CCNP Enterprise: Core Networking (ENCOR) - Scope and Sequence

Last Updated March 13, 2020

Target Audience

The Cisco Networking Academy® CCNP Enterprise curriculum is designed for participants who are seeking professional-level jobs in the ICT industry, or hope to fulfill prerequisites to pursue other CCNP or CCIE certifications. The entire curriculum is appropriate for learners at many education levels and types of institutions, including career and technical schools, secondary schools, universities, colleges and community centers.

Prerequisites

While there are no stated prerequisites for this offering, progression through this course is increased when learners have the following skills:

- High school reading level
- CCNA or equivalent knowledge and skills

CCNP Enterprise v8 Curriculum Description

In this curriculum, Cisco Networking Academy™ participants learn, apply, and practice CCNP Enterprise knowledge and skills through a series of in-depth hands-on experiences that reinforce their learning. The CCNP Enterprise v8 curriculum is presented in two courses that provide integrated and comprehensive coverage of professional-level networking technologies. Upon completion of each course, learners will be prepared to take the certification exam associated with that course. The two course are as follows:

- **CCNP Enterprise: Core Networking (CCNP ENCOR v8)** - aligns to the Cisco Press *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide* and the Implementing Cisco Enterprise Network Core Technologies (ENCOR 350-401) certification exam. The ENCOR course includes implementation of core enterprise network technologies including dual stack (IPv4 and IPv6) architecture, virtualization, infrastructure, network assurance, security, and automation.

- **CCNP Enterprise: Advanced Routing (CCNP ENARSI v8)** - aligns to the Cisco Press *CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide* and the Implementing Cisco Enterprise Advanced Routing and Services (ENARSI 300-410) certification exam. ENARSI includes implementation and troubleshooting of advanced routing technologies and services including Layer 3, VPN services, infrastructure security, infrastructure services, and infrastructure automation.

  These two courses and the corresponding certification exams align to the overall CCNP Enterprise certification. Both of these courses provide learners extensive opportunities for hands-on practical experience and career skills development.

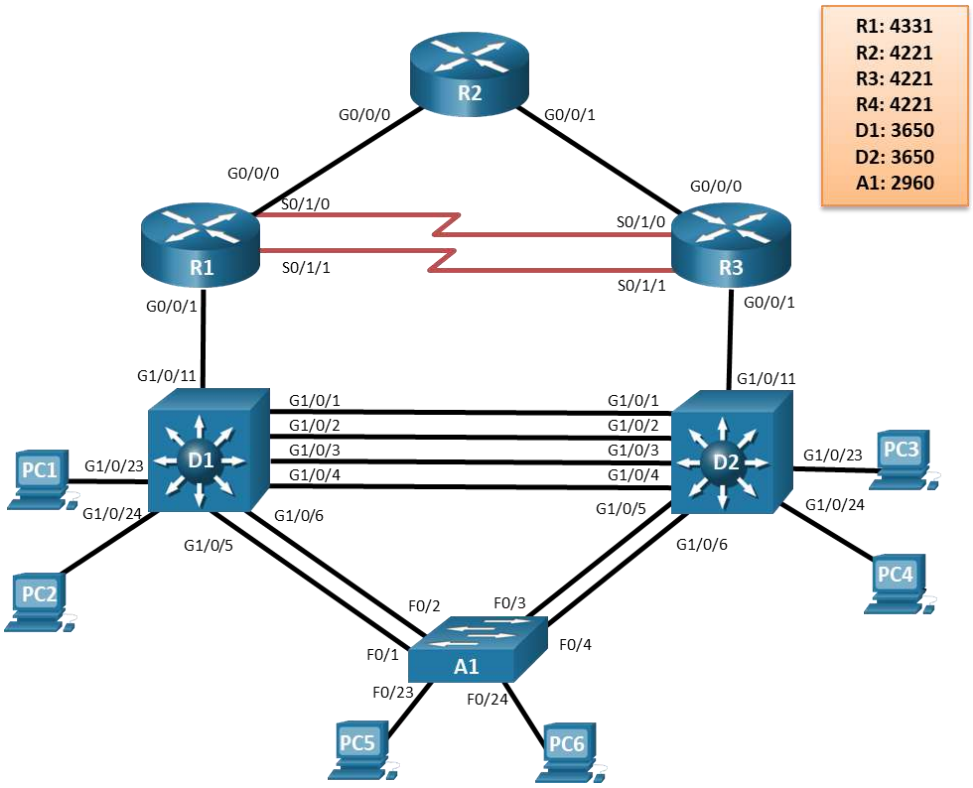
The CCNP Enterprise v8 curriculum includes the following features:

