Implementing Cisco Enterprise Network Core Technologies v1.0 (300-401)

Exam Description: Implementing Cisco Enterprise Network Core Technologies v1.0 (ENCOR 300-401) is a 120-minute exam associated with the CCNP and CCIE Enterprise Certifications. This exam tests a candidate's knowledge of implementing core enterprise network technologies including dual stack (IPv4 and IPv6) architecture, virtualization, infrastructure, network assurance, security and automation. The course, Implementing Cisco Enterprise Network Core Technologies, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

15% 1.0 Architecture

1.1 Explain the different design principles used in an enterprise network
- 1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning
- 1.1.b High availability techniques such as redundancy, FHRP, and SSO

1.2 Analyze design principles of a WLAN deployment
- 1.2.a Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)
- 1.2.b Location services in a WLAN design

1.3 Differentiate between on-premises and cloud infrastructure deployments

1.4 Explain the working principles of the Cisco SD-WAN solution
- 1.4.a SD-WAN control and data planes elements
- 1.4.b Traditional WAN and SD-WAN solutions

1.5 Explain the working principles of the Cisco SD-Access solution
- 1.5.a SD-Access control and data planes elements
- 1.5.b Traditional campus interoperating with SD-Access

1.6 Describe concepts of wired and wireless QoS
- 1.6.a QoS components
- 1.6.b QoS policy

1.7 Differentiate hardware and software switching mechanisms
- 1.7.a Process and CEF
- 1.7.b MAC address table and TCAM
- 1.7.c FIB vs. RIB

10% 2.0 Virtualization

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

30% 3.0 Infrastructure

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 and MST)

3.2 Layer 3
- 3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. linked state, load balancing, path selection, path operations, metrics)
- 3.2.b Configure and verify simple OSPF 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)

3.3 Wireless
- 3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise, band and 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

3.4 IP Services
- 3.4.a Describe Network Time Protocol (NTP)
- 3.4.b Configure and verify NAT/PAT
- 3.4.c Configure first hop redundancy protocols, such as HSRP and VRRP
- 3.4.d Describe multicast protocols, such as PIM and IGMP v2/v3

10% 4.0 Network Assurance

4.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog

4.2 Configure and verify device monitoring using syslog for remote logging

- 4.3 Configure and verify NetFlow and Flexible NetFlow
- 4.4 Configure and verify SPAN/RSPAN/ERSPAN
- 4.5 Configure and verify IPSLA
- 4.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
- 4.7 Configure and verify NETCONF and RESTCONF

20% 5.0 Security

- 5.1 Configure and verify device access control
  - 5.1.a Lines and password protection
  - 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 EAP
  - 5.4.b WebAuth
  - 5.4.c PSK
- 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, MACsec
  - 5.5.e Network access control with 802.1X, MAB, and WebAuth

15% 6.0 Automation

- 6.1 Interpret basic Python components and scripts
- 6.2 Construct valid JSON encoded file
- 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 EEM applet to automate configuration, troubleshooting, or data collection
- 6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack