BID)	An identification number composed of the priority number of the bridge and its MAC address.
Bridge Protocol Data Unit	Data messages exchanged between switches to communicate information about ports, addresses, priorities, and costs. Hello packets are the most common BPDUs.
Switching loop	Redundant paths between segments in which packets are endlessly routed. It is also called a bridge loop.
Root bridge	The bridge with the lowest bridge ID. It is at the top of the STP hierarchy and serves as a reference point for all switches.
Designated bridge	The bridge that is allowed to send and receive frames onto a segment.
Backup bridge	The bridge that takes over when a bridge fails.

Disabled bridge	A bridge that is powered on but does not participate in forwarding or listening to network messages. A bridge must be manually placed in the disabled state.
Listening port	Listening is a transitory state between blocking and learning. After a change has occurred, a port remains in the listening state for a specific period of time. For example, if a bridge goes down, all other bridges go to the listening state while the bridges redefine their roles.
Learning port	A port in the learning state receives packets and builds the bridge database that associates MAC addresses with ports. A timer is associated with this state. The port goes to the forwarding state after the timer expires.
Forwarding port	A port in the forwarding state can both learn and forward. All ports of the root switch are in forwarding mode.
Root port	The port on the designated switch with the lowest port cost back to the root bridge.
Designated port	The port on the segment that is allowed to send and receive frames onto that segment.
Blocking port	Any port that is not a root or a designated port. A blocking port is in blocking state.
EtherChannel	Port link aggregation technology that combines multiple switch ports into a single, logical link between two switches.
Port Aggregation Protocol (PAgP)	A management function that checks the parameter consistency at either end of the link and assists the channel in adapting to link failure or addition. PAgP prevents loops and packet loss due to misconfigured channels and aids in network reliability.
Link Aggregation Control Protocol (LACP)	A management function based on the 802.3ad standard. It has similar functions to PAgP. LACP should be used when configuring EtherChannel between Cisco switches and non-Cisco vendor switches that support 802.3ad.
PortFast	An STP function that allows a port to skip the listening and learning states and go from a blocking state to a forwarding state immediately.
BPDU Guard	An STP function that prevents certain switch ports from connecting to other switches. It prevent switching loops and unauthorized connections.
Rapid Spanning Tree Protocol (Rapid STP)	A variaton of the standard STP specification that improves convergence performance by actively confirming when a switch port is ready to transition to a forwarding state, which reduces convergence time.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.4 Configure EtherChannel

Cisco CCNA 200-301	• Configure EtherChannel using PAGP • Configure EtherChannel using LACP 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP) 2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations • 2.5.a Root port, root bridge (primary/secondary), and other port names • 2.5.b Port states (forwarding/blocking) • 2.5.c PortFast benefits 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

Video/Demo	Time
11.3.1 Spanning Tree Protocol (STP)	10:54
11.3.5 View the MAC Table	5:54
11.3.6 STP Topology	11:26
11.3.7 Advanced STP Features	6:41
11.3.9 Set Up EtherChannels	8:07
Total Video Time	**43:02**

Lab/Activity

- 11.3.11 Configure EtherChannel with PAGP
- 11.3.12 Configure EtherChannel with LACP

Fact Sheets

- 11.3.2 Spanning Tree Protocol Facts
- 11.3.3 Spanning Tree Configurations
- 11.3.4 Switching Loops Facts
- 11.3.8 Advanced STP Facts
- 11.3.10 EtherChannel Facts

Number of Exam Questions

10 questions

Total Time

About 103 minutes

11.4: Spanning Tree Configuration

Lecture Focus Questions:

- Why will a tie breaker never be necessary when selecting the root switch?
- When would you modify an Spanning Tree Protocol (STP) mode?
- How does Per VLAN Spanning Tree Protocol (PVST+) differ from Rapid PVST+?
- How do ports work in a multiple-VLAN environment?
- How are root bridges designated in a multiple-VLAN environment?
- What happens during STP convergence?

In this section, you will learn to:

- Configure the root bridge
- Configure the primary and secondary root bridges
- Configure Rapid PVST+
- Find STP information

Key terms for this section include the following:

Term	Definition
Per VLAN Spanning Tree Protocol	A Spanning Tree mode that maintains a Spanning Tree instance for each VLAN in the network. Also known as PVSTP.
Rapid STP (RSTP)	A Spanning Tree mode that speeds topology changes by actively confirming that a port can safely transition to the forwarding state immediately.
Rapid PVST+	A Spanning Tree mode enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w for each VLAN.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.3 Configure spanning tree • View STP configuration information • Manually configure a switch as a root bridge • Configure Rapid PVST+
Cisco CCNA 200-301	2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations • 2.5.a Root port, root bridge (primary/secondary), and other port names

- 2.5.b Port states (forwarding/blocking)
- 2.5.c PortFast benefits

Video/Demo	Time
11.4.1 STP Design and Implementation	8:34
11.4.2 Set Up STP	5:25
11.4.3 Select a Root Bridge	4:28
11.4.8 STP Troubleshooting	5:01
Total Video Time	**23:28**

Lab/Activity

- 11.4.5 Configure the Root Bridge
- 11.4.6 Configure the Primary and Secondary Root Bridges
- 11.4.7 Configure Rapid PVST+
- 11.4.10 Find STP Information 1
- 11.4.11 Find STP Information 2

Fact Sheets

- 11.4.4 STP Design and Implementation Facts
- 11.4.9 STP Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 104 minutes

11.5: Router-on-a-Stick InterVLAN Routing

Lecture Focus Questions:

- A device must function at which layer in order to provide interVLAN routing?
- Why doesn't trunking enable interVLAN communication?
- Which method allows a single router to perform interVLAN routing using a single physical interface?
- Which function includes the concept of route once, switch many?
- What are the requirements for interVLAN routing?
- What is upstream routing?
- What is a subinterface? What is its role in an interVLAN configuration?
- How do you configure an interface as a trunk? Which commands are used?
- What information does the show run command display?

In this section, you will learn to:

- Configure InterVLAN routing

Key terms for this section include the following:

Term	Definition
Router-on-a-stick	A network configuration that allows traffic to be routed between different VLANs.
Subinterface	A virtual interface created by dividing a router's physical interface into multiple logical interfaces.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.2 Configure interVLAN routing • Configure interVLAN routing

Video/Demo	Time
11.5.1 Routing Between VLANs	5:14
11.5.2 Router-on-a-Stick InterVLAN Routing	7:20
11.5.4 Set Up Router-on-a-Stick InterVLAN Routing	4:28
11.5.7 Troubleshoot InterVLAN Routing	8:21
Total Video Time	**25:23**

Lab/Activity

- 11.5.6 Configure InterVLAN Routing

Fact Sheets

- 11.5.3 InterVLAN Routing Facts
- 11.5.5 InterVLAN Routing Configuration Facts
- 11.5.8 InterVLAN Routing Troubleshooting Facts

Number of Exam Questions
10 questions

Total Time
About 63 minutes

11.6: Switch InterVLAN Routing

Lecture Focus Questions:

- What is the function of the no switchport command?
- What is the most common implementation of Switch Virtual Interface (SVI)?
- Which command enables a switch to be managed from a remote network?
- Which command would you use to display the port types?
- What information does the show interface command provide?
- What is a trunk port?
- How do you create a trunk?

In this section, you will learn to:

- Configure SVI for InterVLAN routing
- Troubleshoot interVLAN routing

Key terms for this section include the following:

Term	Definition
Switch Virtual Interface	A virtual interface that transmits only untagged VLAN packets for a managed switch.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.2 Configure interVLAN routing • Configure interVLAN routing • Troubleshoot interVLAN routing issues

Video/Demo	Time
11.6.1 Switch InterVLAN Routing	6:43
11.6.2 Set Up Layer 3 Switch InterVLAN Routing	4:18
Total Video Time	**11:01**

Lab/Activity

- 11.6.4 Configure SVI for InterVLAN Routing 1
- 11.6.5 Configure SVI for InterVLAN Routing 2
- 11.6.7 Troubleshoot InterVLAN Routing 1
- 11.6.8 Troubleshoot InterVLAN Routing 2

Fact Sheets

- 11.6.3 Layer 3 Switch InterVLAN Routing Facts
- 11.6.6 SVI InterVLAN Troubleshooting Facts

Number of Exam Questions
10 questions

Total Time
About 80 minutes

11.7: Switch Troubleshooting

Lecture Focus Questions:

- What should you look for if the line status is up and the protocol status is down?
- How can you view a single line of information about each IP interface?
- What types of problems are the result of collisions?
- What are late collisions? What is a probable cause?
- What steps do you take to verify connectivity at the Physical layer?
- How do you verify that trunking is enabled correctly on a switch?

In this section, you will learn to:

- Find virtual LAN (VLAN) information
- Troubleshoot VLANs

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	4.1 Configure switch VLANs • View information about VLANs configured on a switch • Troubleshoot VLAN issues
Cisco CCNA 200-301	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

Video/Demo	Time
11.7.1 Troubleshoot Switches	9:05
Total Video Time	**9:05**

Lab/Activity

- 11.7.4 Find VLAN Information
- 11.7.5 Troubleshoot VLANs 1
- 11.7.6 Troubleshoot VLANs 2

Fact Sheets

- 11.7.2 Interface Status Troubleshooting Facts
- 11.7.3 VLAN and Trunking Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 66 minutes

12.1: Access Control Lists (ACLs)

Lecture Focus Questions:

- You want to create an access control list (ACL) that restricts traffic from host 12.0.15.166. What type of access list can you use?
- How many access lists can be applied to a single interface?
- When can you have two access lists for the same direction applied to an interface?
- Where in the access list should you place the most restrictive statements?
- When viewing an access list statement, how can you determine if the list is a standard ACL?
- After creating an ACL list and the list entries, what is the next step in configuring an ACL?
- How are access list statements associated with an access list?
- What happens when you delete an access list statement?
- Why is it an advantage to use a text editor to build and evaluate ACLs before implementing them?
- What type of information does the show log command display?
- How can you view log messages to identify the line in an ACL that is being matched?
- What happens to a packet that does not match any line in an ACL? Why?

In this section, you will learn to:

- Restrict Telnet and SSH access
- Permit traffic
- Block source hosts

The key terms for this section include:

Term	Definition
Access control lists	A list used to deny or permit incoming or outgoing traffic.
Inverse wildcard mask	An inverse wildcard mask in an inverted subnet mask. It indicates which parts of an IP address are available for examination in access control lists.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.1 Configure router security • Restrict router remote access 6.3 Configure access control list • Use ACLs to permit allowed network traffic

	• Use ACLs to block disallowed network traffic
Cisco CCNA 200-301	5.6 Configure and verify access control lists

Video/Demo	Time
12.1.1 ACL Overview	6:53
12.1.2 Set Up ACLs	5:23
12.1.3 Standard ACLs	6:47
12.1.4 Set Up Standard ACLs	8:52
12.1.5 Named ACLs	4:18
12.1.7 Filter Inbound Remote Access	2:38
12.1.12 Troubleshoot ACLs	6:36
Total Video Time	**41:27**

Lab/Activity

- 12.1.8 Restrict Telnet and SSH Access
- 12.1.9 Permit Traffic
- 12.1.10 Block Source Hosts

Fact Sheets

- 12.1.6 Access List Facts
- 12.1.11 Access List Configuration Facts
- 12.1.13 ACL Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 103 minutes

12.2: IPv6 and Extended ACLs

Lecture Focus Questions:

- How does a standard access control list (ACL) differ from an extended ACL?
- Which command is used to add an access list to an interface?
- What are the key differences between IPv4 and IPv6 ACLs?
- What are the two types of IPv6 access lists?
- How is the inverse wildcard mask value calculated?
- What is the purpose of an inverse wildcard mask?
- What does a 0 in a wildcard mask indicate? How are bits identified with a 1 handled?
- How do you calculate the wildcard mask?
- You want to create an access list that restricts ICMP traffic. Which type of access list should you use?

In this section, you will learn to:

- Configure allowed networks
- Create access list statements
- Block invalid addresses
- Allow only specific services

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.3 Configure access control list • Implement standard, extended, and named ACLs • Use wildcard masks in ACLs • Use ACLs to permit allowed network traffic • Use ACLs to block disallowed network traffic • Block disallowed traffic
Cisco CCNA 200-301	5.6 Configure and verify access control lists

Video/Demo	Time
12.2.1 Extended ACLs	5:43
12.2.4 Use APIC-EM Path Trace to Verify ACLs	6:47
12.2.5 ACL Command Format	8:37
12.2.6 Inverse Wildcard Masking	11:32
12.2.8 Set Up Extended ACLs	5:14
Total Video Time	**37:53**

Lab/Activity

- 12.2.10 Configure Allowed Networks
- 12.2.11 Create Access List Statements
- 12.2.12 Block Invalid Addresses
- 12.2.13 Allow Only Specific Services

Fact Sheets

- 12.2.2 Extended ACL Facts
- 12.2.3 IPv6 ACL Facts
- 12.2.7 Wildcard Mask Facts
- 12.2.9 Extended Access List Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 116 minutes

13.1: Network Time Protocol (NTP)

Lecture Focus Questions:

- How does NTP handle time drift?
- What type of devices are authoritative time sources?
- How does slam differ from slew in correcting time?
- How is the concept of stratum implemented by NTP?

Key terms for this section include the following:

Term	Definition
NTP	A protocol that uses UDP packets to send time data to connected devices to keep time synced across a network.
Stratum Level	Hierarchical representation of the time servers in an NTP network. Stratum level 0 is the authoritative time source and Stratum level 1 is the server connected directly to the time source. Each subsequent server increases the stratum level.
Time Drift	An event that makes a system's clock no longer accurate and off by a few seconds or minutes.
Slew	A method for correcting time drift by incrementally correcting the time a few milliseconds at a time.
Slam	A method for correcting time drift by immediately resetting the time.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.2 Configure and verify NTP operating in a client and server mode

Video/Demo	Time
13.1.1 NTP Overview	4:44
Total Video Time	**4:44**

Fact Sheets

13.1.2 NTP Facts

Number of Exam Questions

10 questions

Total Time

About 20 minutes

13.2: System Message Log

Lecture Focus Questions:

- What is the function of syslog messages?
- What is the format of log messages?
- When is a log server appropriate to use?
- What are the syslog message severity levels?

In this section, you will learn to:

- Configure centralized logging with Cisco devices.

Key terms for this section include the following:

Term	Definition
syslog	A system message log that is generated for every event that occurs on a Cisco device.
Facility	A device, protocol, or system software module that generates log message.
Mnemonic	A text string that quickly identifies the nature of the message.
History table	A storage area of syslog files on a Cisco device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.5 Describe the use of syslog features including facilities and levels

Video/Demo	Time
13.2.1 Syslog Overview	4:35
13.2.2 Configure Centralized Logging with Cisco Devices	1:58
Total Video Time	**6:33**

Fact Sheets

13.2.3 Syslog Facts

Number of Exam Questions

10 questions

Total Time

About 22 minutes

13.3: Simple Network Management Protocol

Lecture Focus Questions:

- What is Simple Network Messaging Protocol (SNMP)?
- What roles do SNMP Managers and SNMP agents play?
- How does SNMP use the management information base (MIB)?
- How is SNMPv3 different from prior SNMP versions?

In this section, you will learn to:

- Enable SNMP on Cisco devices.

Key terms for this section include the following:

Term	Definition
Simple Network Messaging Protocol	An application-layer protocol that helps in monitoring network devices.
Community string	Unencrypted cleartext default password used in SNMP version 1 and 2.
Network Management System	Software installed on the SNMP Manager that uses SNMP to monitor and manage network devices.
SNMP Manager	Responsible for polling or querying network devices and using the data from responses to manage uptime and diagnose the devices.
SNMP agent	The software that resides on each managed device that collects data and information on the local device. The agent is responsible for communicating and responding to the SNMP Manager.
Management information base	The set of parameters that defines what the SNMP Manager and agent will monitor and get data for on each device.
Object ID (OID)	Unique identifier that the MIB uses to describe specific characteristics of each network object.
Polling	SNMP communication method where the SNMP Manager queries the agent requesting specific information. These communications occur over port 161.
Trap	SNMP communication method where the agent is configured to send alerts based on defined parameters. These communications occur over port 162.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.4 Explain the function of SNMP in network operations

Video/Demo	Time
13.3.1 SNMP Overview	5:37
13.3.2 Enable SNMP on Cisco Devices	12:22
Total Video Time	**17:59**

Fact Sheets

13.3.3 SNMP Facts

Number of Exam Questions

10 questions

Total Time

About 33 minutes

13.4: NetFlow

Lecture Focus Questions:

- What is a network flow?
- What fields in an IP header identify a network flow?
- What two components makeup NetFlow?
- What are the benefits of NetFlow?
- How do you configure NetFlow on a Cisco router?

In this section, you will learn to:

- Enable NetFlow on Cisco devices

Key terms for this section include the following:

Term	Definition
Flow	A unidirectional stream of IP packets from a source to destination host.
NetFlow cache	Memory storage area where NetFlow data is stored on the device.
NetFlow export mechanism	NetFlow component, also referred to as a transport mechanism, that sends data to a network management collector.
Network management collector	Application used to monitor a network using the data collected by NetFlow.

Video/Demo	Time
13.4.1 NetFlow Overview	4:16
13.4.2 Enable NetFlow on Cisco Devices	1:27
Total Video Time	**5:43**

Fact Sheets

13.4.3 NetFlow Facts

Number of Exam Questions

10 questions

Total Time

About 21 minutes

13.5: Quality of Service (QoS)

Lecture Focus Questions:

- What service does Quality of Service (QoS) provide?
- What are the four metrics used by QoS?
- What are the three models used by QoS?
- What does Network Based Application revision 2 (NBAR2) do?
- What is the difference between policing and shaping?

Key terms for this section include the following:

Term	Definition
Quality of Service	A set of mechanisms that try to guarantee timely delivery of important or time-sensitive communications.
Best effort QoS model	Also known as first in first out (FIFO). Network packets are processed in the same order they are received. This model does not implement any QoS tools or methods.
Bandwidth	Speed of a network. Typically is measured in bits per second.
Delay	Also known as latency. The time it takes a packet to get from the source to its destination is known as one-way delay. Round-trip delay is the amount of time it takes for the packet to be sent, received, sent back and acknowledged by the original sender.
Jitter	The variation in packet arrival rate. This metric has a substantial impact on VOIP traffic.
Packet loss	The percentage of packets that don't make it to the destination.
Integrated services	Services that provide the highest guarantee of QoS. Each application requests network resources. The request will be approved or denied based on available resources.
Differentiated services	A model that prioritizes traffic based on the classification of the network traffic type. Higher priority traffic is processed first.
Classification and marking	A QoS method that identifies the type of network traffic and then alters the packet header to mark the different types of traffic.
Network Based Application (NBAR)/ NBAR2	A Cisco service that can identify protocols and application level traffic in order to route packets more effectively.
Queuing or scheduling	A QoS method that buffers or queues network traffic and processes based on priority. The scheduler is the component that sets the priority levels.
Policing	A QoS tool that drops excess traffic when it exceeds the network speed threshold.
Shaping	A QoS tool that queues data and uses buffers to store the packets until the packets can be sent.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping

Video/Demo	Time
13.5.1 QoS Overview	8:12
Total Video Time	**8:12**

Fact Sheets

13.5.2 QoS Facts

Number of Exam Questions

10 questions

Total Time

About 24 minutes

13.6: Enterprise Networking

Lecture Focus Questions:

- What is the goal of software-defined networking(SDN)?
- What are the three network device planes?
- What is the purpose of a controller in a software-defined networking?
- What communicates through the southbound interface?
- What communicates through the northbound interface?
- What are the three ways to implement an SDN?
- What are three important network documents?
- What is the bottom-up troubleshooting method?

In this section, you will learn to:

- Troubleshoot command lists

Key terms for this section include the following:

Term	Definition
Software-defined networking	Allows the system administrator to control configuration of network devices at the edge of the network using open protocols, such as OpenFlow. This makes vitalizing networks simpler and easier to manage.
Network device planes	All network devices have three planes, or areas, that each carry a type of communication. The three planes on a network device are: • Control Plane. This plane gathers and maintains information needed to make forwarding decisions. Basically, all network information, such as MAC addresses, routing tables, ARP tables, and more, are stored on this plane. • Data Plane. This plane is also referred to as the forwarding plane. This plane connects the network ports on a device and is used to forward traffic flows. Routers and switches use the information from the control plane to forward incoming traffic out the appropriate egress interface. • Management Plane - This plane is responsible for accessing and managing a device through the network so it can be configured. This can include using methods such as SSH, Telnet, or HTTPS.
Application programming interface (API)	A custom protocol or language that allows different types of software or technology to talk with each other.
Network architecture	The way a network is designed and setup physically and logistically.

Physical device diagram	Shows the physical location of every network device. This diagram shows each device, its connections, and how it is physically connected to other devices.
Logical device diagram	Shows how network data flows across the network components such as subnets and VLANs.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	6.2 Compare traditional networks with controller-based networking 6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric) • 6.3.a Separation of control plane and data plane • 6.3.b North-bound and south-bound APIs

Video/Demo	Time
13.6.1 Enterprise Networking Overview	5:30
13.6.3 Troubleshooting Models	5:56
13.6.4 Troubleshoot Command List	5:10
Total Video Time	**16:36**

Fact Sheets

- 13.6.2 Enterprise Networking Facts
- 13.6.5 LAN Switch Troubleshooting Facts

Number of Exam Questions

10 questions

Total Time

About 37 minutes

13.7: Cloud Resources

Lecture Focus Questions:

- What is the cloud?
- What resources can be used in the cloud?
- What are the five characteristics of a cloud service?
- Explain the difference between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- What are the different methods of cloud deployment?

