To earn your CCNP Enterprise, CCIE Enterprise Infrastructure, or CCIE Enterprise Wireless certification, you must pass the **350-401 ENCOR** exam. This exam tests your knowledge of:

- # 1.0 Architecture 15%
  - 1.1 Explain the different design principles used in an enterprise network
    - 1.1.a High-level enterprise network design such as 2-tier, 3-tier, fabric, and cloud
    - 1.1.b High availability techniques such as redundancy, FHRP, and SSO
  - 1.2 Describe wireless network design principles
    - 1.2.a Wireless deployment models (centralized, distributed, controller-less, controller-based, cloud, remote branch)
    - 1.2.b Location services in a WLAN design
    - 1.2.c Client density
  - 1.3 Explain the working principles of the Cisco SD-WAN solution
    - 1.3.a SD-WAN control and data planes elements
    - 1.3.b Benefits and limitations of SD-WAN solutions
  - 1.4 Explain the working principles of the Cisco SD-Access solution
    - 1.4.a SD-Access control and data planes elements
    - 1.4.b Traditional campus interoperating with SD-Access
  - 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
- # 2.0 Virtualization 10%
  - 2.1 Describe device virtualization technologies
    - 2.1.a Hypervisor type 1 and 2
    - 2.1.b Virtual machine
    - 2.1.c Virtual switching
  - 2.2 Configure and verify data path virtualization technologies
    - 2.2.a VRF
    - 2.2.b GRE and IPsec tunneling
  - 2.3 Describe network virtualization concepts
    - 2.3.a LISP
    - 2.3.b VXLAN
- # 3.0 Infrastructure 30%

- 3.1 Layer 2
  - 3.1.a Troubleshoot static and dynamic 802.1q trunking protocols
  - 3.1.b Troubleshoot static and dynamic EtherChannels
  - 3.1.c Configure and verify common Spanning Tree Protocols (RSTP, MST) and Spanning Tree enhancements such as root guard and BPDU guard
- 3.2 Layer 3
  - 3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics, and area types)
  - 3.2.b Configure simple OSPFv2/v3 environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point, and broadcast network types, and passive-interface)
  - 3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
  - 3.2.d Describe policy-based routing
- 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
- 3.4 IP Services
  - 3.4.a Interpret network time protocol configurations such as NTP and PTP
  - 3.4.b Configure NAT/PAT
  - 3.4.c Configure first hop redundancy protocols, such as HSRP, VRRP
  - 3.4.d Describe multicast protocols, such as RPF check, PIM and IGMP v2/v3

. 4.0 Network Assurance

10%

- 4.1 Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
- 4.2 Configure and verify Flexible NetFlow
- 4.3 Configure SPAN/RSPAN/ERSPAN

- 4.4 Configure and verify IPSLA
- 4.5 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
- 4.6 Configure and verify NETCONF and RESTCONF

5.0 Security

20%

- 5.1 Configure and verify device access control
  - 5.1.a Lines and local user authentication
  - 5.1.b Authentication and authorization using AAA
- 5.2 Configure and verify infrastructure security features
  - 5.2.a ACLs
  - 5.2.b CoPP
- 5.3 Describe REST API security
- 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)
- 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

6.0 Automation

15%

- 6.1 Interpret basic Python components and scripts
- 6.2 Construct valid JSON-encoded files
- 6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG
- 6.4 Describe APIs for Cisco DNA Center and vManage
- 6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
- 6.6 Construct an EEM applet to automate configuration, troubleshooting, or data collection
- 6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

The above topics are likely to be included on the 350-401 ENCOR exam. The topics are subject to change at any time to reflect the latest technologies aligned to Cisco's products.