- Primary source of content for the learner is the Cisco Press Official Cert Guides.
- Assessments and practice activities are focused on specific certification competencies to increase retention.
- Embedded assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
- Hands-on labs help students develop critical thinking and complex problem-solving skills.
- Cisco Packet Tracer simulation-based learning activities are added as **optional** instructor resources to support review of CCNA skills.
- Video demonstrations give insight into complex workflows and processes and provides exposure to advance networking tools and operations.

Lab Equipment Requirements

Detailed equipment information, including descriptions and part numbers is available in the CCNP Enterprise Equipment List, which is located on the Cisco NetAcad Equipment Information site (https://www.netacad.com/portal/resources/equipment-information). The labs in the CCNP Enterprise curriculum use the following topology and equipment:

CCNP Enterprise Baseline Physical Topology (for both ENCOR and ENARSI)



Baseline Equipment Bundle:

- 3x Cisco 4221 with SEC license (2 with NIM-2T)
- 2x Cisco Catalyst 3650 Switches (WS-C3650-24TS-E)
- 1x Cisco Catalyst 2960+ Switch (WS-C2960+24TC-L)
- Ethernet cables as shown in the topology
- 2x CAB-SS-V35MT= (10' DTE Serial Cable)
- 2x CAB-SS-V35FC= (10' DCE Serial Cable)
- PCs - minimum system requirements
    - CPU: Intel Pentium 4, 2.53 GHz or equivalent •
    - Operating Systems, such as Microsoft Windows, Linux, and Mac OS•
    - 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

Software:

- Cisco IOS versions:
    - Routers: Version IOS-XE 16.9.4 or higher, universal feature set.
    - Layer 3 Switches: Version IOS-XE 16.9.4 or higher, ipservices feature set.
    - Layer 2 Switches: Version IOS 15.2.7 or higher, lanbaseK9 feature set
- Packet Tracer v7.3 (optional for CCNA skills review activities)

- Open-source server software for various services and protocols, such as HTTP, DHCP, FTP, TFTP, etc.
- Terminal emulation and SSH client software, such as Tera Term and PuTTy for lab PCs.
- Oracle VirtualBox, most recent version.
- Wireshark version: latest stable version
- Terminal emulation software for the installed PC operating system

CCNP Enterprise: Core Networking (ENCOR) Outline

Listed below are the current set of chapters and their associated competencies outlined for this course. Each chapter aligns one-to-one to a chapter in the Cisco Press *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*. The size of the chapter will depend on the depth of knowledge and skill needed to master the competencies in the associated chapter.

No.	Chapter Title	Topic	Objective
1	Packet Forwarding		Compare hardware and software switching mechanisms.
		Network Device Communication	Explain how L2 and L3 devices forward traffic.
		Forwarding Architectures	Explain the process of hardware and software Cisco Express Forwarding.
2	Spanning Tree Protocol		Configure spanning tree protocol in a switched environment.
		Spanning Tree Protocol (STP) Fundamentals	Explain the purpose of the spanning tree protocol in a switched LAN environment with redundant inter-switch links.
		Rapid Spanning Tree Protocol (RSTP)	Explain how Rapid PVST+ operates.
3	Advanced Spanning Tree		Configure STP with protection mechanisms.
		STP Topology Tuning	Explain how to modify the root bridge to control the topology.
		Additional STP Protection Mechanisms	Configure BPDU Guard and LoopGuard to protect an STP installation.
4	Multiple Spanning Tree Protocol		Configure multiple versions of the spanning tree protocol.
		Multiple Spanning Tree Protocol (MST)	Configure multiple versions of the spanning tree protocol.
5	VLAN Trunks and EtherChannel Bundles		Configure multiple versions of the spanning tree protocol.
		VLAN Trunking Protocol (VTP)	Troubleshoot VLAN and trunk configurations in a switched network.
		Dynamic Trunking Protocol (DTP)	Configure Dynamic Trunking Protocol
		EtherChannels	Configure EtherChannel.
6	IP Routing Essentials		Configure routers using different algorithms to determine the best path.
		Routing Protocol Overview	Compare algorithms used by different routing protocols to forward packets.
		Path Selection	Explain how routers determine the best path.