Key terms for this section include the following:

Term	Definition
Cloud	Computing resources that are offered or delivered as a service over a network.
Hypervisor	Special software that creates and runs virtual machines.
Infrastructure as a Service	A cloud service model where servers, network hardware, storage, and more are provided through the cloud.
Platform as a Service	A cloud service that provides a development platform where application developers can deploy code without the developer having to install and configure the operating system, platform, and associated service.
Software as a Service	A cloud service model where applications are provided through the cloud.
Public cloud	A cloud service deployment that is open to the public. This service can be free or fee based.
Private cloud	A cloud service deployment that consists of an infrastructure designed and operated solely for a single organization.
Community cloud	A cloud service deployment that consists of several organizations sharing infrastructure that they all have in common, such as an application or regulatory requirements.
Hybrid cloud	A cloud service deployment that is a combination of private, community, or public clouds that offers different aspects of services.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	1.2 Describe characteristics of network topology architectures • 1.2.f On-premises and cloud 1.12 Explain virtualization fundamentals (virtual machines)

Video/Demo	Time
13.7.1 Cloud Resources Overview	6:40

Total Video Time **6:40**

Fact Sheets

- 13.7.2 Cloud Resources Facts
- 13.7.3 Cloud Services Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

13.8: Virtual Private Networks and Remote Switch Access

Lecture Focus Questions:

- What is a virtual private network (VPN)?
- How does a VPN work?
- What are common VPN protocols?
- What are the VPN auto-triggers?
- How is Always On different from a VPN?

In this section, you will learn to:

- Set up secure remote access

Key terms for this section include the following:

Term	Definition
Virtual private network	Provides a secure connection to remote resources over the internet. Often referred to as tunneling.
Wide area network (WAN)	A network spread over a large distance that consists of multiple local area networks (LANs).
VPN trigger	A rule that, when configured and a specified condition is met, automatically enables the VPN connection.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	4.8 Configure network devices for remote access using SSH 5.5 Describe remote access and site-to-site VPNs

Video/Demo	Time
13.8.1 Virtual Private Networks	4:43
13.8.4 Set Up Secure Remote Access	3:48
Total Video Time	**8:31**

Fact Sheets

- 13.8.2 Virtual Private Networks Facts
- 13.8.3 IPsec Virtual Private Networks Facts

Number of Exam Questions

10 questions

Total Time

About 29 minutes

13.9: Default Gateway Redundancy

Lecture Focus Questions:

- What problem does First Hop Redundancy Protocol (FHRP) help with?
- What are the two main FHRP options?
- How does Hot Standby Router Protocol (HSRP) work?
- By default, what identifies the default active HSRP router?
- How does Gateway Load Balancing Protocol (GLBP) work?

In this section, you will learn to:

- Configure HSRP

Key terms for this section include the following:

Term	Definition
Gateway	Router that forwards internal traffic to external resources.
First Hop Redundancy Protocols	Set of protocols that automate the switching of a secondary router to become the default gateway.
Hot Standby Router Protocol	A Cisco proprietary FHRP that sets one router as an active router and other routers in the group as standby routers.
Gateway Load Balancing Protocol	FHRP that balances network load equally between multiple redundant routers.
Active Virtual Gateway (AVG)	Router in GLBP that is responsible for replying to ARP requests and balancing traffic between all routers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	3.5 Describe the purpose of first hop redundancy protocol 6.1 Explain how automation impacts network management

Video/Demo	Time
13.9.1 Default Gateway Router Redundancy	5:11
13.9.3 Set Up HSRP	6:28
Total Video Time	**11:39**

Lab/Activity

- 13.9.5 Configure HSRP

Fact Sheets

- 13.9.2 Redundant Default Gateway Facts
- 13.9.4 HSRP Configuration Facts

Number of Exam Questions

10 questions

Total Time
About 44 minutes

13.10: Network Automation

Lecture Focus Questions:

- How can automation help a network?
- What is automation? What is orchestration?
- What are the common data formats?
- How does an application programming interface (API) work?

Key terms for this section include the following:

Term	Definition
Automation	When a task or process is performed with minimal human intervention.
Orchestration	The arranging of tasks that results in a coordinated process or workflow.
Data format	A structured way to organize data so that it can be stored or exchanged.
Application programming interface	Software that allows other applications to access data or services. It implements a set of rules that describe how an application can interact.
REST API	API that works on top of the HTTP protocol. The REST API defines a set of functions developers can use to perform requests and receive responses using these GET and POST HTTP commands.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	6.1 Explain how automation impacts network management 6.2 Compare traditional networks with controller-based networking 6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric) • 6.3.a Separation of control plane and data plane • 6.3.b North-bound and south-bound APIs 6.4 Compare traditional campus device management with Cisco DNA Center enabled device 6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding) 6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible 6.7 Interpret JSON encoded data

Video/Demo	Time
13.10.1 Network Automation Overview	4:52

Total Video Time **4:52**

Fact Sheets

- 13.10.2 Network Automation Facts
- 13.10.3 REST API Facts
- 13.10.4 Cisco DNA Center Facts

Number of Exam Questions

10 questions

Total Time

About 30 minutes

14.1: Network Threats

Lecture Focus Questions:

- What are the three components of AAA?
- What are the differences between the TACACS+ and RADIUS protocols?
- If an AAA server goes down, how can you maintain management connectivity?
- What are the different categories of hackers?
- What are common motivations for a hacker?
- What separates a hacker from a script kiddie?
- Do today's hackers need as much technical knowledge as previous hackers?
- How does a passive attack differ from an active attack?
- How does educating and training users maintain a secure network environment?
- Which areas of your network should you focus on to best understand it?
- How does segmenting your network increase network security?

Key terms for this section include the following:

Term	Definition
Authentication	The act of identifying a network user.
Authorization	The act of permitting or denying network resources.
Accounting	The process of documenting user actions and collecting user data.
RADIUS	An AAA server used by Microsoft servers.
TACACS+	An AAA server developed by Cisco.
Threat actor	A person or organization that poses a threat to an organization's security.
Advanced persistent threat (APT)	A stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period.
Threat modeling	The process of analyzing the security of the organization and determine security holes.
White hat	A skilled hacker who uses skills and knowledge for defensive purposes only. The white hat hacker interacts only with systems for which express access permission has been given.
Black hat	A skilled hacker who uses skills and knowledge for illegal or malicious purposes.
Gray hat	A skilled hacker who falls in the middle of the white hat and black hat hackers. The gray hat may cross the line of what is ethical, but usually has good intentions and isn’t malicious like a black hat hacker.
Suicide hacker	A hacker who is concerned only with taking down the target for a cause.

