CCIE Enterprise Infrastructure

Introduction

Software, networking, and infrastructure grow more and more interconnected every day. Applications deliver exciting new experiences, and with intent-based networking, organizations can take advantage of automation to scale and secure their networking infrastructure. With CCIE Enterprise Infrastructure certification, your opportunities to help maximize that potential are boundless. Just ask hiring managers: 71% of them say that certifications increase their confidence in an applicant's abilities.

CCIE Enterprise Infrastructure certification helps you position yourself as a technical leader in the ever-changing landscape of networking technologies. The certification covers core technology areas and validates your end-to-end lifecycle skills in complex enterprise networks from planning and design to operating and optimizing.

Exams and Recommended Training

1. 350-401 ENCOR: Implementing and Operating Cisco Enterprise Network Core Technologies

The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.1 course gives you the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. You'll also learn to implement security principles, implement automation and programmability within an enterprise network, and how to overlay network design by using SD-Access and SD-WAN solutions.

This course helps you prepare to take the 350-401 Implementing Cisco® Enterprise Network Core Technologies (ENCOR) exam, which is part of four new certifications:

- CCNP® Enterprise
- CCIE® Enterprise Infrastructure
- CCIE Enterprise Wireless
- Cisco Certified Specialist – Enterprise Core

Duration

5 Days

Course Objectives

After taking this course, you should be able to:

- 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
- Implementation of redundant switched networks using Spanning Tree Protocol
- Troubleshooting link aggregation using Etherchannel
- Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing

Protocol (EIGRP)

- Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6
- Implementing External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
- Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)
- Implementing 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
- Implementing 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, include 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
- Troubleshooting 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 scriptwriting and analysis
- Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF
- Describe APIs in Cisco DNA Center and vManage

Prerequisites

Knowledge and skills you should have before attending this course:

- Implementation of Enterprise LAN networks
- Basic understanding of Enterprise routing and wireless connectivity
- Basic understanding of Python scripting

Target Audience

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

Course Outline

- Examining Cisco Enterprise Network Architecture
- Understanding Cisco Switching Paths
- Implementing Campus LAN Connectivity
- Building Redundant Switched Topology
- Implementing Layer 2 Port Aggregation
- Understanding EIGRP
- Implementing OSPF
- Optimizing OSPF
- Exploring EBGP
- Implementing Network Redundancy
- Implementing NAT
- Introducing Virtualization Protocols and Techniques
- Understanding Virtual Private Networks and Interfaces
- Understanding Wireless Principles
- Examining Wireless Deployment Options
- Understanding Wireless Roaming and Location Services
- Examining Wireless AP Operation
- Understanding Wireless Client Authentication
- Troubleshooting Wireless Client Connectivity
- Introducing Multicast Protocols
- Introducing QoS
- Implementing Network Services
- Using Network Analysis Tools
- Implementing Infrastructure Security
- Implementing Secure Access Control
- Understanding Enterprise Network Security Architecture
- Exploring Automation and Assurance Using Cisco DNA Center
- Examining the Cisco SD-Access Solution
- Understanding the Working Principles of the Cisco SD-WAN Solution
- Understanding the Basics of Python Programming
- Introducing Network Programmability Protocols
- Introducing APIs in Cisco DNA Center and vManage

Lab Outline

- Investigate the CAM
- Analyze Cisco Express Forwarding

- Troubleshoot VLAN and Trunk Issues
- Tuning Spanning Tree Protocol (STP) and Configuring Rapid Spanning Tree Protocol (RSTP)
- Configure Multiple Spanning Tree Protocol
- Troubleshoot EtherChannel
- Implement Multi-area OSPF
- Implement OSPF Tuning
- Apply OSPF Optimization
- Implement OSPFv3
- Configure and Verify Single-Homed EBGP
- Implementing Hot Standby Routing Protocol (HSRP)
- Configure Virtual Router Redundancy Protocol (VRRP)
- Implement NAT
- Configure and Verify Virtual Routing and Forwarding (VRF)
- Configure and Verify a Generic Routing Encapsulation (GRE) Tunnel
- Configure Static Virtual Tunnel Interface (VTI) Point-to-Point Tunnels
- Configure Wireless Client Authentication in a Centralized Deployment
- Troubleshoot Wireless Client Connectivity Issues
- Configure Syslog
- Configure and Verify Flexible NetFlow
- Configuring Cisco IOS Embedded Event Manager (EEM)
- Troubleshoot Connectivity and Analyze Traffic with Ping, Traceroute, and Debug
- Configure and Verify Cisco IP SLAs
- Configure Standard and Extended ACLs
- Configure Control Plane Policing
- Implement Local and Server-Based AAA
- Writing and Troubleshooting Python Scripts
- Explore JavaScript Object Notation (JSON) Objects and Scripts in Python
- Use NETCONF Via SSH
- Use RESTCONF with Cisco IOS XE Software

2. CCIE Enterprise Infrastructure v1.0 (Practical Exam)

The Cisco CCIE Enterprise Infrastructure (v1.0) Practical Exam is an eight-hour, hands-on exam that requires a candidate to plan, design, deploy, operate, and optimize dual-stack solutions (IPv4 and IPv6) for complex enterprise networks.

Candidates are expected to program and automate the network within their exam, as per the exam topics below.

The following topics are general guidelines for the content likely to be included in the exam. Your knowledge, skills, and abilities on these topics will be tested throughout the entire network lifecycle unless explicitly specified otherwise within this document.

Duration

8 Hours

Prerequisites

There are no formal prerequisites for CCIE Enterprise Infrastructure, but you should have a thorough understanding of the exam topics before taking the exam.

CCIE candidates are recommended to have five to seven years of experience with designing, deploying, operating, and optimizing enterprise networking technologies and solutions prior to taking the exam.

Course Outline

- Network Infrastructure
    - 1.1 Switched campus
        - 1.1.a Switch administration
            - 1.1.a i Managing MAC address table
            - 1.1.a ii Errdisable recovery
            - 1.1.a iii L2 MTU
        - 1.1.b Layer 2 protocols
            - 1.1.b i CDP, LLDP
            - 1.1.b ii UDLD
        - 1.1.c VLAN technologies
            - 1.1.c i Access ports
            - 1.1.c ii Trunk ports (802.1Q)
            - 1.1.c iii Native VLAN
            - 1.1.c iv Manual VLAN pruning
            - 1.1.c v VLAN database
            - 1.1.c vi Normal range and extended range VLANs
            - 1.1.c vii Voice VLAN
            - 1.1.c viii VTP
        - 1.1.d EtherChannel
            - 1.1.d i LACP, static
            - 1.1.d ii Layer 2, Layer 3
            - 1.1.d iii Load balancing
            - 1.1.d iv EtherChannel Misconfiguration Guard
        - 1.1.e Spanning- Tree Protocol
            - 1.1.e i PVST+, Rapid PVST+, MST
            - 1.1.e ii Switch priority, port priority, path cost, STP timers
            - 1.1.e iii PortFast, BPDU Guard, BPDU Filter
            - 1.1.e iv Loop Guard, Root Guard

    - 1.2 Routing Concepts
        - 1.2.a Administrative distance
        - 1.2.b VRF-lite
        - 1.2.c Static routing
        - 1.2.d Policy Based Routing
        - 1.2.e VRF aware routing with any routing protocol
        - 1.2.f Route filtering with any routing protocol
        - 1.2.g Manual summarization with any routing protocol
        - 1.2.h Redistribution between any pair of routing protocols
        - 1.2.i Routing protocol authentication
        - 1.2.j Bidirectional Forwarding Detection

    - 1.3 EIGRP
        - 1.3.a Adjacencies
        - 1.3.b Best path selection
            - 1.3.b i RD, FD, FC, successor, feasible successor
            - 1.3.b ii Classic Metrics and Wide Metrics
        - 1.3.c Operations
            - 1.3.c i General operations
            - 1.3.c ii Topology table
            - 1.3.c iii Packet types
            - 1.3.c iv Stuck In Active
            - 1.3.c v Graceful shutdown
        - 1.3.d EIGRP load-balancing
            - 1.3.d i Equal-cost
            - 1.3.d ii Unequal-cost
            - 1.3.d iii Add-path

        - 1.3.e EIGRP Named Mode
        - 1.3.f Optimization, convergence and scalability
            - 1.3.f i Fast convergence requirements
            - 1.3.f ii Query propagation boundaries
            - 1.3.f iii IP FRR (single hop)
            - 1.3.f iv Leak-map with summary routes
            - 1.3.f v EIGRP stub with leak map

    - 1.4 OSPF (v2 and v3)
        - 1.4.a Adjacencies
        - 1.4.b Network types, area types
        - 1.4.c Path preference
        - 1.4.d Operations
            - 1.4.d i General operations
            - 1.4.d ii Graceful shutdown
            - 1.4.d iii GTSM (Generic TTL Security Mechanism)
        - 1.4.e Optimization, convergence and scalability
            - 1.4.e i Metrics
            - 1.4.e ii LSA throttling, SPF tuning, fast hello
            - 1.4.e iii LSA propagation control (area types)
            - 1.4.e iv Stub router
            - 1.4.e v Loop-free alternate
            - 1.4.e vi Prefix suppression

