CCDE Written Exam (352-001) version 2.0

Exam Description: Cisco CCDE® Written Exam (352-001) version 2 is a 2-hour test with 90−110 questions that will validate that professionals have the expertise to gather and clarify network functional requirements, develop network designs to meet functional specifications, develop an implementation plan, convey design decisions and their rationale, and possess expert-level network infrastructure knowledge. 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.

26% 1.0 Layer 2 Control Plane

- 1.1 Describe fast convergence techniques and mechanisms
  - 1.1.a Down detection
  - 1.1.b Interface dampening
- 1.2 Describe loop detection and mitigation protocols
  - 1.2.a Spanning tree types
  - 1.2.b Spanning tree tuning techniques
- 1.3 Describe mechanisms that are available for creating loop-free topologies
  - 1.3.a REP
  - 1.3.b Multipath
  - 1.3.c Switch clustering
  - 1.3.d Flex links
  - 1.3.e Loop detection and mitigation
- 1.4 Describe the effect of transport mechanisms and their interaction with routing protocols over different types of links
- 1.5 Describe multicast routing concepts
- 1.6 Describe the effect of fault isolation and resiliency on network design
  - 1.6.a Fault isolation
  - 1.6.b Fate sharing
  - 1.6.c Redundancy
  - 1.6.d Virtualization
  - 1.6.e Segmentation

37% 2.0 Layer 3 Control Plane

- 2.1 Describe route aggregation concepts and techniques

- 2.1.a Purpose of route aggregation
- 2.1.b When to leak routes / avoid suboptimal routing
- 2.1.c Determine aggregation location and techniques

2.2 Describe the theory and application of network topology layering
- 2.2.a Layers and their purposes in various environments

2.3 Describe the theory and application of network topology abstraction
- 2.3.a Purpose of link state topology summarization
- 2.3.b Use of link state topology summarization

2.4 Describe the effect of fault isolation and resiliency on network design or network reliability
- 2.4.a Fault isolation
- 2.4.b Fate sharing
- 2.4.c Redundancy

2.5 Describe metric-based traffic flow and modification
- 2.5.a Metrics to modify traffic flow
- 2.5.b Third-party next hop

2.6 Describe fast convergence techniques and mechanisms
- 2.6.a Protocol timers
- 2.6.b Loop-free alternates

2.7 Describe factors affecting convergence
- 2.7.a Recursion
- 2.7.b Microloops
- 2.7.c Transport

2.8 Describe unicast routing protocol operation (OSPF, EIGRP, ISIS, BGP, and RIP) in relation to network design
- 2.8.a Neighbor relationships
- 2.8.b Loop-free paths
- 2.8.c Flooding domains and stubs
- 2.8.d iBGP scalability

2.9 Analyze operational costs and complexity
- 2.9.a Routing policy
- 2.9.b Redistribution methods

2.10 Describe the interaction between routing protocols and topologies

2.11 Describe generic routing and addressing concepts
- 2.11.a Policy-based routing
- 2.11.b NAT
- 2.11.c Subnetting
- 2.11.d RIB-FIB relationships

2.12 Describe multicast routing concepts
- 2.12.a General multicast concepts
- 2.12.b Source specific
- 2.12.c MSDP/anycast
- 2.12.d PIM
- 2.12.e mVPN

2.13 Describe IPv6 concepts and operation
- 2.13.a General IPv6 concepts
- 2.13.b IPv6 security
- 2.13.c IPv6 transition techniques

17% 3.0 Network Virtualization

3.1 Describe Layer 2 and Layer 3 tunnelling technologies
- 3.1.a Tunnelling for security
- 3.1.b Tunnelling for network extension
- 3.1.c Tunnelling for resiliency
- 3.1.d Tunnelling for protocol integration
- 3.1.e Tunnelling for traffic optimization

3.2 Analyze the implementation of tunnelling
- 3.2.a Tunnelling technology selection
- 3.2.b Tunnelling endpoint selection
- 3.2.c Tunnelling parameter optimization of end-user applications
- 3.2.d Effects of tunnelling on routing
- 3.2.e Routing protocol selection and tuning for tunnels

20% 4.0 Design Considerations

4.1 Analyze various QoS performance metrics
- 4.1.a Application requirements
- 4.1.b Performance metrics

4.2 Describe types of QoS techniques
- 4.2.a Classification and marking
- 4.2 b Shaping
- 4.2.c Policing
- 4.2.d Queuing

4.3 Identify QoS strategies based on customer requirements
- 4.3.a DiffServ
- 4.3.b IntServ

4.4 Identify network management requirements

4.5 Identify network application reporting requirements

4.6 Describe technologies, tools, and protocols that are used for network management

4.7 Describe the reference models and processes that are used in network management, such as FCAPS, ITIL®), and TOGAF

4.8 Describe best practices for protecting network infrastructure
- 4.8.a Secure administrative access
- 4.8.b Control plane protection

4.9 Describe best practices for protecting network services
- 4.9.a Deep packet inspection
- 4.9.b Data plane protection

4.10 Describe tools and technologies for identity management

4.11 Describe tools and technologies for IEEE 802.11 wireless deployment

4.12 Describe tools and technologies for optical deployment

4.13 Describe tools and technologies for SAN fabric deployment