Networking Academy

CCNA 7.0
DRAFT Scope and Sequence

Last Updated November 15, 2019

Target Audience

The Cisco Networking Academy® CCNA® 7.0 curriculum is designed for participants who are seeking associate-level jobs in the ICT industry or hope to fulfill prerequisites to pursue more specialized ICT skills. The CCNA 7.0 curriculum provides an integrated and comprehensive coverage of networking topics including: IP routing and switching fundamentals, network security and services, and network programmability and automation, while providing learners extensive opportunities for hands-on practical experience and career skills development.

The curriculum is appropriate for learners at many education levels and types of institutions, including high schools, secondary schools, universities, colleges, career and technical schools, and community centers.

Prerequisites

There are no prerequisites for this offering. Learners are expected to have the following skills:

- High school reading level
- Basic computer literacy
- Basic PC operating system navigation skills
- Basic internet usage skills

Curriculum Description

In this curriculum, Cisco Networking Academy™ participants develop workforce readiness skills and build a foundation for success in networking-related careers and degree programs. With the support of video and rich interactive media, participants learn, apply and practice CCNA knowledge and skills through a series of in-depth hands-on experiences and simulated activities that reinforce their learning. Upon completion of this offering, learners will be prepared to take the Cisco CCNA certification exam.

CCNA 7.0 teaches comprehensive networking concepts and skills, from network applications to the protocols and services provided to those applications. Learners will progress from basic networking to more complex enterprise and theoretical networking models later in the curriculum.

CCNA 7.0 includes the following features:

- There are three courses that make up the CCNA 7.0 curriculum.
- The three courses align to and cover the competencies outlined for the CCNA Certification Exam (200-301).
- Each course is comprised of multiple modules. Each module is comprised of topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Each topic contains a Check Your Understanding interactive quiz, or some other way to assess understanding, such as a lab or a Packet Tracer. These topic-level assessments are designed to tell learners if they have a good grasp of the topic content, or if they need to review before continuing. Learners can ensure their level of understanding well before taking a graded quiz or exam. Check Your Understanding quizzes do not affect the learner's overall grade.

- Students learn the basics of routing, switching, and wireless, advanced technologies to prepare for the Cisco CCNA exam, networking related degree programs, and associate-level networking careers.
- The language used to describe networking concepts is designed to be easily understood by learners at all levels and embedded interactive activities help reinforce comprehension.
- Assessments and practice activities are focused on specific competencies to increase retention and provide flexibility in the learning path.
- Multimedia learning tools, including videos, games, and quizzes, address a variety of learning styles and help stimulate learning and promote increased knowledge retention.
- Hands-on labs and Cisco® Packet Tracer simulation-based learning activities help students develop critical thinking and complex problem-solving skills.
- Embedded assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
- Cisco Packet Tracer activities are designed for use with the latest version of Packet Tracer.

Courses

The curriculum is divided into three courses. Each course contains roughly 70 hours of course work. Course names and descriptions are as follows:

CCNAv7: Introduction to Networks (ITN) The first course in the CCNA curriculum introduces the architectures, models, protocols, and networking elements that connect users, devices, applications and data through the Internet and across modern computer networks - including IP addressing and Ethernet fundamentals. By the end of the course, students can build simple local area networks (LAN) that integrate IP addressing schemes, foundational network security, and perform basic configurations for routers and switches.

CCNAv7: Switching, Routing, and Wireless Essentials (SRWE) The second course in the CCNA curriculum focuses on switching technologies and router operations that support small-to-medium business networks and includes wireless local area networks (WLAN) and security concepts. Students learn key switching and routing concepts. They can perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN.

CCNAv7: Enterprise Networking, Security, and Automation (ENSA) The third course in the CCNA curriculum describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access along with the introduction of software-defined networking, virtualization, and automation concepts that support the digitalization of networks. Students gain skills to configure and troubleshoot enterprise networks, and learn to identify and protect against cybersecurity threats. They are introduced to network management tools and learn key concepts of software-defined networking, including controller-based architectures and how application programming interfaces (APIs) enable network automation.

