

CCIE Enterprise Wireless

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 wireless networking infrastructure. With CCIE Enterprise Wireless 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 Wireless certification helps you prove your skills in the ever-changing landscape of wireless technologies. The certification covers core technology areas and validates your end-to-end lifecycle skills in complex enterprise wireless 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 scripting 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 EIGRP
- 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 Wireless (v1.0) Exam Topics (Practical Exam)

The Cisco CCIE Enterprise Wireless v1.0 Practical Exam is an eight-hour, hands-on exam that requires a candidate to plan, design, implement, operate, and optimize complex Enterprise Wireless networks.

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

The following topics are general guidelines for the content likely to be included on 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 Wireless, 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 wireless technologies and solutions prior to taking the exam.

Course Outline

- Radio Frequency and Standards
 - 1.1 IEEE 802.11 standards and protocols
 - 1.2 RF Design / Site survey
 - 1.2.a Define the tasks/goals for a preliminary site survey
 - 1.2.b Conduct the site survey
 - 1.2.c Determine AP quantity, placement and antenna type
 - 1.3 Indoor and outdoor RF deployments
 - 1.3.a Coverage
 - 1.3.b Throughput
 - 1.3.c Voice
 - 1.3.d Location
 - 1.3.e High Density / Very High Density
 - 1.4 RF operational models
 - 1.4.a Radio resource management (Auto-RF, manual, hybrid, Flexible Radio Assignment, TPC and DCA, CHD)
 - 1.4.b Channel use (Co-channel, radar, non-WiFi interference, Dynamic Bandwidth Selection)
 - 1.4.c Power level, overlap
 - 1.4.d RF profiles
 - 1.4.e Data rates
 - 1.4.f RX-SOP
 - 1.4.g CleanAir and EDRRM
 - 1.4.h Air Time Fairness (ATF)
- Enterprise Wired Campus
 - 2.1 Layer 2 technologies to support wireless deployments
 - 2.1.a VLANs
 - 2.1.b STP
 - 2.1.c Etherchannel
 - 2.1.d CDP, LLDP
 - 2.2 Data/Control plane technologies to support a SD-Access wireless deployment
 - 2.2.a VXLAN and LISP
 - 2.2.b VRFs
 - 2.3 AP powering options
 - 2.4 IPv4 and IPv6 connectivity
 - 2.4.a Subnetting
 - 2.4.b Static and inter-VLAN routing
 - 2.5 Multicast on the switching infrastructure
 - 2.5.a PIM
 - 2.5.b Basic IGMP (including IGMP snooping)
 - 2.5.c MLD
 - 2.6 QoS on the switching infrastructure
 - 2.6.a MQC
 - 2.6.b MLS QoS
 - 2.7 Services to support a wireless deployment
 - 2.7.a DNS
 - 2.7.b DHCPv4 / DHCPv6
 - 2.7.c NTP, SNTP
 - 2.7.d SYSLOG
 - 2.7.e SNMP
- Enterprise Wireless Network
 - 3.1 WLC interfaces and ports
 - 3.2 Lightweight APs
 - 3.2.a AP modes
 - 3.2.b AP Logging

- 3.2.c AP CLI troubleshooting
 - 3.2.d AP level configuration settings
 - 3.2.e WLC discovery and AP join process
 - 3.2.f AP join profile
 - 3.3 High availability, redundancy, and resilience
 - 3.3.a SSO
 - 3.3.b N+1, N+N
 - 3.3.c Patching and rolling upgrades for IOS-XE
 - 3.3.d ISSU
 - 3.4 Wireless segmentation with profiles and groups
 - 3.4.a RF profiles
 - 3.4.b AP groups
 - 3.4.c Flex groups
 - 3.4.d Site tag
 - 3.4.e RF tag
 - 3.4.f Policy tag
 - 3.5 FlexConnect and Office Extend
 - 3.6 All controller deployment models
 - 3.7 Mesh
 - 3.8 WGB on IOS and on COS APs
 - 3.9 Controller Mobility
 - 3.9.a L2/L3 roaming
 - 3.9.b Multicast optimization
 - 3.9.c Mobility group scaling
 - 3.9.d Inter-OS controller mobility
 - 3.9.e Mobility anchoring
 - 3.9.f Mobility encryption
- Wireless Security and Identity Management
 - 4.1 Secure management access and control plane
 - 4.1.a Device administration with TACACS+/RADIUS
 - 4.1.b CPU ACLs
 - 4.1.c Management via wireless and dynamic interface
 - 4.1.d Password policies
 - 4.1.e AP authorization
 - 4.2 Identity management
 - 4.2.a Basic PKI for dot1X and WebAuth
 - 4.2.b Internal and external identity sources
 - 4.2.c Identity PSK
 - 4.3 Wireless security and Network access policies
 - 4.3.a Client authentication and authorization
 - 4.3.b Client profiling and provisioning
 - 4.3.c RADIUS attributes
 - 4.3.d CoA
 - 4.3.e ACLs
 - 4.3.f L2/L3 security
 - 4.3.g Certificates
 - 4.3.h Local policies
 - 4.4 Guest management
 - 4.4.a Local web authentication
 - 4.4.b Central web authentication
 - 4.4.c Basic sponsor policy
 - 4.5 Access Point switchport authentication
 - 4.5.a MAB
 - 4.5.b 802.1X
 - 4.5.c NEAT
 - 4.5.d Switchport macros
 - 4.6 TrustSec for SD-Access Wireless

- 4.6.a SGTs
 - 4.6.b SGACLs
 - 4.7 Intrusion detection and prevention features
 - 4.7.a Rogue policies
 - 4.7.b MFP
 - 4.7.c Standards and custom signatures
 - 4.7.d Client exclusion policies
 - 4.7.e Switchport tracing
- Wireless Business Application and Services
 - 5.1 QoS policies
 - 5.1.a QoS profiles
 - 5.1.b EDCA
 - 5.1.c WMM
 - 5.1.d Bi-Directional Rate Limiting
 - 5.1.e Admission control
 - 5.1.f QoS maps
 - 5.1.g FastLane
 - 5.2 AVC and netflow
 - 5.3 Client roaming optimization
 - 5.3.a Band Select
 - 5.3.b Load Balancing
 - 5.3.c 802.11r and Adaptive Fast Transition
 - 5.3.d 802.11k/v
 - 5.4 Wireless Multicast
 - 5.4.a Multicast modes in the controllers
 - 5.4.b Multicast snooping
 - 5.4.c Multicast direct
 - 5.4.d Multicast VLAN
 - 5.5 mDNS
 - 5.5.a mDNS proxy
 - 5.5.b Service discovery (both classic deployment and Wide Area Bonjour)
 - 5.5.c Service filtering
- Automation, Analytics, and Assurance
 - 6.1 Prime Infrastructure
 - 6.1.a Basic operations
 - 6.1.a i Create and deploy templates
 - 6.1.a ii Operate maps
 - 6.1.a iii Import infrastructure devices
 - 6.1.a iv Audits
 - 6.1.a v Client troubleshooting
 - 6.1.a vi Notification receivers
 - 6.1.a vii Reports
 - 6.1.a viii Monitoring policies
 - 6.1.a ix Prime Infrastructure jobs
 - 6.1.b WLAN Security management
 - 6.1.b i Configure rogue management
 - 6.1.b ii Manage alarms and events
 - 6.2 Cisco CMX/DNA Spaces
 - 6.2.a Management access
 - 6.2.b Network services
 - 6.2.b i Analytics & Metrics
 - 6.2.b ii Location
 - 6.2.b iii Profiles
 - 6.2.b iv Engage
 - 6.2.c Operational Insights
 - 6.2.d API calls using python scripts

- 6.3 Cisco DNA Center
 - 6.3.a Wireless Automation
 - 6.3.a i Day 0 - Provisioning
 - 6.3.a ii SWIM
 - 6.3.a iii Application policies
 - 6.3.a iv Security policies
 - 6.3.a v Operate Maps
 - 6.3.b Assurance
 - 6.3.b i Network health and WLC/AP 360
 - 6.3.b ii Client health and client 360
 - 6.3.b iii Application experience
 - 6.3.b iv Sensors
 - 6.3.b v iPCAP and on demand captures
 - 6.3.b vi Network telemetry
 - 6.3.c SD Access
 - 6.3.c i Fabric enabled wireless
 - 6.3.c ii SDA policy and segmentation