		Static Routing	Configure static, default, and floating static routes.
7	EIGRP		Configure EIGRP to improve network performance.
		EIGRP Fundamentals	Describe the basic features of EIGRP.
		Path Metric Calculation	Describe the algorithm used by EIGRP to determine the best path.
		Failure Detection and Timers	Explain how different types of packets are used to establish and maintain an EIGRP neighbor relationship.
		Summarization	Configure EIGRP autosummarization.
8	OSPF		Implement multiarea OSPFv2.
		OSPF Fundamentals	Explain the features and characteristics of the OSPF routing protocol.
		OSPF Configuration	Configure single-area OSPFv2 in a point-to-point network.
		Default Route Advertisement	Configure OSPF to propagate a default route.
		Common OSPF Optimizations	Configure OSPF to improve network performance.
9	Advanced OSPF		Use advanced OSPF features to optimize network performance.
		Areas	Explain why multiarea OSPF is used.
		Link-State Announcements	Explain how multiarea OSPFv2 uses link state advertisements.
		Discontiguous Network	Explain how to connect discontiguous areas in OSPFv2.
		OSPF Path Selection	Explain how OSPF determines the best path.
		Summarization of Routes	Configure summarization between OSPF areas.
		Route Filtering	Explain how to filter routes in OSPFv2 to improve performance.
10	OSPFv3		Implement single-area OSPFv3.
		OSPFv3 Fundamentals	Compare the characteristics and operations of OSPFv2 to OSPFv3.
		OSPFv3 Configuration	Configure single-area OSPFv3.
		IPv4 Support on OSPFv3	Explain how IPv4 traffic is supported in OSPFv3.

11	BGP		Configure eBGP in a single-homed remote access network.
		BGP Fundamentals	Describe basic BGP features.
		Basic BGP Configuration	Configure an eBGP branch connection.
		Route Summarization	Configure summarization in BGP to improve performance.
		Multiprotocol BGP for IPv6	Configure BGP to support and summarize IPv6 traffic.
12	Advanced BGP		Explain how advanced BGP features improve performance.
		BGP Multihoming	Explain how BGP multihoming to ISPs provides resilient internet service.
		Conditional Matching	Explain how ACLs and prefix matching assist in fine tuning the BGP routing process.
		Route-maps	Explain the purpose of Route-maps in BGP.
		BGP Route Filtering and Manipulation	Explain how BGP uses route filtering and manipulation to improve performance.
		BGP Communities	Explain the function and purpose of BGP communities.
		Understanding BGP Path Selection	Explain what processes are used by BGP for path selection.
13	Multicast		Explain the concepts and protocols that are required to understand multicast operation.
		Multicast Fundamentals	Describe the overall concepts and need for multicasting.
		Multicast Addressing (L2 & L3)	Describe the address scopes used by multicast to operate at layer 2 and layer 3.
		Internet Group Management Protocol	Explain how IGMP v2 and IGMP v3 allow multicast groups to start receiving multicast traffic.
		Protocol Independent Multicast	Explain the concepts, operation and features of the multicast routing protocol PIM.
		Rendezvous Points	Describe the purpose, function, and operation of a rendezvous point in the multicast network.
14	QoS		Explain the mechanisms used by QoS to ensure transmission quality.

		The Need for QoS	Explain how network transmission characteristics impact quality.
		QoS Models	Describe the different QoS models.
		Classification and Marking	Describe how QoS classifies and marks traffic based on conditioning policies.
		Policing and Shaping	Explain how policing and shaping algorithms affect excess IP traffic.
		Congestion Management and Avoidance	Explain how congestion management and avoidance tools are used to avoid network congestion.
15	IP Services		Configure IP services for managed networks that provide redundancy, address translation and synchronization.
		Time Synchronization	Implement NTP between an NTP client and NTP server.
		First Hop Redundancy Protocols (FHRP)	Configure HSRP using Cisco IOS commands.
		Network Address Translation (NAT)	Configure NAT services on the edge router to provide IPv4 address scalability.
16	Overlay Tunnels		Configure overlay tunnels to secure site-to-site and remote access connectivity.
		Generic Routing Encapsulation (GRE) Tunnels	Configure a site-to-site GRE tunnel.
		IPsec Fundamentals	Explain how the IPsec framework is used to secure network traffic.
		Cisco Location/ID Separation Protocol (LISP)	Explain how the routing architecture, LISP, addresses internet routing scalability problems.
		Virtual Extensible Local Area Network (VXLAN)	Explain how a virtual extensible local area network
17	Wireless Signals and Modulation		Explain the theory of wireless signals and the methods used to carry data wirelessly.
		Understanding Basic Wireless Theory	Describe the technology and characteristics of radio frequency signals
		Carrying Data Over an RF Signal	Explain methods used to carry data over an RF signal.
		Maintaining AP-Client Compatibility	Identify the standards and methods used to maintain AP to client compatibility.

		Using Multiple Radios to Scale Performance	Explain how to use multiple radio components to scale performance.
		Maximizing the AP-Client Throughput	Explain techniques used to maximize AP to client throughput.
18	Wireless Architecture Infrastructure		Select appropriate wireless topologies and antennas to allow APs to pair with WLCs in an enterprise network.
		Wireless LAN Topologies	Compare how APs operate in autonomous and lightweight mode.
		Pairing Lightweight APs and WLCs	Explain how lightweight APs pair with WLCs.
		Leveraging Antennas for Wireless Coverage	Select appropriate antennas for APs based on requirements.
19	Understanding Wireless Roaming and Location Services		Explain how to configure a wireless network to support and manage wireless roaming.
		Roaming Overview	Explain how mobile clients roam between autonomous APs and intracontrollers.
		Roaming Between Centralized Controllers	Explain L2 and L3 roaming strategies.
		Locating Devices in a Wireless Network	Describe techniques and business rationale for locating devices in a wireless network.
20	Authenticating Wireless Clients		Compare different methods to authenticate wireless clients before gaining access to the wireless network.
		Open Authentication	Explain when wireless clients should access a network using open authentication.
		Authenticating with a Pre-Shared Key	Explain how to configure secure wireless connections on a WLAN using authentication with a pre-shared key.
		Authenticating with EAP	Explain how to configure secure wireless connections on a WLAN using authentication with EAP.
		Authenticating with WebAuth	Explain how to configure secure wireless connections on a WLAN using authentication with WebAuth.
21	Troubleshooting Wireless Connectivity		Troubleshoot wireless connectivity issues using tools and strategies.
		Troubleshooting Client Connectivity from the WLC	Troubleshoot connectivity issues with a single wireless client.