Cyber terrorist	A hacker motivated by religious or political beliefs who wants to create severe disruption or widespread fear.
State-sponsored hacker	A hacker who works for a government and attempts to gain top-secret information by hacking other governments.
Hacktivist	A hacker whose main purpose is to protest an event or situation and draw attention to their own views and opinions.
Script kiddie	An extremely unskilled person who uses tools and scripts developed by real hackers.
Active attack	An attack where perpetrators attempt to compromise or affect the operations of a system in some way.
Passive attack	An attack where perpetrators attempt to gather information without affecting the flow of that information from the targeted network.
External attack	An attack where unauthorized individuals try to breach a network from off-site.
Inside attack	An attack initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized.
Entry point	A location or device that is vulnerable to attacks.
Network baseline	The normal network activity including typical traffic patterns, data usage, and server loads that is used to identify unusual or atypical activity, which can indicate an attack.
Network segmentation	Dividing a network into segments for performance or security reasons.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS) 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.8 Differentiate authentication, authorization, and accounting concepts

Video/Demo	Time
14.1.1 Network Security Using AAA	5:09
14.1.3 Threat Actor Types	6:36
14.1.5 Network Threats Overview	8:34
Total Video Time	**20:19**

Fact Sheets

- 14.1.2 AAA Security Facts
- 14.1.4 Threat Actor Type Facts
- 14.1.6 Network Threats Facts

Number of Exam Questions
10 questions

Total Time
About 46 minutes

14.2: Network Security Best Practices

Lecture Focus Questions:

- How can you secure physical access to computer systems?
- What configuration changes could you make to prevent data loss on a Windows system?
- What are the characteristics of a strong password?
- How can you limit wired network connectivity to only authorized systems?
- How can you make it more difficult for an unauthorized person to connect to a wired network?
- Which network devices should be put in a DMZ? Which systems should not?
- What is the role of a content filter?
- What can you do to obscure a wireless network?
- How can you prevent data emanation from a wireless network?

In this section, you will learn to:

- Change the default password on a switch.

Key terms for this section include the following:

Term	Definition
Demilitarized Zone (DMZ)	A physical or logical subnet that separates an internal local area network from untrusted networks.
Biometric authentication	A type of authentication that relies on the unique physical characteristics of individuals to verify their identity for secure access.
Multifactor authentication	A type of authentication that requires multiple authentication credentials to verify the user's identity for a login or other transaction.
MAC address filtering	A feature that restricts access to the wired network switch to hosts that have specific MAC addresses.
Wi-Fi Protected Setup (WPS)	A network security standard that makes wireless networks easier to manage.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.2 Configure switch security • Configure switch passwords
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

	5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

Video/Demo	Time
14.2.1 Wired Network Security Best Practices	9:55
14.2.3 Wireless Network Security Best Practices	9:51
14.2.5 Search defaultpassword.com	2:19
14.2.6 Change Default Passwords	2:57
Total Video Time	**25:02**

Lab/Activity

- 14.2.7 Change the Default Password on a Switch

Fact Sheets

- 14.2.2 Wired Network Security Facts
- 14.2.4 Wireless Network Security Facts

Number of Exam Questions

10 questions

Total Time

About 58 minutes

14.3: Switch Security

Lecture Focus Questions:

- How does a switch identify devices that are in different VLANs?
- What is the function of a trunk port?
- When trunking is used, how is the receiving switch able to identify which VLAN the frame belongs to?
- What is required for devices to communicate between VLANs?
- How is port security different from port filtering?

In this section, you will learn to:

- Configure port security.
- Harden a switch.
- Secure access to a switch.
- Configure DHCP snooping.
- Configure dynamic ARP inspection.

Key terms for this section include the following:

Term	Definition
MAC flooding	An attack that overloads the switch's MAC forwarding table to make the switch function like a hub.
ARP spoofing/ ARP poisoning	An attack that associates the attacker's MAC address with the IP address of victim devices.
VLAN hopping	An attack that occurs when an attacking host on a VLAN attempts to gain access to traffic on other VLANs that normally it would not have access to.
Switch spoofing	An attack where the attacker uses special software to manipulate VLAN tagging and trunking to make it appear that the attacker's computer is a trunking switch.
Double tagging	An attack on switches that adds two VLAN tags instead of one to the header of the frames that it transmits.
MAC spoofing	An attack that changes the source MAC address on frames sent by the attacker.
Dynamic Trunking Protocol (DTP)	DTP allows switches to automatically detect trunk ports and negotiate the trunking protocol used between devices. DTP is not secure and allows unauthorized devices to modify configuration information. You should disable the DTP services on the switch's end user (access) ports before implementing the switch configuration into the network.
MAC filtering	A switch feature that restricts which devices can connect to a given port based on its MAC address.

Port authentication	A switch feature that follows the 802.1x protocol to allow only authenticated devices to connect to the LAN through the switch.
Content-Addressable Memory (CAM) table/ MAC table	A table maintained by a switch that contains MAC addresses and their corresponding port locations.
SecureConfigured	A MAC address that has been manually identified as an allowed address.
SecureDynamic	A MAC address that has been dynamically learned and allowed by the switch.
SecureSticky	A MAC address that is manually configured or dynamically learned and saved.
DHCP Snooping	A security feature on some switches that filters out untrusted DHCP messages.
Dynamic ARP Inspection (DAI)	A security feature on some switches that inspects and verifies each ARP request to ensure a valid IP to MAC binding.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.2 Configure switch security • Secure switch access • Enable switch port security • Restrict switch remote access 6.4 Implement security measures • Implement device hardening
Cisco CCNA 200-301	2.1 Configure and verify VLANs (normal range) spanning multiple switches • 2.1.a Access ports (data and voice) • 2.1.c Connectivity 2.2 Configure and verify interswitch connectivity • 2.2.a Trunk ports • 2.2.c Native VLAN 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

Video/Demo	Time
14.3.1 Switch Attacks	5:25
14.3.3 Secure Network Switches	5:01
14.3.5 Set Up DHCP Snooping and Dynamic ARP Inspection	1:45
14.3.7 Set Up Port Security	4:23
14.3.13 Configure Switch Hardening	9:51
Total Video Time	**26:25**

Lab/Activity

- 14.3.6 Configure DHCP Snooping and Dynamic ARP Inspection
- 14.3.10 Configure Port Security 1
- 14.3.11 Configure Port Security 2
- 14.3.12 Configure Port Security 3
- 14.3.14 Harden a Switch
- 14.3.15 Secure Access to a Switch
- 14.3.16 Secure Access to a Switch 2

Fact Sheets

- 14.3.2 Switch Attack Facts
- 14.3.4 Switch Security Facts
- 14.3.8 Port Security Facts
- 14.3.9 Port Security Configuration Facts

Number of Exam Questions

10 questions

Total Time

About 141 minutes

14.4: Malware

Lecture Focus Questions:

- What are the different types of malware?
- Which component of malware actually causes damage?
- What is the purpose of a Trojan horse?
- What are some ways malware can infect a system?
- What is the best way to analyze malware?

Key terms for this section include the following:

Term	Definition
Malware	Any software that is designed to perform malicious and disruptive actions.
The Computer Fraud and Abuse Act	This law was originally passed to address federal computer-related offenses and the cracking of computer systems.
The Patriot Act	This act expanded the powers already included in the Computer Fraud and Abuse Act.
CAN-SPAM Act	This law was designed to thwart the spread of spam.
Crypter	Software that protects the malware code from being analyzed and reverse engineered. It also helps prevent detection from anti-virus software.
Exploit	The act of taking advantage of a bug or vulnerability to execute malware.
Injector	A program that injects malware into vulnerable running processes.
Obfuscator	The a tool designed to conceal malware through various techniques.
Packer	The a tool designed to compress malware to help hide it.
Payload	The destructive component of malware. The payload is the part that performs the malware's intended activity.
Malicious code	Code that defines the malware's basic functionality, such as deleting data or opening backdoors into the target.
Sheep dipping	The process of analyzing emails, suspect files, and systems for malware.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
14.4.1 Malware Overview	9:41
14.4.3 Trojans and Backdoors	5:37
14.4.5 Malware Concerns	3:52
14.4.7 Malware Analysis	4:26
Total Video Time	**23:36**

Fact Sheets

- 14.4.2 Malware Overview Facts
- 14.4.4 Trojan and Backdoor Facts
- 14.4.6 Malware Concern Facts
- 14.4.8 Malware Analysis Facts

Number of Exam Questions

10 questions

Total Time

About 54 minutes

14.5: Combat Malware

Lecture Focus Questions:

- What are the best methods for detecting malware?
- What steps should you take when penetration testing for malware?
- What actions should be taken when malware is discovered?

In this section, you will learn to:

- Detect open ports with nmap
- View open ports with netstat
- Scan for open ports from a remote computer
- Counter malware with Windows Defender

Key terms for this section include the following:

Term	Definition
Heuristic algorithm	Heuristic algorithms generate fairly accurate results in a short amount of time by focusing on speed, instead of accuracy and completeness.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Implement anti-malware measures • Scan and detect open ports
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
14.5.1 Anti-Malware Software	5:05
14.5.2 Scan for Open Ports with Netstat	3:11
14.5.3 Track Port Usage with TCPView	2:32
Total Video Time	**10:48**

Lab/Activity

- 14.5.5 Detect Open Ports with Nmap
- 14.5.6 View Open Ports with netstat
- 14.5.7 Scan for Open Ports from a Remote Computer
- 14.5.8 Counter Malware with Windows Defender

Fact Sheets

- 14.5.4 Anti-Malware Software Facts

Number of Exam Questions

10 questions

Total Time

About 74 minutes

14.6: Sniffing

Lecture Focus Questions:

- What is network sniffing?
- Which tools can be used for network sniffing?
- How can sniffing methods be used to exploit switched networks?
- What are some countermeasures to network sniffing?

In this section, you will learn to:

- Spoof MAC addresses with SMAC
- Filter and analyze traffic with Wireshark

Key terms for this section include the following:

Term	Definition
Sniffing	Sniffing is the process of collecting information as it crosses the network.
Promiscuous mode	Promiscuous mode gives the network interface permission to grab every frame that comes its way, even if it's addressed to someone else.
MAC spoofing	MAC spoofing is the process of changing the MAC address of the interface driver in an attempt to impersonate another host on the network.
MAC flooding	MAC flooding is the process of overloading a switch's CAM table in hopes that it will respond by broadcasting all traffic across the network.
ARP poisoning	ARP poisoning is the process of sending spoofed messages onto a network in an attempt to associate your MAC address with the IP address of another host so the target machine will send frames to your system.
Port mirroring	Port mirroring creates a duplicate of all network traffic on a port and sends it to another device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Implement device hardening • Analyze network traffic using Wireshark
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

	5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
14.6.1 Sniffing	6:39
14.6.3 Sniff Network Traffic with Wireshark	6:49
14.6.4 Capture Traffic with TCPDump	5:41
14.6.5 Use SMAC to Spoof MAC Addresses	3:46
14.6.8 Sniffing Countermeasures and Detection	2:55
14.6.9 Detect Promiscuous Mode	3:17
Total Video Time	**29:07**

Lab/Activity

- 14.6.6 Spoof MAC Addresses with SMAC
- 14.6.7 Filter and Analyze Traffic with Wireshark

Fact Sheets

- 14.6.2 Sniffer Facts
- 14.6.10 Sniffing Countermeasure and Detection Facts

Number of Exam Questions

10 questions

Total Time

About 74 minutes

14.7: Session Hijacking

Lecture Focus Questions:

- What is session hijacking? How can it be used to gather sensitive information?
- What are some methods that can be used for session hijacking at the application and network layers?
- What actions can be taken to prevent session hijacking?

In this section, you will learn to:

- Capture HTTP POST Packets with Wireshark
- Hijack a web session

Key terms for this section include the following:

Term	Definition
Session hijacking	The process of taking over an established connection between a host and a web server. The session token can be stolen or a predicted session token can be used.
Session ID	A combination of numbers and letters assigned to an open connection between a user and a server.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
14.7.1 Session Hijacking Overview	2:37
14.7.3 Client-Side and Network Attacks	8:03
14.7.5 Configure a Man-in-the-Middle DHCP Attack	6:56
14.7.7 Hijack a Web Session	3:34
14.7.9 Session Hijacking Countermeasures	3:54
Total Video Time	**25:04**

Lab/Activity

- 14.7.6 Capture HTTP POST Packets with Wireshark
- 14.7.8 Hijack a Web Session

Fact Sheets

- 14.7.2 Session Hijacking Facts
- 14.7.4 Client-Side and Network Attack Facts
- 14.7.10 Session Hijacking Countermeasure Facts

Number of Exam Questions

10 questions

Total Time

About 75 minutes

14.8: Denial of Service

Lecture Focus Questions:

- What is the difference between a denial-of-service attack and a distributed denial-of-service attack?
- What are the four categories of denial-of-service attacks?
- What types of devices can be used in a denial-of-service attack?
- What measures can be taken to protect your network or devices from a denial-of-service or distributed denial-of-service attack?

In this section, you will learn to:

- Analyze ICMP traffic in Wireshark
- Analyze a DDoS attack

Key terms for this section include the following:

Term	Definition
Denial-of-service attack	A denial-of-service attack occurs when a computer is used to flood a server with more packets than it can handle.
Distributed denial-of-service attack	Distributed denial-of-service attacks use numerous computers and internet connections across the globe to overload target systems.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Analyze network traffic using Wireshark • Analyze network traffic for potential security risks
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
14.8.1 Denial of Service (DoS) Overview	6:44
14.8.3 DoS Attack Types	5:13
14.8.5 Perform a SYN Flood	6:20
14.8.7 Launch a DoS and DDoS Attack	5:44
14.8.9 DoS Countermeasures	3:43

Total Video Time **27:44**

Lab/Activity

- 14.8.6 Analyze ICMP Traffic in Wireshark
- 14.8.8 Analyze a DDoS Attack

Fact Sheets

- 14.8.2 Denial of Service (DoS) Facts
- 14.8.4 DoS Attack Type Facts
- 14.8.10 DoS Countermeasure Facts

Number of Exam Questions

10 questions

Total Time

About 77 minutes

15.1: Cryptography

Lecture Focus Questions:

- What is the difference between a transposition cipher and a substitution cipher?
- A user needs to communicate securely with five other users using symmetric key encryption. How many keys are required?
- How are symmetric keys typically exchanged between communication partners?
- What is an advantage of increasing the number of bits in the key? What is a disadvantage?
- How do public keys differ from private keys? What is the relationship between the two?
- For which type of environment is asymmetric cryptography best suited?
- Why does asymmetric encryption require fewer keys than symmetric encryption?
- What is public key infrastructure (PKI)?
- Where is PKI used?
- What are the key components of PKI?

In this section, you will learn to:

- Compare an MD5 hash

Key terms for this section include the following:

Term	Definition
Cryptography	The science and study of concealing information that is used in electronic communication to protect the privacy of passwords, secret keys, and data.
Cipher/Algorithm	A process or formula used to convert or otherwise hide the meaning of a message.
Key	A variable in a cipher that is used to encrypt or decrypt a message.
Plain text	The readable form of a communication that is visible to everyone.
Ciphertext	An encrypted form of a communication that makes the communication unreadable to all but those who have the decryption cipher or key.
Encryption	The process of using an algorithm or cipher to transform data from clear text to ciphertext. The intent is to protect the confidentiality, integrity, and authenticity of the message.
Decryption	The process of converting data from ciphertext into plain text so that it can be read.
Steganography	The process of hiding data or a message so that only the sender and the recipient suspect that the hidden data exists.

Cryptanalysis	The method that is used to recover data that has been encrypted without having access to the key used in the encryption process.
Symmetric encryption	A form of cryptography that provides confidentiality with a weak form of authentication or integrity.
Block cipher	Symmetric encryption that transposes plain text to ciphertext in chunks (block by block).
Stream cipher	A symmetric encryption that is performed on each bit within a stream of data in real time.
Ron's Cipher v5 or Ron's Code v5 (RC5)	A symmetric cryptography method that implements a symmetric-key block cipher cryptographic algorithm produced by RSA Security, Inc.
Ron's Cipher v6 or Ron's Code v6 (RC6)	A symmetric-key block cipher cryptographic algorithm that was produced by RSA Security, Inc.
International Data Encryption Algorithm (IDEA)	A symmetric cryptography method that is a minor revision of an earlier PES (Proposed Encryption Standard). It uses 64-bit blocks with 128-bit keys and is used by Pretty Good Privacy (PGP) email encryption.
Data Encryption Standard (DES)	A very popular symmetric cryptography method created by the National Security Agency (NSA). It was one of the first symmetric encryption methods. It is now obsolete due to known weaknesses.
Triple DES (3DES)	An enhanced version of DES that corrects DES's known weaknesses.
Advanced Encryption Standard (AES)	An iterative symmetric block cipher that was developed as a replacement for DES in 2001.
Blowfish	A keyed symmetric block cipher that was intended to be free of the problems associated with other algorithms and replace DES.
Twofish	A symmetric block cipher that permits a wide variety of tradeoffs between speed, software size, key setup time, and memory.
Asymmetric encryption	An encryption method that uses two mathematically related keys called a key pair.
Challenge-Handshake Authentication Protocol (CHAP)	Challenge-Handshake Authentication Protocol is a procedure that uses a challenge/response (three-way handshake) mechanism to protect passwords.
Diffie-Hellman Key Exchange	Diffie-Hellman Key Exchange is an asymmetric algorithm that generates symmetric keys simultaneously at sender and recipient sites over non-secure channels.
Digital Signature Algorithm (DSA)	A federal standard for digital signatures that uses modular exponentiation and the discrete logarithm problem.

Elliptic Curve Cryptography (ECC)	A public-key cryptography method that is based on groups of numbers in an elliptical curve.
Extensible Authentication Protocol (EAP)	A framework that provides a standardized method to negotiate wireless authentications between wireless devices.
Message Digest Function (MD5)	An algorithm that produces a value of 128 bits with 32 hexadecimal characters.
Rivest, Shamir, Adleman (RSA)	A public-key cryptosystem that is used for secure data transmission.
Secure Hashing Algorithm (SHA)	A cryptographic function that produces a hash value for input data.
Public key infrastructure	A security architecture often used to ensure data transmissions between entities are validated and secure.
Certificate management system	The primary component that manages the certificate process.
Digital certificates	Electronic passwords created using PKI that allow secure data exchange over the internet.
Validation authority (VA)	The PKI component used to verify the validity of a digital certificate by way of the X.509 standard and RFC 5280.
Certificate authority (CA)	The organization that issues the digital certificate and is also the controller of the PKI certificates.
Registration authority (RA)	The entity that acts as the verifier for the CA.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Implement anti-malware measures
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control) 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

Video/Demo	Time
15.1.1 Cryptography	5:21
15.1.3 Symmetric Encryption	4:12
15.1.5 Asymmetric Encryption	5:41

15.1.7 Verify MD5 Hash Integrity	2:51
15.1.9 Public Key Infrastructure	6:51
Total Video Time	**24:56**

Lab/Activity

- 15.1.8 Compare an MD5 Hash

Fact Sheets

- 15.1.2 Cryptography Facts
- 15.1.4 Symmetric Encryption Facts
- 15.1.6 Asymmetric Encryption Facts
- 15.1.10 Public Key Infrastructure Facts

Number of Exam Questions

10 questions

Total Time

About 67 minutes

15.2: Cryptanalysis and Cryptographic Attack Countermeasures

Lecture Focus Questions:

- What are three types of cryptanalysis methods?
- What are common code breaking methods?
- What are three countermeasures that can be used to prevent cryptography attacks?

Key terms for this section include the following:

Term	Definition
Linear cryptanalysis	Linear cryptanalysis finds the affine approximations to the action of a cipher.
Differential cryptanalysis	A form of cryptanalysis applicable to symmetric key algorithms. Differential cryptanalysis works on statistical differences between ciphertexts of chosen data.
Integral cryptanalysis	An integral cryptanalysis attack is useful against block ciphers based on substitution-permutation networks. It is an extension of differential cryptanalysis.
Brute force attack	An attack in which cryptography keys are discovered by trying every possible combination.
Frequency analysis	The study of the frequency of letters or groups of letters in a ciphertext.
One-time pad	A cryptography method that contains many non-repeating, randomly chosen groups of letters or numbers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Routing and Switching Pro	6.4 Implement security measures • Implement anti-malware measures
Cisco CCNA 200-301	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) 5.2 Describe security program elements (user awareness, training, and physical access control)

Video/Demo	Time
15.2.1 Cryptanalysis and Cryptographic Attack Countermeasures	5:57
15.2.3 Data Encryption	4:33
Total Video Time	**10:30**

Fact Sheets

- 15.2.2 Cryptanalysis and Cryptographic Attack Countermeasures Facts

Number of Exam Questions

10 questions

Total Time

About 26 minutes

Practice Exams

A.0: TestOut Routing and Switching Pro Practice Exams

TestOut Routing and Switching Pro Certification Practice Exam (15 questions)

B.0: Cisco CCNA 200-301 Practice Exams

Appendix A: Approximate Time for the Course

The total time for the LabSim for Routing and Switching Pro course is approximately **70 hours and 45 minutes**. Time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo times
- Text Lessons (5 minutes assigned per text lesson)
- Simulations (12 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **36 hours and 4 minutes** of Practice Test material at the end of the course.

The breakdown for this course is as follows:

Module Sections	Time	Videos	Labs	Text	Exams
1.0: Introduction to Routing and Switching Pro					
1.1: Introduction	35	30	0	5	0
Total	**0:35**	**0:30**	**0:00**	**0:05**	**0:00**
2.0: Networking Concepts					
2.1: TCP/IP Networking Model	49	24	0	15	10
2.2: OSI Networking Model	37	12	0	15	10
2.3: Networking Basics	29	9	0	10	10
2.4: Data Encapsulation and Communications	36	16	0	10	10
2.5: Ethernet	47	17	0	20	10
2.6: Network Devices	51	26	0	15	10
Total	**4:09**	**1:44**	**0:00**	**1:25**	**1:00**
3.0: Cisco Devices					
3.1: Cisco Device Connection	40	20	0	10	10
3.2: Command Line Interface (CLI)	75	18	12	35	10
3.3: IOS Licensing	25	10	0	5	10
3.4: Device Settings	73	12	36	15	10
3.5: Device Passwords	71	15	36	10	10
3.6: Cisco Discovery Protocol (CDP)	79	11	48	10	10
Total	**6:03**	**1:26**	**2:12**	**1:25**	**1:00**
4.0: IP Addressing					
4.1: IPv4 Addressing Overview	58	33	0	15	10
4.2: Subnets	59	29	0	20	10
4.3: Subnet Planning and Design	48	9	24	5	10
4.4: Route Summarization	30	10	0	10	10
4.5: IPv6 Addressing Overview	56	16	0	30	10
4.6: Dynamic Host Configuration Protocol (DHCP)	68	12	36	10	10
4.7: The Domain Name System (DNS)	107	27	60	10	10

Total	**7:06**	**2:16**	**2:00**	**1:40**	**1:10**
5.0: Switching					
5.1: Layer 2 Switching Overview	60	30	0	20	10
5.2: Switch Interface Configuration	98	13	60	15	10
Total	**2:38**	**0:43**	**1:00**	**0:35**	**0:20**
6.0: IPv4 Routing					
6.1: IPv4 Routing	35	15	0	10	10
6.2: Static Routing	40	8	12	10	10
6.3: Dynamic Routing	58	16	12	20	10
6.4: IPv4 Routing Troubleshooting	43	28	0	5	10
6.5: Network Communications Troubleshooting	51	9	12	20	10
Total	**3:47**	**1:16**	**0:36**	**1:05**	**0:50**
7.0: IPv4 Routing Protocols					
7.1: Open Shortest Path First (OSPF) Overview	37	22	0	5	10
7.2: OSPF for IPv4	30	15	0	5	10
7.3: OSPF Configuration	70	19	36	5	10
7.4: OSPF LSA Types and Databases	31	16	0	5	10
7.5: Adjacency Troubleshooting	51	12	24	5	10
7.6: EIGRP for IPv4 Routing	36	21	0	5	10
7.7: EIGRP for IPv4 Configuration	52	25	12	5	10
Total	**5:07**	**2:10**	**1:12**	**0:35**	**1:10**
8.0: IPv6 Routing					
8.1: IPv6 Routing Overview	39	19	0	10	10
8.2: OSPFv3	27	12	0	5	10
8.3: EIGRPv6	28	13	0	5	10
Total	**1:34**	**0:44**	**0:00**	**0:20**	**0:30**
9.0: Wireless Networks					
9.1: Wireless Concepts	36	16	0	10	10
9.2: Wireless Standards	42	27	0	5	10
9.3: Wireless Configuration	59	20	24	5	10
9.4: Wireless Network Design	70	26	24	10	10
9.5: Wireless Network Implementation	43	16	12	5	10
9.6: SOHO Configuration	66	29	12	15	10
9.7: Wireless Security	66	34	12	10	10
9.8: Wireless Troubleshooting	77	26	36	5	10
Total	**7:39**	**3:14**	**2:00**	**1:05**	**1:20**
10.0: WAN Implementation					
10.1: WAN Types	29	9	0	10	10
10.2: Leased Line WAN Links	61	17	24	10	10
10.3: Network Address Translation (NAT)	71	20	36	5	10
10.4: WAN Troubleshooting	64	13	36	5	10
Total	**3:45**	**0:59**	**1:36**	**0:30**	**0:40**
11.0: Advanced Switching					
11.1: Virtual LANs (VLANs)	44	12	12	10	10
11.2: Trunking	82	16	36	20	10
11.3: Spanning Tree	103	44	24	25	10
11.4: Spanning Tree Configuration	104	24	60	10	10

11.5: Router-on-a-Stick InterVLAN Routing		63	26	12	15	10
11.6: Switch InterVLAN Routing		80	12	48	10	10
11.7: Switch Troubleshooting		66	10	36	10	10
	Total	**9:02**	**2:24**	**3:48**	**1:40**	**1:10**
12.0: Access Control Lists						
12.1: Access Control Lists (ACLs)		103	42	36	15	10
12.2: IPv6 and Extended ACLs		116	38	48	20	10
	Total	**3:39**	**1:20**	**1:24**	**0:35**	**0:20**
13.0: Network Management						
13.1: Network Time Protocol (NTP)		20	5	0	5	10
13.2: System Message Log		22	7	0	5	10
13.3: Simple Network Management Protocol		33	18	0	5	10
13.4: NetFlow		21	6	0	5	10
13.5: Quality of Service (QoS)		24	9	0	5	10
13.6: Enterprise Networking		37	17	0	10	10
13.7: Cloud Resources		27	7	0	10	10
13.8: Virtual Private Networks and Remote Switch Access		29	9	0	10	10
13.9: Default Gateway Redundancy		44	12	12	10	10
13.10: Network Automation		30	5	0	15	10
	Total	**4:47**	**1:35**	**0:12**	**1:20**	**1:40**
14.0: Network Security						
14.1: Network Threats		46	21	0	15	10
14.2: Network Security Best Practices		58	26	12	10	10
14.3: Switch Security		141	27	84	20	10
14.4: Malware		54	24	0	20	10
14.5: Combat Malware		74	11	48	5	10
14.6: Sniffing		74	30	24	10	10
14.7: Session Hijacking		75	26	24	15	10
14.8: Denial of Service		77	28	24	15	10
	Total	**9:59**	**3:13**	**3:36**	**1:50**	**1:20**
15.0: Cryptography						
15.1: Cryptography		67	25	12	20	10
15.2: Cryptanalysis and Cryptographic Attack Countermeasures		26	11	0	5	10
	Total	**1:33**	**0:36**	**0:12**	**0:25**	**0:20**

Total Course Time 70:45

Practice Exams

A.0: TestOut Routing and Switching Pro Practice Exams	**Number of Questions**	**Time**
A.2: TestOut Routing and Switching Pro Practice Exams - All Questions	99	19:48
A.3: TestOut Routing and Switching Pro Certification Practice Exam	15	2:00
Total	**114**	**21:48**

B.0: Cisco CCNA 200-301 Practice Exams	**Number of Questions**	**Time**
B.2: Cisco 200-301 CCNA Practice Exams - 20 Random	120	2:00

B.3: Cisco 200-301 CCNA Practice Exams - All Questions	616	10:16
B.4: Cisco 200-301 CCNA Practice Exams - Practice Certification	90	2:00
Total	**826**	**14:16**
Total Practice Exam Time 36:04		