CCNAv7
Enterprise Networking, Security, and Automation (ENSA), Scope and Sequence

Last Updated December 10, 2019

Target Audience

The Cisco Networking Academy® CCNAv7 curriculum is designed for participants who are seeking entry-level jobs in the ICT industry or hope to fulfill prerequisites to pursue more specialized ICT skills. The CCNAv7 curriculum is presented in three courses: Introduction to Networks (ITN), Switching, Routing and Wireless Essentials (SRWE), and Enterprise Networking, Security, and Automation (ENSA). These three courses provide 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

Students are required to have successfully completed both the Introduction to Networks (ITN) and the Switching, Routing and Wireless Essentials (SRWE) courses prior to beginning this course. Learners are also expected to have the following skills:

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

CCNAv7 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 all three course offerings, learners will be prepared to take the Cisco CCNA Unified certification exam.

CCNAv7 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.

CCNAv7 includes the following features:

- There are three offerings that make up the CCNAv7 curriculum.
- The three offerings align to and cover the competencies outlined for the CCNA Certification Exam.
- Each offering 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 advanced technologies to prepare for the Cisco CCNA exam, networking-related degree programs, and entry-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.

Lab Equipment Requirements

Current designs for lab topologies leverage equipment used in previous CCNAv6 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 previous CCNAv6 is available in the CCNA Equipment List, which is located on the Cisco NetAcad Equipment Information site (https://www.netacad.com/portal/resources/equipment-information).

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 15.0 or higher, IP Base feature set.
    - Switches: Version 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.

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

The third course in the CCNAv7 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. ENSA also introduces 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.

Listed below are the current set of modules and their associated competencies outlined for this course. 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.

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

CCNAv7: 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 filter traffic.
	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.
	Configure Extended IPv4 ACLs	Configure extended IPv4 ACLs to filter traffic according to networking requirements.

Module	Topic	Objective
NAT for IPv4		Configure 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.
	NAT64	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.
	Traditional WAN Connectivity	Compare traditional WAN connectivity options.
	Modern WAN Connectivity	Compare modern WAN connectivity options.
	Internet-Based Connectivity	Compare internet-based WAN connectivity options.
Module	**Topic**	**Objective**
VPN and IPsec Concepts		Explain how VPNs and IPsec 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 protocols to manage the network.
	Device Discovery with CDP	Use CDP to map a network topology.
	Device Discovery with LLDP	Use LLDP to map a network topology.
	NTP	Implement NTP between an NTP client and NTP server.
	SNMP	Explain SNMP operation.
	Syslog	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 of an IOS system image.
Module	**Topic**	**Objective**
Network Design		Explain the characteristics of scalable network architectures.
	Hierarchical Networks	Explain how data, voice, and video are converged in a switched network.
	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	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.