		Troubleshooting Connectivity Problems at the AP	Explain how to troubleshoot connectivity issues at the AP.
22	Enterprise Network Architecture		Explain the characteristics of scalable network architectures.
		Hierarchical LAN Design Model	Describe the three layers of a hierarchical network and how they are used in network design.
		Enterprise Network Architecture Options	Explain how enterprise campus architectures can be used to scale from a small environment to a large campus-size network.
23	Fabric Technologies		Explain how fabric networks allow traditional networks to be more manageable, flexible, secure, and scalable.
		The Need for SD-Access	Explain how SD-Access is effective for configuration and maintenance in growing and ever-changing networks.
		What is SD-Access?	Describe the two main components of SD-Access.
		SD-Access Architecture	Explain the functions of the four layers of SD-Access architecture.
		What is Software-Defined WAN (SD-WAN)?	Describe the benefits of utilizing an SD-WAN.
		Cisco SD-WAN Architecture	Describe Cisco's current solutions for SD-WAN.
		Cisco SD-WAN Cloud OnRamp	Explain how the SD-WAN Cloud ONRamp solution addresses optimal cloud SaaS application access and IaaS connectivity.
24	Network Assurance		Troubleshoot an enterprise network using common tools and techniques.
		Network Diagnostic Tools	Troubleshoot common and advanced network problems.
		NetFlow	Configure NetFlow to monitor traffic in a business network.
		Switched Port Analyzer (SPAN) Technologies	Explain the features and characteristics of SPAN.
		Local SPAN	Explain how to configure SPAN to capture packets on local switch ports.
		Remote SPAN (RSPAN)	Compare the use of local SPAN and RSPAN.

		Encapsulated Remote SPAN (ERSPAN)	Explain how to configure ERSPAN to monitor traffic in one area of the network and route the SPAN traffic to a traffic analyzer in another area of the network.
		IP SLA	Use an ICMP echo-based IP SLA to troubleshoot network connectivity issues.
		Cisco DNA Center with Assurance	Explain how Cisco DNA center enable intent-based networking.
25	Secure Access Control		Compare secure solutions for different places in the network
		Network Security Design for Threat Defense	Describe Cisco SAFE, a security architectural framework, that helps design secure solutions for PINs.
		Next-Generation Endpoint Security	Explain how to design endpoint security that will detect the rapidly evolving threats to organizations.
		Network Access Control (NAC)	Compare current and next generation network access control technologies.
26	Network Device Access Control and Infrastructure Security		Configure network access control using tools and features that provide device and infrastructure security.
		Access Control Lists (ACLs)	Verify the functionality of a configured ACL in relation to the network topology.
		Terminal Lines and Password Protection	Explain techniques that secure and control access to VTY lines on network devices.
		Authentication, Authorization, and Accounting (AAA)	Configure access control using the local database and AAA server.
		Zone-Based Firewalls (ZBFWs)	Explain how to configure zone-based firewalls to provide stateful network security.
		Control Plane Policing (CoPP)	"Configure ACLs with CoPP policies that protect the CPU from unexpected extreme rates of traffic.
		Device Hardening	Configure network devices with device hardening features to mitigate security threats.
27	Virtualization		Explain the purpose and characteristics of network and server virtualization.
		Server Virtualization	Describe the virtualization of network devices and services.

		Network Functions Virtualization	Explain how the Network Functions Virtualization
28	Foundational Network Programmability Concepts		Explain common network programmability concepts and programmatic methods of management.
		Command Line Interface – CLI	Explain the pros and cons of using the CLI to manage devices on a network.
		Application Programming Interface – API	Explain how APIs enable computer to computer communications.
		Tools and Resources	Describe tools and resources related to using APIs and REST functions.
		Data Formats (XML and JSON)	Compare JSON and XML data formats.
		Cisco DNA Center APIs	Explain how Cisco DNA center enable intent-based networking.
		Cisco vManage APIs	Compare the use of vManage APIs to Cisco DNA Center APIs.
		Data Models and Supporting Protocols	Describe data models and tools used in a programmatic approach.
		Cisco DevNet	Explain how DevNet encourages communities of network programmers.
		GitHub	Explain how GitHub tracks changes in your files and facilitates collaboration and code sharing.
		Basic Python Components and Scripts	Use Python to access and manipulate values in lists and dictionaries.
29	Introduction to Automation Tools		Explain the benefits and operation of various automation tools.
		Embedded Event Manager (EEM)	Explain how the Embedded Event Manager is used to automate configuration, troubleshooting, and data collection.
		Agent-based vs. Agentless Management Tools	Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack.