CCIE Routing and Switching Written Exam (350-001) version 4.0

Exam Description: The Cisco CCIE® Routing and Switching Written Exam (350-001) is a 2-hour test with 80−110 questions that will validate that professionals have the expertise to: configure, validate, and troubleshoot complex enterprise network infrastructure; understand how infrastructure components interoperate; and translate functional requirements into specific device configurations. The exam is closed book and no outside reference materials are allowed.

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. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

16% 1.0 Implement Layer 2 Technologies

- 1.1 Implement STP
  - 1.1.a IEEE 802.1D
  - 1.1.b IEEE 802.1W
  - 1.1.c IEEE 802.1S
  - 1.1.d Loop guard
  - 1.1.e Root guard
  - 1.1.f BPDU guard
  - 1.1.g Storm control
  - 1.1.h Unicast flooding
  - 1.1.i Port roles, failure propagation, and loop guard operation
- 1.2 Implement VLAN and VTP
- 1.3 Implement trunk and trunk protocols, EtherChannel, and load balancing
- 1.4 Implement Ethernet technologies
  - 1.4.a Speed and duplex
  - 1.4.b Ethernet, Fast Ethernet, and Gigabit Ethernet
  - 1.4.c PPPoE
- 1.5 Implement SPAN, RSPAN, and flow control
- 1.6 Implement Frame Relay
  - 1.6.a LMI
  - 1.6.b Traffic shaping
  - 1.6.c Full mesh
  - 1.6.d Hub and spoke
  - 1.6.e DE

1.7 Implement HDLC and PPP

10% 2.0 Implement IPv4

2.1 Implement IPv4 addressing, subnetting, and VLSM

2.2 Implement IPv4 tunneling and GRE

2.3 Implement IPv4 RIPv2

2.4 Implement IPv4 OSPF
- 2.4.a Standard OSPF areas
- 2.4.b Stub area
- 2.4.c Totally stubby area
- 2.4.d NSSA
- 2.4.e Totally NSSA
- 2.4.f LSA types
- 2.4.g Adjacency on a point-to-point and on a multi-access network
- 2.4.h OSPF graceful restart

2.5 Implement IPv4 EIGRP
- 2.5.a Best path
- 2.5.b Loop-free paths
- 2.5.c EIGRP operations when alternate loop-free paths are available and not available
- 2.5.d EIGRP queries
- 2.5.e Manual summarization and auto-summarization
- 2.5.f EIGRP stubs

2.6 Implement IPv4 BGP
- 2.6.a Next hop
- 2.6.b Peering
- 2.6.c IBGP and EBGP

2.7 Implement policy routing

2.8 Implement Cisco PfR and Cisco OER

2.9 Implement filtering, route redistribution, summarization, synchronization, attributes, and other advanced features

4% 3.0 Implement IPv6

3.1 Implement IPv6 addressing and different addressing types
3.2 Implement IPv6 neighbor discovery
3.3 Implement basic IPv6 functionality protocols
3.4 Implement tunneling techniques
3.5 Implement OSPFv3
3.6 Implement EIGRPv6
3.7 Implement filtering and route redistribution

4% **4.0** **Implement MPLS Layer 3 VPNs**

- 4.1 Implement MPLS
- 4.2 Implement Layer 3 VPNs on provider edge (PE), provider (P), and customer edge (CE) routers
- 4.3 Implement VRF and Multi-VRF Customer Edge (VRF-Lite)

6% **5.0** **Implement IP Multicast**

- 5.1 Implement PIM sparse mode
- 5.2 Implement MSDP
- 5.3 Implement inter-domain multicast routing
- 5.4 Implement PIM Auto-RP, unicast RP, and BSR
- 5.5 Implement multicast tools, features, and source-specific multicast
- 5.6 Implement IPv6 multicast, PIM, and related multicast protocols such as MLD

9% **6.0** **Implement Network Security**

- 6.1 Implement access lists
- 6.2 Implement zone-based firewall
- 6.3 Implement uRPF
- 6.4 Implement IP source guard
- 6.5 Implement AAA (configuring the AAA server is not required, only the client-side is configured)
- 6.6 Implement CoPP
- 6.7 Implement Cisco IOS Firewall
- 6.8 Implement Cisco IOS IPS
- 6.9 Implement SSH
- 6.10 Implement IEEE 802.1X
- 6.11 Implement NAT
- 6.12 Implement routing protocol authentication
- 6.13 Implement device access control
- 6.14 Implement security features

3% **7.0** **Implement Network Services**

- 7.1 Implement HSRP
- 7.2 Implement GLBP
- 7.3 Implement VRRP
- 7.4 Implement NTP
- 7.5 Implement DHCP
- 7.6 Implement WCCP

6% **8.0** **Implement QoS**

- 8.1 Implement MQC
  - 8.1.a NBAR
  - 8.1.b CBWFQ, MDRR, and LLQ
  - 8.1.c Classification
  - 8.1.d Policing
  - 8.1.e Shaping
  - 8.1.f Marking
  - 8.1.g WRED and RED

8.1.h Compression

8.2 Implement Layer 2 QoS: WRR, SRR, and policies

8.3 Implement LFI for Frame Relay

8.4 Implement generic traffic shaping

8.5 Implement RSVP

8.6 Implement Cisco AutoQoS

30% 9.0 Troubleshoot a Network

9.1 Troubleshoot complex Layer 2 network issues
9.2 Troubleshoot complex Layer 3 network issues
9.3 Troubleshoot a network in response to application problems
9.4 Troubleshoot network services
9.5 Troubleshoot network security

6% 10.0 Optimize the Network

10.1 Implement syslog and local logging
10.2 Implement IP SLA
10.3 Implement NetFlow
10.4 Implement SPAN, RSPAN, and RITE
10.5 Implement SNMP
10.6 Implement Cisco IOS EEM
10.7 Implement RMON
10.8 Implement FTP
10.9 Implement TFTP
10.10 Implement TFTP server on router
10.11 Implement SCP
10.12 Implement HTTP and HTTPS
10.13 Implement Telnet

6% 11.0 Evaluate Proposed Changes to a Network

11.1 Evaluate interoperability of proposed technologies against deployed technologies
- 11.1.a Make changes to routing protocol parameters
- 11.1.b Migrate parts of a network to IPv6
- 11.1.c Route protocol migration
- 11.1.d Add multicast support
- 11.1.e Migrate STP
- 11.1.f Evaluate the effect of new traffic on existing QoS design

11.2 Determine the operational effect of proposed changes to an existing network
- 11.2.a Downtime of network or portions of network
- 11.2.b Performance degradation
- 11.2.c Introduction of security breaches

11.3 Suggest alternative solutions when incompatible changes are proposed to an existing network

- 11.3.a Hardware and software upgrades
- 11.3.b Topology shifts
- 11.3.c Reconfigurations