    - 1.5 BGP
        - 1.5.a IBGP and EBGP peer relationships
            - 1.5.a i Peer-group/update-group, template
            - 1.5.a ii Active, passive
            - 1.5.a iii Timers
            - 1.5.a iv Dynamic neighbors
            - 1.5.a v 4-bytes AS numbers
            - 1.5.a vi Private AS
        - 1.5.b Path selection
            - 1.5.b i Attributes
            - 1.5.b ii Best path selection algorithm
            - 1.5.b iii Load-balancing
        - 1.5.c Routing policies
            - 1.5.c i Attribute manipulation
            - 1.5.c ii Conditional advertisement
            - 1.5.c iii Outbound Route Filtering
            - 1.5.c iv Standard and extended communities
            - 1.5.c v Multi-homing
        - 1.5.d AS path manipulations
            - 1.5.d i local-AS, allowas-in, remove-private-as
            - 1.5.d ii Prepend
            - 1.5.d iii Regexp
        - 1.5.e Convergence and scalability
            - 1.5.e i Route reflector
            - 1.5.e ii Aggregation, as-set
        - 1.5.f Other BGP features
            - 1.5.f i Multipath, add-path
            - 1.5.f ii Soft reconfiguration, Route Refresh

    - 1.6 Multicast
        - 1.6.a Layer 2 multicast
            - 1.6.a i IGMPv2, IGMPv3
            - 1.6.a ii IGMP Snooping, PIM Snooping
            - 1.6.a iii IGMP Querier

- 1.6.a iv IGMP Filter
- 1.6.a v MLD

- 1.6.b Reverse path forwarding check
- 1.6.c PIM
  - 1.6.c i Sparse Mode
  - 1.6.c ii Static RP, BSR, AutoRP
  - 1.6.c iii Group to RP Mapping
  - 1.6.c iv Bidirectional PIM
  - 1.6.c v Source-Specific Multicast
  - 1.6.c vi Multicast boundary, RP announcement filter
  - 1.6.c vii PIMv6 Anycast RP
  - 1.6.c viii IPv4 Anycast RP using MSDP
  - 1.6.c ix Multicast multipath

- Software Defined Infrastructure
  - 2.1 Cisco SD Access
    - 2.1.a Design a Cisco SD Access solution
      - 2.1.a i Underlay network (IS-IS, manual/PnP)
      - 2.1.a ii Overlay fabric design (LISP, VXLAN, Cisco TrustSec)
      - 2.1.a iii Fabric domains (single-site and multi-site using SD-WAN transit)
    - 2.1.b Cisco SD Access deployment
      - 2.1.b i Cisco DNA Center device discovery and device management
      - 2.1.b ii Add fabric node devices to an existing fabric
      - 2.1.b iii Host onboarding (wired endpoints only)
      - 2.1.b iv Fabric border handoff
    - 2.1.c Segmentation
      - 2.1.c i Macro-level segmentation using VNs
      - 2.1.c ii Micro-level segmentation using SGTs (using Cisco ISE)
    - 2.1.d Assurance
      - 2.1.d i Network and client health (360)
      - 2.1.d ii Monitoring and troubleshooting

  - 2.2 Cisco SD-WAN
    - 2.2.a Design a Cisco SD-WAN solution
      - 2.2.a i Orchestration plane (vBond, NAT)
      - 2.2.a ii Management plane (vManage)
      - 2.2.a iii Control plane (vSmart, OMP)
      - 2.2.a iv Data plane (vEdge/cEdge)
    - 2.2.b WAN edge deployment
      - 2.2.b i Onboarding new edge routers
      - 2.2.b ii Orchestration with zero-touch provisioning/Plug-And-Play
      - 2.2.b iii OMP
      - 2.2.b iv TLOC
    - 2.2.c Configuration templates
    - 2.2.d Localized policies
    - 2.2.e Centralized policies

- Transport Technologies and Solutions
  - 3.1 MPLS
    - 3.1.a Operations
      - 3.1.a i Label stack, LSR, LSP
      - 3.1.a ii LDP
      - 3.1.a iii MPLS ping, MPLS traceroute
    - 3.1.b L3VPN
      - 3.1.b i PE-CE routing
      - 3.1.b ii MP-BGP VPNv4/VPNv6
      - 3.1.b iii Extranet (route leaking)

- 3.2 DMVPN
  - 3.2.a Troubleshoot DMVPN Phase 3 with dual-hub
    - 3.2.a i NHRP
    - 3.2.a ii IPsec/IKEv2 using pre-shared key
    - 3.2.a iii Per-Tunnel QoS
  - 3.2.b Identify use-cases for FlexVPN
    - 3.2.b i Site-to-site, Server, Client, Spoke-to-Spoke
    - 3.2.b ii IPsec/IKEv2 using pre-shared key
    - 3.2.b iii MPLS over FlexVPN

- Infrastructure Security and Services
  - 4.1 Device Security on Cisco IOS XE
    - 4.1.a Control plane policing and p rotection
    - 4.1.b AAA

  - 4.2 Network Security
    - 4.2.a Switch security features
      - 4.2.a i VACL, PACL
      - 4.2.a ii Storm control
      - 4.2.a iii DHCP Snooping, DHCP option 82
      - 4.2.a iv IP Source Guard
      - 4.2.a v Dynamic ARP Inspection
      - 4.2.a vi Port Security
      - 4.2.a vii Private VLAN
    - 4.2.b Router security features
      - 4.2.b i IPv6 Traffic Filters
      - 4.2.b ii IPv4 Access Control Lists
      - 4.2.b iii Unicast Reverse Path Forwarding
    - 4.2.c IPv6 infrastructure security features
      - 4.2.c i RA Guard
      - 4.2.c ii DHCP Guard
      - 4.2.c iii Binding table
      - 4.2.c iv Device tracking
      - 4.2.c v ND Inspection/Snooping
      - 4.2.c vi Source Guard
    - 4.2.d IEEE 802.1X Port-Based Authentication
      - 4.2.d i Device roles, port states
      - 4.2.d ii Authentication process
      - 4.2.d iii Host modes

  - 4.3 System Management
    - 4.3.a Device management
      - 4.3.a i Console and VTY
      - 4.3.a ii SSH, SCP
      - 4.3.a iii RESTCONF, NETCONF
    - 4.3.b SNMP
      - 4.3.b i v2c
      - 4.3.b ii v3
    - 4.3.c Logging
      - 4.3.c i Local logging, syslog, debugs, conditional debugs
      - 4.3.c ii Timestamps

  - 4.4 Quality of Service
    - 4.4.a End to end L3 QoS using MQC
      - 4.4.a i DiffServ
      - 4.4.a ii CoS and DSCP Mapping
      - 4.4.a iii Classification
      - 4.4.a iv Network Based Application Recognition (NBAR)

- 4.4.a v Marking using IP Precedence, DSCP, CoS
- 4.4.a vi Policing, shaping
- 4.4.a vii Congestion management and avoidance
- 4.4.a viii HQoS, Sub-rate Ethernet Link

- 4.5 Network Services
  - 4.5.a First-Hop Redundancy Protocols
    - 4.5.a i HSRP, GLBP, VRRP
    - 4.5.a ii Redundancy using IPv6 RS/RA
  - 4.5.b Network Time Protocol
    - 4.5.b i Master, client
    - 4.5.b ii Authentication
  - 4.5.c DHCP on Cisco IOS
    - 4.5.c i Client, server, relay
    - 4.5.c ii Options
    - 4.5.c iii SLAAC/DHCPv6 interaction
    - 4.5.c iv Stateful, stateless DHCPv6
    - 4.5.c v DHCPv6 Prefix Delegation
  - 4.5.d IPv4 Network Address Translation
    - 4.5.d i Static NAT, PAT
    - 4.5.d ii Dynamic NAT, PAT
    - 4.5.d iii Policy-based NAT, PAT
    - 4.5.d iv VRF aware NAT, PAT
    - 4.5.d v IOS-XE VRF-Aware Software Infrastructure (VASI) NAT

- 4.6 Network optimization
  - 4.6.a IP SLA
    - 4.6.a i ICMP probes
    - 4.6.a ii UDP probes
    - 4.6.a iii TCP probes
  - 4.6.b Tracking object
  - 4.6.c Flexible Netflow

- 4.7 Network operations
  - 4.7.a Traffic capture
    - 4.7.a i SPAN
    - 4.7.a ii RSPAN
    - 4.7.a iii ERSPAN
    - 4.7.a iv Embedded Packet Capture
  - 4.7.b Cisco IOS-XE troubleshooting tools
    - 4.7.b i Packet Trace
    - 4.7.b ii Conditional debugger (debug platform condition)

- Infrastructure Automation and Programmability
  - 5.1 Data encoding formats
    - 5.1.a JSON
    - 5.1.b XML

  - 5.2 Automation and scripting
    - 5.2.a EEM applets
    - 5.2.b Guest shell
      - 5.2.b i Linux environment
      - 5.2.b ii CLI Python module
      - 5.2.b iii EEM Python module

  - 5.3 Programmability
    - 5.3.a Interaction with vManage API
      - 5.3.a i Python requests library and Postman

        - 5.3.a ii Monitoring endpoints
        - 5.3.a iii Configuration endpoints
    - 5.3.b Interaction with Cisco DNA Center API
        - 5.3.b i HTTP request (GET, PUT, POST) via Python requests library and Postman
    - 5.3.c Interaction with Cisco IOS XE API
        - 5.3.c i Via NETCONF/YANG using Python ncclient library
        - 5.3.c ii Via RESTCONF/YANG using Python requests library and Postman
    - 5.3.d Deploy and verify model-driven telemetry
        - 5.3.d i Configure on-change subscription using gRPC