Implementing and Operating Cisco Service Provider Network Core Technologies (300-501)

Exam Description: The Implementing and Operating Cisco Service Provider Network Core Technologies v1.0 (SPCOR 350-501) exam is a 120-minute exam associated with the CCNP Service Provider, CCIE Service Provider, and Cisco Certified Specialist - Service Provider Core certifications. This exam tests a candidate's knowledge of implementing core service provider network technologies including core architecture, services, networking, automation, quality of services, security, and network assurance. The course, Implementing and Operating Cisco Service Provider 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 Describe service provider architectures
  - 1.1.a Core architectures (Metro Ethernet, MPLS, unified MPLS, SR)
  - 1.1.b Transport technologies (Optical, xDSL, DOCSIS, TDM, and xPON)
  - 1.1.c Mobility (packet core, RAN xHaul transport for 4G and 5G)
- 1.2 Describe Cisco network software architecture
  - 1.2.a IOS
  - 1.2.b IOS XE
  - 1.2.c IOS XR
- 1.3 Describe service provider virtualization
  - 1.3.a NFV infrastructure
  - 1.3.b VNF workloads
  - 1.3.c OpenStack
- 1.4 Describe QoS architecture
  - 1.4.a MPLS QoS models (Pipe, Short Pipe, and Uniform)
  - 1.4.b MPLS TE QoS (MAM, RDM, CBTS, PBTS, and DS-TE)
  - 1.4.c DiffServ and IntServ QoS models
  - 1.4.d Trust boundaries between enterprise and SP environments
  - 1.4.e IPv6 flow label
- 1.5 Configure and verify control plane security
  - 1.5.a Control plane protection techniques (LPTS and CoPP)
  - 1.5.b BGP-TTL security and protocol authentication
  - 1.5.c BGP prefix suppression
  - 1.5.d LDP security (authentication and label allocation filtering)

1.5.e BGP sec
1.5.f BGP flowspec

1.6 Describe management plane security
1.6.a Traceback
1.6.b AAA and TACACS
1.6.c RestAPI security
1.6.d DdoS

1.7 Implement data plane security
1.7.a uRPF
1.7.b ACLs
1.7.c RTBH

30% 2.0 Networking

2.1 Implement IS-IS (IPv4 and IPv6)
2.1.a Route advertisement
2.1.b Area addressing
2.1.c Multitopology
2.1.d Metrics

2.2 Implement OSPF (v2 and v3)
2.2.a Neighbor adjacency
2.2.b Route advertisement
2.2.c Multiarea (addressing and types)
2.2.d Metrics

2.3 Describe BGP path selection algorithm

2.4 Implement BGP (v4 and v6 for IBGP and EBGP)
2.4.a Neighbors
2.4.b Prefix advertisement
2.4.c Address family
2.4.d Path selection
2.4.e Attributes
2.4.f Redistribution

2.5 Implement routing policy language and route maps (BGP, OSPF, IS-IS)

2.6 Troubleshoot routing protocols
2.6.a Neighbor adjacency (IS-IS, OSPF, BGP)
2.6.b Route advertisement (IS-IS, OSPF, BGP)

2.7 Describe IPv6 transition (NAT44, NAT64, 6RD, MAP, and DS Lite)

2.8 Implement high availability
2.8.a NSF / graceful restart
2.8.b NSR

2.8.c BFD
2.8.d Link aggregation

20% 3.0 MPLS and Segment Routing

3.1 Implement MPLS
- 3.1.a LDP sync
- 3.1.b LDP session protection
- 3.1.c LDP neighbors
- 3.1.d Unified MPLS
- 3.1.e MPLS OAM

3.2 Describe traffic engineering
- 3.2.a IS-IS and OSPF extensions
- 3.2.b RSVP functionality
- 3.2.c FRR

3.3 Describe segment routing
- 3.3.a Segment types
- 3.3.b IGP control plane
- 3.3.c Segment routing traffic engineering
- 3.3.d TI-LFa
- 3.3.e PCE-PCC architectures

20% 4.0 Services

4.1 Describe VPN services
- 4.1.a EVPN
- 4.1.b Inter-AS VPN
- 4.1.c CSC
- 4.1.d mVPN

4.2 Configure L2VPN and Carrier Ethernet
- 4.2.a Ethernet services (E-Line, E-Tree, E-Access, E-LAN)
- 4.2.b IEEE 802.1ad, IEEE 802.1ah, and ITU G.8032
- 4.2.c Ethernet OAM
- 4.2.d VLAN tag manipulation

4.3 Configure L3VPN
- 4.3.a Intra-AS VPN
- 4.3.b Shared services (Extranet and Internet)

4.4 Implement multicast services
- 4.4.a PIM (PIM-SM, PIM-SSM, and PIM-BIDIR)
- 4.4.b IGMP v1/v2/v3 and MLD

4.5 Implement QoS services
- 4.5.a Classification and marking
- 4.5.b Congestion avoidance, traffic policing, and shaping

15% **5.0 Automation and Assurance**

- 5.1 Describe the programmable APIs used to include Cisco devices in network automation
- 5.2 Interpret an external script to configure a Cisco device using a REST API
- 5.3 Describe the role of Network Services Orchestration (NSO)
- 5.4 Describe the high-level principles and benefits of a data modeling language, such as YANG
- 5.5 Compare agent vs. agentless configuration management tools, such as Chef, Puppet, Ansible, and SaltStack
- 5.6 Describe data analytics and model-driven telemetry in service provider
- 5.7 Configure dial-in/out telemetry streams using gRPC
- 5.8 Configure and verify NetFlow/IPFIX
- 5.9 Configure and verify NETCONF and RESTCONF
- 5.10 Configure and verify SNMP (v2c/v3)