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

Exam Description: Implementing Cisco Enterprise Network Core Technologies v1.2 (ENCOR 350-401) 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 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	Explain the working principles of the Cisco Catalyst SD-WAN solution
		1.2.a SD-WAN control and data planes elements
		1.2.b Benefits and limitations of Catalyst SD-WAN solution
	1.3	Explain the working principles of the Cisco SD-Access solution
		1.3.a SD-Access control and data planes elements
		1.3.b Traditional campus interoperating with SD-Access
	1.4	Interpret QoS configurations
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, 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   IP Services
        3.3.a   Interpret network time protocol configurations such as NTP and PTP
        3.3.b   Configure NAT/PAT
        3.3.c   Configure first hop redundancy protocols, such as HSRP, VRRP
        3.3.d   Describe multicast protocols, such as RPF check, PIM SM, IGMP v2/v3, SSM, bidir, and MSDP

10%   4.0   Network Assurance
    4.1   Diagnose network problems using 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 how Cisco Catalyst Center (formerly Cisco DNA Center) is used to apply network configuration, monitoring, and management using traditional and AI-powered workflows
    4.6   Configure and verify NETCONF and RESTCONF

20%   5.0   Security
    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   Describe the components of network security design
    5.4.a   Threat defense
    5.4.b   Endpoint security
    5.4.c   Next-generation firewall
    5.4.d   TrustSec and MACsec

15%   6.0   Automation and Artificial Intelligence
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 Catalyst Center and SD-WAN Manager
6.5   Interpret REST API response codes and results in payload using Cisco Catalyst Center and RESTCONF
6.6   Construct an EEM applet to automate configuration, troubleshooting, or data collection
6.7   Compare agent vs. agentless orchestration tools