

CCNP Enterprise, Minor Update

Products and technologies are evolving faster than ever before. To ensure that our certification programs remain relevant to current practice and keep up with the fast pace of change, we are committed to an annual maintenance review. Minor reviews ensure exam topics are clear, introduce new topics, and phase out older products and solutions that are less relevant today. The aim is to make the minor adjustments needed to match the evolution of technologies while ensuring the changes are minimal so that they do not disrupt a candidate's study plans.

Below is a summary of the changes for the CCNP Enterprise Core that will go live on March 19, 2026.

Across all exams, the following product names were changed:

- Cisco SD-WAN was changed to Cisco Catalyst SD-WAN.
- Cisco DNA Center was changed to Cisco Catalyst Center.
- Cisco vBond was changed to SD-WAN Validator.
- Cisco vManager was changed to SD-WAN Manager.
- Cisco vSmart was changed to SD-WAN Controller.

350-401 Implementing Cisco Enterprise Network Core Technologies v1.2

The tasks highlighted in red were removed:

- 1.2 Describe wireless network design principles
 - 1.2.a Wireless deployment models (centralized, distributed, controller-based, cloud, remote branch)
 - 1.2.b Location services in a WLAN design
 - 1.2.c Client density
- 1.5 Interpret wired and wireless QoS configurations
 - 1.5.a QoS components
 - 1.5.b QoS policy
- 1.6 Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables
- 3.3 Wireless
 - 3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference, noise, bands, channels, and wireless client devices capabilities
 - 3.3.b Describe AP modes and antenna types
 - 3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)
 - 3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming
 - 3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues using GUI only
 - 3.3.f Describe wireless segmentation with groups, profiles, and tags
- 5.4 Configure and verify wireless security features
 - 5.4.a 802.1X
 - 5.4.b WebAuth
 - 5.4.c PSK
 - 5.4.d EAPOL (4-way handshake)

CCNP Enterprise, Minor Update

- 5.5 Describe the components of network security design
 - 5.5.a Threat defense
 - 5.5.b Endpoint security
 - 5.5.c Next-generation firewall
 - 5.5.d TrustSec and MACsec
 - 5.5.e Network access control with 802.1X, MAB, and WebAuth

300-410 Implementing Cisco Enterprise Advanced Routing and Services v1.1

- 4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps, telemetry)
- 4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow, Ipflix)

300-415 Implementing Cisco Catalyst SD-WAN Solutions v1.2

- 3.7 Describe configuration and policy groups, feature profiles, and workflows
- 4.3 Configure end-to-end segmentation
 - 4.3.a VPN segmentation and membership
 - 4.3.b Topologies
- 4.4 Configure Cisco Catalyst SD-WAN application-aware routing including AI-driven Predictive Path Recommendation
- 6.1 Describe authentication, monitoring, reporting, and troubleshooting from SD-WAN Manager

300-420 Designing Cisco Enterprise Networks v1.1

- 1.5 Create stable, secure, and scalable routing designs for BGP
 - 1.5.a Address families
 - 1.5.b Basic route filtering
 - 1.5.c Attributes for path preference
 - 1.5.d Route reflectors & confederations
 - 1.5.e Load sharing
- 2.1 Design campus networks for high availability
 - 2.1.a First Hop Redundancy Protocols
 - 2.1.b Platform abstraction techniques
 - 2.1.c Graceful restart, NSF, NSR
 - 2.1.d BFD
- 4.5 Design multicast services (SSM, PIM bidirectional, MSDP, service-reflection)

300-440 Designing and Implementing Secure Cloud Connectivity v1.0

- 1.1 Describe internet-based connectivity to cloud providers (AWS, Azure, and Google Cloud)
 - 1.1.a Native IPsec
 - 1.1.b Cisco Catalyst SD-WAN internet cloud connectivity
- 2.4 Describe cloud-native security policies for AWS, Azure, and Google Cloud, such as east/west traffic within the cloud provider, backhaul internet traffic, inbound connectivity to the internet

CCNP Enterprise, Minor Update

- 3.1 Configure GRE/IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint, or to a secure internet gateway
- 4.1 Configure Cisco Catalyst SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud, or for a secure internet gateway
- 5.1 Diagnose IPsec internet-based secure cloud connectivity between an on-premises Cisco IOS XE router to a native AWS, Azure, and Google Cloud endpoint, or to a secure internet gateway
- 5.3 Diagnose Cisco Catalyst SD-WAN internet-based secure cloud connectivity for AWS, Azure, and Google Cloud, or for a secure internet gateway

300-435 Automating Cisco Enterprise Solutions v2.0

Major revision – new blueprint below.

- 1.0 Network Automation Foundation
 - 1.1 Describe OpenConfig, IETF, and native YANG models
 - 1.2 Describe NETCONF and RESTCONF
 - 1.3 Construct a JSON payload based on a YANG model using tools such as YANG Suite and pyang
 - 1.4 Construct the XML payload based on a YANG model using tools such as YANG Suite and pyang
 - 1.5 Interpret a YANG module tree generated per RFC8340
- 2.0 Device-Level Network Automation
 - 2.1 Construct a network automation solution with Python using Netmiko to manage and monitor configurations
 - 2.2 Construct a network automation solution with Python using ncclient to manage and monitor configurations
 - 2.3 Construct a network automation solution with Python using RESTCONF to manage and monitor configurations
 - 2.4 Construct a network automation solution with Ansible to manage configurations
 - 2.5 Construct a device-level network automation solution for Day 0 provisioning
 - 2.6 Troubleshoot network automation solutions based on RESTCONF, NETCONF and YANG models
 - 2.7 Construct on-box automations using EEM, guest shell, and on-box Python
- 3.0 Controller-Based Network Automation
 - 3.1 Construct a controller-based network automation solution for Day-0 provisioning
 - 3.2 Construct a controller-based network automation solution with Python to manage and monitor configurations
 - 3.3 Construct advanced network configuration templates using Jinja2 constructs such as loops, conditionals, output modifiers, and filters
 - 3.4 Construct a controller-based network automation solution with Ansible to manage configurations
 - 3.5 Construct security automation solutions such as policy enforcement, compliance monitoring, and network segmentation
 - 3.6 Troubleshoot network automation solutions based on REST APIs
- 4.0 Operations
 - 4.1 Describe the use of Cisco platform APIs for the testing and validation phase of a network automation solution
 - 4.2 Describe the use of simulations related to enterprise operations
 - 4.3 Construct a controller-based network automation solution to manage device software versions
 - 4.4 Construct a controller-based network automation solution to monitor network health
 - 4.5 Configure a subscription for model driven telemetry on a Cisco IOS XE device (CLI, NETCONF, and RESTCONF)
 - 4.6 Implement webhook-based monitoring using controllers



CCNP Enterprise, Minor Update

5.0	AI in Automation
5.1	Describe AI in controller-based platforms
5.2	Describe AI-assisted code development for network automation
5.3	Describe the security risks in a given AI-based network automation solution
5.4	Construct an MCP server to provide network information to an AI agent using Python FastMCP

300-445 Designing and Implementing Enterprise Network Assurance v1.0

No changes were made.