By the end of the CCNA course series, students gain practical, hands-on experience preparing them for the CCNA certification exam and career-ready skills for associate-level roles in the Information & Communication Technologies (ICT) industry.

Below is a summary list of the modules currently planned in each of the three courses. A detailed list, including a description of each topic contained within each module can be found in the curriculum outline section of this document.

CCNAv7: Introduction to Networks (ITN)

CCNAv7: Introduction to Networks (ITN)	
Module	**Objective**
Networking Today	Explain the advances in modern network technologies.
Basic Switch and Device Configuration	Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.
Protocols and Models	Explain how network protocols enable devices to access local and remote network resources.

Physical Layer	Explain how physical layer protocols, services, and network media support communications across data networks.
Number Systems	Calculate numbers between decimal and binary systems.
Data Link Layer	Explain how media access control in the data link layer supports communication across networks.
Ethernet Switching	Explain how Ethernet operates in a switched network.
Network Layer	Explain how routers use network layer protocols and services to enable end-to-end connectivity.
Address Resolution	Explain how ARP and ND enable communication on a local area network.
Basic Router Configuration	Implement initial settings on a router and end devices.
IPv4 Addressing	Calculate an IPv4 subnetting scheme to efficiently segment your network.
IPv6 Addressing	Implement an IPv6 addressing scheme.
ICMP	Use various tools to test network connectivity.
Transport Layer	Compare the operations of transport layer protocols in supporting end-to-end communication.
Application Layer	Explain the operation of application layer protocols in providing support to end-user applications.
Network Security Fundamentals	Configure switches and routers with device hardening features to enhance security.
Build a Small Network	Implement a network design for a small network to include a router, a switch, and end devices.

CCNAv7: Switching, Routing, and Wireless Essentials (SRWE)

CCNAv7: Switching, Routing, and Wireless Essentials (SRWE)	
Module	**Objective**
Basic Device Configuration	Configure devices by using security best practices.
Switching Concepts	Explain how Layer 2 switches forward data.
VLANs	Implement VLANs and trunking in a switched network.
Inter-VLAN Routing	Troubleshoot inter-VLAN routing on Layer 3 devices.
STP	Explain how STP enables redundancy in a Layer 2 network.
EtherChannel	Troubleshoot EtherChannel on switched links.
DHCPv4	Implement DHCPv4 to operate across multiple LANs.
SLAAC and DHCPv6 Concepts	Explain the operation of dynamic address allocation in IPv6 networks.
FHRP Concepts	Explain how FHRPs provide default gateway services in a redundant network.
LAN Security Concepts	Explain how vulnerabilities compromise LAN security.
Switch Security Configuration	Configure switch security to mitigate LAN attacks.
WLAN Concepts	Explain how WLANs enable network connectivity.
WLAN Configuration	Implement a WLAN using a wireless router and WLC.
Routing Concepts	Explain how routers use information in packets to make forwarding decisions.
IP Static Routing	Configure IPv4 and IPv6 floating static routes.
Troubleshoot Static and Default Routes	Explain how to troubleshoot static and default route configurations.

CCNAv7: Enterprise Networking, Security, and Automation (ENSA)

CCNAv7: Enterprise Networking, Security, and Automation (ENSA)

Module	Objective
Single-Area OSPFv2 Concepts	Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
Single-Area OSPFv2 Configuration	Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
Network Security Concepts	Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
ACL Concepts	Explain how ACLs are used as part of a network security policy.
ACLs for IPv4 Configuration	Implement IPv4 ACLs to filter traffic and secure administrative access.
NAT for IPv4	Implement NAT services on the edge router to provide IPv4 address scalability.
WAN Concepts	Explain how WAN access technologies can be used to satisfy business requirements.
VPN and IPsec Concepts	Explain how VPNs and IPsec are used to secure site-to-site and remote access connectivity.
QoS Concepts	Explain how networking devices implement QoS.
Network Management	Implement network management protocols to monitor the network.
Network Design	Explain the characteristics of scalable network architectures.
Network Troubleshooting	Troubleshoot enterprise networks.
Network Virtualization	Explain the purpose and characteristics of network virtualization.
Network Automation	Explain how network automation is enabled through RESTful APIs and configuration management tools.

Lab Equipment Requirements

Current designs for lab topologies leverage equipment used in previous CCNA 6.0 version and include options to utilize a 2 router + 2 switch + 1 wireless router physical equipment bundle described below. Labs with more complex topologies will rely on PT as a complementary environment to be used in addition to the physical labs. Detailed equipment information, including descriptions and part numbers for the equipment used in the new CCNAv7 courses ~~previous CCNA 6 version~~ is available in the CCNAv7 Equipment List, which is located on the Cisco NetAcad Equipment Information site.

Baseline Equipment Bundle:

- 2 x ISR4221/K9 Routers
- 2 x WS-C2960+24TC-L Catalyst switches
- 1 wireless router (generic brand) with WPA2 support
- Ethernet patch cables
- PCs - minimum system requirements
  - CPU: Intel Pentium 4, 2.53 GHz or equivalent •
  - OS: Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows 10, Ubuntu 14.04 LTS, macOS High Sierra and Mojave •
  - RAM: 4 GB
  - Storage: 500 MB of free disk space
  - Display resolution: 1024 x 768
  - Language fonts supporting Unicode encoding (if viewing in languages other than English)
  - Latest video card drivers and operating system updates
- Internet connection for lab and study PCs
- Optional equipment for connecting to a WLAN
  - 1 printer or integrated printer/scanner/copier for the class to share
  - Smartphones and tablets are desirable for use with the labs

Software:

- Cisco IOS versions:
  - Routers: Version IOS XE 16.0 or higher, IP Base feature set.
  - Switches: Version IOS 15.0 or higher, lanbaseK9 feature set.
- Packet Tracer v7.3
- Open-source server software:
  - For various services and protocols, such as Telnet, SSH, HTTP, DHCP, FTP, TFTP, etc.
- Tera Term source SSH client software for lab PCs.
- Oracle VirtualBox, most recent version.
- Wireshark version 2.5 or higher.

CCNA v7.0 Curriculum Outline

This curriculum provides a comprehensive introduction to the networking field and in-depth exposure to fundamental networking, LAN switching, wireless LANs, basic routing, Cybersecurity, WAN concepts, VPNs, QoS, virtualization, and network automation. Threaded throughout the course are security concepts and skills including threat mitigation through LAN security, ACLs, and IPsec. Through hands-on lab activities, students learn how to implement network technologies and troubleshoot common issues.

Listed below are the current set of modules and their associated competencies outlined for this curriculum. Each module is an integrated unit of learning that consists of content, activities and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency. Some modules are considered foundational, in that the artifacts presented, while not assessed, enable learning of concepts that are covered on the CCNA certification exam.

~~The distribution and mapping of these modules into courses will be defined in future updates to this scope and sequence document.~~

CCNA v7.0 Curriculum Outline – Draft August 2019

CCNAv7: Introduction to Networks (ITN)		
Module	**Topic**	**Objective**
Networking Today		Explain the advances in modern network technologies.
	Networks Affect Our Lives	Explain how networks affect our daily lives.
	Network Components	Explain how host and network devices are used.
	Network Representations and Topologies	Explain network representations and how they are used in network topologies.
	Common Types of Networks	Compare the characteristics of common types of networks.
	Internet Connections	Explain how LANs and WANs interconnect to the internet.
	Reliable Network	Describe the four basic requirements of a reliable network.
	Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
	Network Security	Identify some basic security threats and solutions for all networks.
	The IT Professional	Explain employment opportunities in the networking field.
Module	**Topic**	**Objective**

Basic Switch and Device Configuration		Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.
	Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
	IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
	The Command Structure	Describe the command structure of Cisco IOS software.
	Basic Device Configuration	Configure a Cisco IOS device using CLI.
	Save Configurations	Use IOS commands to save the running configuration.
	Ports and Addresses	Explain how devices communicate across network media.
	Configure IP Addressing	Configure a host device with an IP address.
	Verify Connectivity	Verify connectivity between two end devices.
Module	**Topic**	**Objective**
Protocols and Models		Explain how network protocols enable devices to access local and remote network resources.
	The Rules	Describe the types of rules that are necessary to successfully communicate.
	Protocols	Explain why protocols are necessary in network communication.
	Protocol Suites	Explain the purpose of adhering to a protocol suite.
	Standards Organizations	Explain the role of standards organizations in establishing protocols for network interoperability.
	Reference Models	Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
	Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
	Data Access	Explain how local hosts access local resources on a network.
Module	**Topic**	**Objective**
Physical Layer		Explain how physical layer protocols, services, and network media support communications across data networks.

