Implementing and Operating Cisco Enterprise Network Core Technologies v1.3 (ENCOR)

Price	Duration	Delivery Methods
$3,195.00	5 Daytime Classes or 10 Evening Classes	Virtual, Private Group,

CAREER SKILLS+™

The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.3 training gives you the knowledge and skills needed to install, configure, operate, and troubleshoot an enterprise network and introduces you to overlay network design by using SD-Access and SD-WAN solutions. You'll also learn to understand and implement security principles and automation and programmability within an enterprise network. This course also prepares you for the 350-401 Implementing Cisco Enterprise Network Core Technologies (ENCOR) exam.

Who Should Attend

Mid-level network engineers
Network administrators
Network support technicians
Help desk technicians

Course Objectives

- Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers
- Compare and contrast the various hardware and software switching mechanisms and operation while defining the Ternary

Content Addressable Memory (TCAM) and Content Addressable Memory (CAM) along with process switching, fast switching, and Cisco Express Forwarding concepts
• Troubleshoot Layer 2 connectivity using VLANs and trunking
Implement redundant switched networks using Spanning Tree Protocol
Troubleshoot link aggregation using Etherchannel
• Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP)
• Implement and optimize Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types and areas, summarization, and route filtering for IPv4 and IPv6
• Implement External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
Implement network redundancy using protocols such as Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)
•Implement internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT)
•Describe the virtualization technology of servers, switches, and the various network devices and components
Implement overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP)
• Describe the components and concepts of wireless networking, including Radio Frequency (RF) and antenna characteristics, and define the specific wireless standards
• Describe the various wireless deployment models available, including autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture
• Describe wireless roaming and location services
• Describe how APs communicate with WLCs to obtain software, configurations, and centralized management
Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC
• Troubleshoot wireless client connectivity issues using various available tools
• Troubleshoot Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management

Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager
• Explain the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting
• Configure secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP
• Implement scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits
• Describe the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other security features
• Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience
• Describe the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways
• Define the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane
• Describe the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points
• Describe the concepts and features of Quality of Service (QoS), and describe the need within the enterprise network
• Explain basic Python components and conditionals with script writing and analysis
• Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF
• Describe APIs in Cisco DNA Center and Manage

Agenda

• Explaining the Rationale for IPv6

- Evaluating IPv6 Features and Benefits
- Understanding Market Drivers
- Understanding the IPv6 Addressing Architecture
- Describing the IPv6 Header Format
- Enabling IPv6 on Hosts
- Enabling IPv6 on Cisco Routers
- Using ICMPv6 and Neighbor Discovery
- Troubleshooting IPv6
- IPv6 Mobility
- Describing DNS in an IPv6 Environment
- Understanding DHCPv6 Operations
- Understanding QoS Support in an IPv6 Environment
- Using Cisco IOS Software Features
- Routing with RIPng
- Examining OSPFv3
- Examining Integrated IS-IS
- Examining EIGRP for IPv6
- Understanding MP-BGP
- Configuring IPv6 Policy-Based Routing
- Configuring FHRP for IPv6
- Configuring Route Redistribution
- Implementing Multicast in an IPv6 Network
- Using IPv6 MLD
- Implementing Dual-Stack
- Describing IPv6 Tunneling Mechanisms
- Configuring IPv6 ACLs
- Using IPsec, IKE, and VPNs
- Discussing Security Issues in an IPv6 Transition Environment
- Understanding IPv6 Security Practices
- Configuring Cisco IOS Firewall for IPv6
- Examining IPv6 Address Allocation
- Understanding the IPv6 Multihoming Issue
- Identifying IPv6 Enterprise Deployment Strategies
- Identifying IPv6 Service Provider Deployment
- Understanding Support for IPv6 in MPLS
- Understanding 6VPE
- Understanding IPv6 Broadband Access Services
- Planning and Implementing IPv6 in Enterprise Networks
- Planning and Implementing IPv6 in Service Provider Networks
- Planning and Implementing IPv6 in Branch Networks

Lab Outline
Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Enabling IPv6 on Hosts
- Using Neighbor Discovery
- Using Prefix Delegation
- Routing with OSPFv3
- Routing with IS-IS
- Routing with EIGRP
- Routing with BGP and MP-BGP
- Multicasting
- Implementing Tunnels for IPv6
- Configuring Advanced ACLs
- Implementing IPsec and IKE
- Configuring Cisco IOS Firewall
- Configuring 6PE and 6VPE