	Purpose of the Physical Layer	Describe the purpose and functions of the physical layer in the network.
	Physical Layer Characteristics	Describe characteristics of the physical layer.
	Copper Cabling	Identify the basic characteristics of copper cabling.
	UTP Cabling	Explain how UTP cable is used in Ethernet networks.
	Fiber-Optic Cabling	Describe fiber-optic cabling and its main advantages over other media.
	Wireless Media	Connect devices using wired and wireless media.
Module	**Topic**	**Objective**
Number Systems		Calculate numbers between decimal and binary systems.
	Binary Number System	Calculate numbers between decimal and binary systems.
	Hexadecimal Number System	Calculate numbers between decimal and hexadecimal systems.
Module	**Topic**	**Objective**
Data Link Layer		Explain how media access control in the data link layer supports communication across networks.
	Purpose of the Data Link Layer	Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.
	Topologies	Compare the characteristics of media access control methods on WAN and LAN topologies.
	Data Link Frame	Describe the characteristics and functions of the data link frame.
Module	**Topic**	**Objective**
Ethernet Switching		Explain how Ethernet operates in a switched network.
	Ethernet Frame	Explain how the Ethernet sublayers are related to the frame fields.
	Ethernet MAC Address	Describe the Ethernet MAC address.
	The MAC Address Table	Explain how a switch builds its MAC address table and forwards frames.
	Switch Speeds and Forwarding Methods	Describe switch forwarding methods and port settings available on Layer 2 switch ports.

Module	**Topic**	**Objective**
Network Layer		Explain how routers use network layer protocols and services to enable end-to-end connectivity.
	Network Layer Characteristics	Explain how the network layer uses IP protocols for reliable communications.
	IPv4 Packet	Explain the role of the major header fields in the IPv4 packet.
	IPv6 Packet	Explain the role of the major header fields in the IPv6 packet.
	How a Host Routes	Explain how network devices use routing tables to direct packets to a destination network.
	Router Routing Tables	Explain the function of fields in the routing table of a router.
Module	**Topic**	**Objective**
Address Resolution		Explain how ARP and ND enable communication on a local area network.
	MAC and IP	Compare the roles of the MAC address and the IP address.
	ARP	Describe the purpose of ARP.
	Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.
Module	**Topic**	**Objective**
Basic Router Configuration		Implement initial settings on a router and end devices.
	Configure Initial Router Settings	Configure initial settings on a IOS Cisco router.
	Configure Interfaces	Configure two active interfaces on a Cisco IOS router.
	Configure the Default Gateway	Configure devices to use the default gateway.
Module	**Topic**	**Objective**
IPv4 Addressing		Calculate an IPv4 subnetting scheme to efficiently segment your network.
	IPv4 Address Structure	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
	IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.

	Types of IPv4 Addresses	Explain public, private, and reserved IPv4 addresses.
	Network Segmentation	Explain how subnetting segments a network to enable better communication.
	Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.
	Subnet a /16 and /8 Prefix	Calculate IPv4 subnets for a /16 and /8 prefix.
	Subnet to Meet Requirements	Given a set of requirements for subnetting, implement an IPv4 addressing scheme.
	Variable Length Subnet Masking	Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).
	Structured Design	Implement a VLSM addressing scheme.
Module	**Topic**	**Objective**
IPv6 Addressing		Implement an IPv6 addressing scheme.
	IPv4 Issues	Explain the need for IPv6 addressing.
	IPv6 Addressing	Explain how IPv6 addresses are represented.
	Types of IPv6 Addresses	Compare types of IPv6 network addresses.
	IPv6 Unicast Addresses	Configure global unicast addresses.
	Dynamic IPv6 Unicast Addresses	Configure global unicast addresses dynamically.
	IPv6 Multicast Addresses	Describe multicast addresses.
	Subnet an IPv6 Network	Explain how to implement IPv6 address assignments in a business network.
Module	**Topic**	**Objective**
ICMP		Use various tools to test network connectivity.
	ICMP Messages	Explain how ICMP is used to test network connectivity.
	Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.
Module	**Topic**	**Objective**
Transport Layer		Compare the operations of transport layer protocols in supporting end-to-end communication.
	Transportation of Data	Explain the purpose of the transport layer in managing the transportation of data in end-to-end communication.

	TCP and UDP Overview	Explain characteristics of the TCP and UDP protocols, including port numbers and their uses.
	TCP Communication Process	Explain how TCP session establishment and termination processes facilitate reliable communication.
	Reliability and Flow Control	Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.
	UDP Communication	Describe the UDP client processes to establish communication with a server.
Module	**Topic**	**Objective**
Application Layer		Explain the operation of application layer protocols in providing support to end-user applications.
	Application, Session, and Presentation	Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications.
	Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
	Web and Email Protocols	Explain how web and email protocols operate.
	IP Addressing Services	Explain how DNS and DHCP operate.
	File Sharing Services	Explain how file transfer protocols operate.
Module	**Topic**	**Objective**
Network Security Fundamentals		Configure switches and routers with device hardening features to enhance security.
	Security Threats and Vulnerabilities	Explain why basic security measure are necessary on network devices.
	Network Attacks	Identify security vulnerabilities.
	Network Attack Mitigation	Identify general mitigation techniques.
	Device Security	Configure network devices with device hardening features to mitigate security threats.
Module	**Topic**	**Objective**
Build a Small Network		Implement a network design for a small network to include a router, a switch, and end devices.
	Devices in a Small Network	Identify the devices used in a small network.
	Small Network Applications and Protocols	Identify the protocols and applications used in a small network.
	Scale to Larger Networks	Explain how a small network serves as the basis of larger networks.

	Verify Connectivity	Use the output of the ping and tracert commands to verify connectivity and establish relative network performance.
	Show Commands	Use show commands to verify the configuration and status of network devices.
	Host and IOS Commands	Use host and IOS commands to acquire information about the devices in a network.
	Troubleshooting Methodologies	Describe common network troubleshooting methodologies.
	Troubleshooting Scenarios	Troubleshoot issues with devices in the network.

CCNAv7: Switching, Routing, and Wireless Essentials (SRWE)		
Module	**Topic**	**Objective**
Basic Device Configuration		Configure devices by using security best practices.
	Configure a Switch with Initial Settings	Configure initial settings on a Cisco switch.
	Configure Switch Ports	Configure switch ports to meet network requirements
	Secure Remote Access	Configure secure management access on a switch.
	Configure Basic Router Settings	Configure basic settings on a router to route between two directly-connected networks, using CLI.
	Verify Directly Connected Networks	Verify connectivity between two networks that are directly connected to a router.
Module	**Topic**	**Objective**
Switching Concepts		Explain how Layer 2 switches forward data.
	Frame Forwarding	Explain how frames are forwarded in a switched network.
	Switching Domains	Compare a collision domain to a broadcast domain.
Module	**Topic**	**Objective**
VLANs		Implement VLANs and trunking in a switched network.
	Overview of VLANs	Explain the purpose of VLANs in a switched network.
	VLANs in a Multi-Switched Environment	Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.
	VLAN Configuration	Configure a switch port to be assigned to a VLAN based on requirements.
	VLAN Trunks	Configure a trunk port on a LAN switch.
	Dynamic Trunking Protocol	Configure Dynamic Trunking Protocol (DTP).
Module	**Topic**	**Objective**
Inter-VLAN Routing		Troubleshoot inter-VLAN routing on Layer 3 devices.
	Inter-VLAN Routing Operation	Describe options for configuring inter-VLAN routing.
	Configure Router-on-a-Stick Inter-VLAN Routing	Configure router-on-a-stick inter-VLAN routing.
	Inter-VLAN Routing using Multilayer Switches	Configure inter-VLAN routing using Layer 3 switching.

	Inter-VLAN Configuration Issues	Troubleshoot common inter-VLAN configuration issues
Module	**Topic**	**Objective**
STP		Explain how STP enables redundancy in a Layer 2 network.
	Purpose of STP	Explain common problems in a redundant, L2 switched network.
	STP Operations	Explain how a simple, switched network that uses STP operates.
	Evolution of STP	Explain how Rapid PVST+ operates.
Module	**Topic**	**Objective**
EtherChannel		Troubleshoot EtherChannel on switched links.
	EtherChannel Operation	Describe EtherChannel technology.
	Configure EtherChannel	Configure EtherChannel.
	Verify and Troubleshoot EtherChannel	Troubleshoot EtherChannel.
Module	**Topic**	**Objective**
DHCPv4		Implement DHCPv4 to operate across multiple LANs.
	DHCPv4 Operation	Implement DHCPv4 to operate across multiple LANs.
	Configure DHCPv4 Server	Configure a router as a DHCPv4 server.
	Configure DHCPv4 Client	Configure a router as a DHCPv4 client.
Module	**Topic**	**Objective**
SLAAC and DHCPv6 Concepts		Explain the operation of dynamic address allocation in IPv6 networks.
	SLAAC and DHCPv6	Explain the operation of DHCPv6.
	Configuring DHCPv6	Configure stateful and stateless DHCPv6.
Module	**Topic**	**Objective**
FHRP Concepts		Explain how FHRPs provide default gateway services in a redundant network.
	First Hop Redundancy	Explain the purpose and operation of first hop redundancy protocols.
Module	**Topic**	**Objective**
LAN Security Concepts		Explain how vulnerabilities compromise LAN security.
	Endpoint Security	Explain how use endpoint security to mitigate attacks.
	Access Control	Explain how AAA and 802.1x are used to authenticate LAN endpoints and devices.
	Layer 2 Security Threats	Identify Layer 2 vulnerabilities.

	MAC Address Table Attack	Explain how a MAC address table attack compromises LAN security.
	LAN Attacks	Explain how LAN attacks compromises LAN security.
Module	**Topic**	**Objective**
Switch Security Configuration		Configure switch security to mitigate LAN attacks.
	Implement Port Security	Implement port security to mitigate MAC address table attacks.
	Mitigate VLAN Attacks	Configure DTP and native VLAN to mitigate VLAN attacks.
	Mitigate DHCP Attacks	Configure DHCP snooping to mitigate DHCP attacks.
	Mitigate ARP Attacks	Configure ARP inspection to mitigate ARP attacks.
	Mitigate STP Attacks	Configure portfast and bpdu guard.
Module	**Topic**	**Objective**
WLAN Concepts		Explain how WLANs enable network connectivity.
	Introduction to Wireless	Describe WLAN technology and standards.
	Components of WLANs	Describe the components of a WLAN infrastructure.
	WLAN Operation	Explain how wireless technology enables WLAN operation.
	CAPWAP Operation	Explain how a WLC uses CAPWAP to manage multiple APs.
	Channel Management	Describe channel management in a WLAN.
	WLAN Threats	Describe threats to WLANs.
	Secure WLANs	Describe WLAN security mechanisms.
Module	**Topic**	**Objective**
WLAN Configuration		Implement a WLAN using a wireless router and WLC.
	Remote Site WLAN Configuration	Configure a WLAN to support a remote site.
	WLC Configuration	Configure a WLAN using the GUI on a WLC.
	Troubleshoot WLAN Issues	Explain how to troubleshoot common wireless configuration issues.
Module	**Topic**	**Objective**
Routing Concepts		Explain how routers use information in packets to make forwarding decisions.
	Features of a Router	Describe the primary functions and features of a router.
	Forwarding Packets from Source to Destination	Explain the path determination function of a router.
	Basic Router Settings	Configure basic settings on a router.

	IP Routing Table	Describe the structure of a routing table.
	Dynamic and Static Routing	Compare static and dynamic routing concepts.
Module	**Topic**	**Objective**
IP Static Routing		Configure IPv4 and IPv6 floating static routes.
	Configure IP Static Routes	Configure IPv4 and IPv6 static routes.
	Configure IP Default Static Routes	Configure IPv4 and IPv6 default static routes.
	Configure Floating Static Routes	Configure a floating static route to provide a backup connection.
	Configure Static Host Routes	Configure IPv4 and IPv6 static host routes that direct traffic to a specific host.
Module	**Topic**	**Objective**
Troubleshoot Static and Default Routes		Explain how to troubleshoot static and default route configurations.
	Packet Processing with Static Routes	Explain how a router processes packets when a static route is configured.
	Troubleshoot IPv4 Static and Default Route Configuration	Explain how to troubleshoot common static and default route configuration issues.

CCNAv7: Enterprise Networking, Security, and Automation (ENSA)		
Module	**Topic**	**Objective**
Single-Area OSPFv2 Concepts		Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
	OSPF Features and Characteristics	Describe basic OSPF features and characteristics.
	OSPF Packets	Describe the OSPF packet types used in single-area OSPF.
	OSPF Operation	Explain how single-area OSPF operates.
Module	**Topic**	**Objective**
Single-Area OSPFv2 Configuration		Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
	OSPF Router ID	Configure an OSPFv2 router ID.
	Point-to-Point OSPF Networks	Configure single-area OSPFv2 in a point-to-point network.
	Multiaccess OSPF Networks	Configure the OSPF interface priority to influence the DR/BDR election in a multiaccess network.
	Modify Single-Area OSPFv2	Implement modifications to change the operation of single-area OSPFv2.
	Default Route Propagation	Configure OSPF to propagate a default route.
	Verify Single-Area OSPFv2	Verify a single-area OSPFv2 implementation.
Module	**Topic**	**Objective**
Network Security Concepts		Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
	Current State of Cybersecurity	Describe the current state of cybersecurity and vectors of data loss.
	Threat Actors	Describe the threat actors who exploit networks.
	Threat Actor Tools	Describe tools used by threat actors to exploit networks.
	Malware	Describe malware types.
	Common Network Attacks	Describe common network attacks.
	IP Vulnerabilities and Threats	Explain how IP vulnerabilities are exploited by threat actors.
	TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities are exploited by threat actors.
	IP Services	Explain how IP services are exploited by threat actors.
	Network Security Best Practices	Describe best practices for protecting a network.

	Cryptography	Describe common cryptographic processes used to protect data in transit.
Module	**Topic**	**Objective**
ACL Concepts		Explain how ACLs are used as part of a network security policy.
	Purpose of ACLs	Explain how ACLs are used as part of a network security policy.
	Wildcard Masks in ACLs	Explain how ACLs use wildcard masks.
	Guidelines for ACL Creation	Explain how to create ACLs.
	Types of IPv4 ACLs	Compare standard and extended IPv4 ACLs.
Module	**Topic**	**Objective**
ACLs for IPv4 Configuration		Implement IPv4 ACLs to filter traffic and secure administrative access.
	Configure Standard IPv4 ACLs	Configure standard IPv4 ACLs to filter traffic to meet networking requirements.
	Modify IPv4 ACLs	Use sequence numbers to edit existing standard IPv4 ACLs.
	Secure VTY Ports with a Standard IPv4 ACL	Configure a standard ACL to secure vty access.
	Structure of an Extended IPv4 ACL	Explain the structure of an extended access control entry (ACE).
	Configure Extended IPv4 ACLs	Configure extended IPv4 ACLs to filter traffic according to networking requirements.
Module	**Topic**	**Objective**
NAT for IPv4		Implement NAT services on the edge router to provide IPv4 address scalability.
	NAT Characteristics	Explain the purpose and function of NAT.
	Types of NAT	Explain the operation of different types of NAT.
	NAT Advantages	Describe the advantages and disadvantages of NAT.
	Configure Static NAT	Configure static NAT using the CLI.
	Configure Dynamic NAT	Configure dynamic NAT using the CLI.
	Configure PAT	Configure PAT using the CLI.
	NAT and IPv6	Describe NAT for IPv6.
Module	**Topic**	**Objective**
WAN Concepts		Explain how WAN access technologies can be used to satisfy business requirements.
	Purpose of WANs	Explain the purpose of a WAN.
	WAN Operations	Explain how WANs operate.

	Private WAN Infrastructures	Compare private WAN technologies.
	Public WAN Infrastructure	Compare public WAN technologies.
	Selecting WAN Services	Describe the appropriate WAN protocol and service for a specific network requirement.
	Serial Communications	Explain the fundamentals of point-to-point serial communication across a WAN.
	Broadband Connections	Compare remote access broadband connection options for small to medium-sized businesses.
Module	**Topic**	**Objective**
VPN and IPsec Concepts		Explain how VPNs and IPsec are used to secure site-to-site and remote access connectivity.
	VPN Technology	Describe benefits of VPN technology.
	Types of VPNs	Describe different types of VPNs
	IPsec	Explain how the IPsec framework is used to secure network traffic.
Module	**Topic**	**Objective**
QoS Concepts		Explain how networking devices implement QoS.
	Network Transmission Quality	Explain how network transmission characteristics impact quality.
	Traffic Characteristics	Describe minimum network requirements for voice, video, and data traffic.
	Queuing Algorithms	Describe the queuing algorithms used by networking devices.
	QoS Models	Describe the different QoS models.
	QoS Implementation Techniques	Explain how QoS uses mechanisms to ensure transmission quality.
Module	**Topic**	**Objective**
Network Management		Implement network management protocols to monitor the network.
	Device Discovery with CDP	Use CDP to map a network topology.
	Device Discovery with LLDP	Use CDP to map a network topology.
	NTP	Implement NTP between an NTP client and NTP server.
	SNMP Operation	Explain how SNMP operates.
	Syslog Operation	Explain syslog operation.
	Router and Switch File Maintenance	Use commands to back up and restore an IOS configuration file.
	IOS Image Management	Perform an upgrade an IOS system image.

Module	Topic	Objective
Network Design		Explain the characteristics of scalable network architectures.
	Converged Networks	Explain how data, voice, and video are converged in a switched network.
	Switched Networks	Describe a switched network in a small to medium-sized business.
	Cisco Validated Designs	Describe hierarchical small business network designs.
	Scalable Networks	Explain considerations for designing a scalable network.
	Switch Hardware	Explain how switch hardware features support network requirements.
	Router Hardware	Describe the types of routers available for small to-medium-sized business networks.
Module	**Topic**	**Objective**
Network Troubleshooting		Troubleshoot enterprise networks.
	Network Documentation	Explain how network documentation is developed and used to troubleshoot network issues.
	Troubleshooting Process	Describe the general troubleshooting process.
	Isolate the Issue Using Layered Models	Compare troubleshooting methods that use a systematic, layered approach.
	Troubleshooting Tools	Describe different networking troubleshooting tools.
	Symptoms and Causes of Network Problems	Determine the symptoms and causes of network problems using a layered model.
	Troubleshooting IP Connectivity	Troubleshoot a network using the layered model.
Module	**Topic**	**Objective**
Network Virtualization		Explain the purpose and characteristics of network virtualization.
	Cloud Computing	Explain the importance of cloud computing.
	Virtualization	Explain the importance of virtualization.
	Virtual Network Infrastructure	Describe the virtualization of network devices and services.
	Software-Defined Networking	Describe software-defined networking.
	Controllers	Describe controllers used in network programming.
Module	**Topic**	**Objective**
Network Automation		Explain how network automation is enabled through RESTful APIs and configuration management tools.
	Automation Overview	Describe automation.
	Data Formats	Compare JSON, YAML, and XML data formats.

	APIs	Explain how APIs enable computer to computer communications.
	REST	Explain how REST enables computer to computer communications.
	Configuration Management	Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack
	IBN and Cisco DNA Center	Explain how Cisco DNA center enables intent-based networking.