CCDE Written Exam Topics v2.1

The Cisco CCDE® written exam (352-001) version 2.1 is a two-hour test with 90–110 questions that test a candidate's combined knowledge of routing protocols, internetworking theory and design principles.

The exam assesses a candidate's understanding of network design in the areas of routing, tunneling, Quality of Service, Management, Cost, Capacity, and Security. This exam combines in-depth technical concepts with Network Design principles and is intended for a Network Professional with at least 7 years of experience in Network Engineering or Advanced Network Design. Product-specific knowledge including version of code, implementation and operations specific concepts is not tested on the CCDE exam. 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.

---

*NOTE: This CCDE written exam topics version 2.1 includes Evolving Technologies v1.1 domain and should be referenced for written exams scheduled **on** August 30, 2018 and beyond.*

24% 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
  - 1.4.a Describe multicast routing concepts
- 1.5 Describe the impact of fault isolation and resiliency on network design
  - 1.5.a Fault isolation
  - 1.5.b Fate sharing
  - 1.5.c Redundancy
  - 1.5.d Virtualization
  - 1.5.e Segmentation

33% 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 impact 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 Neighbour 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

15% 3.0 Network Virtualization

- 3.1 Describe Layer 2 and Layer 3 tunneling technologies
  - 3.1.a Tunneling for security
  - 3.1.b Tunneling for network extension
  - 3.1.c Tunneling for resiliency
  - 3.1.d Tunneling for protocol integration
  - 3.1.e Tunneling for traffic optimization
- 3.2 Analyze the implementation of tunneling
  - 3.2.a Tunneling technology selection
  - 3.2.b Tunneling endpoint selection
  - 3.2.c Tunneling parameter optimization of end-user applications
  - 3.2.d Effects of tunneling on routing
  - 3.2.e Routing protocol selection and tuning for tunnels

18% 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 used for network management
- 4.7 Describe the reference models and processes 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 802.11 wireless deployment
- 4.12 Describe tools and technologies for optical deployment
- 4.13 Describe tools and technologies for SAN fabric deployment

10% 5.0 Evolving Technologies v1.1

- 5.1 Cloud
  - 5.1.a Compare and contrast public, private, hybrid, and multicloud design considerations
    - 5.1.a (i) Infrastructure, platform, and software as a service (XaaS)
    - 5.1.a (ii) Performance, scalability, and high availability

- 5.1.a (iii) Security implications, compliance, and policy
- 5.1.a (iv) Workload migration
- 5.1.b Describe cloud infrastructure and operations
  - 5.1.b (i) Compute virtualization (containers and virtual machines)
  - 5.1.b (ii) Connectivity (virtual switches, SD-WAN and SD-Access)
  - 5.1.b (iii) Virtualization functions (NFVi, VNF, and L4/L5)
  - 5.1.b (iv) Automation and orchestration tools (CloudCenter, DNA-center, and Kubernetes)

5.2 Network programmability (SDN)

- 5.2.a Describe architectural and operational considerations for a programmable network
  - 5.2.a (i) Data models and structures (YANG, JSON and XML)
  - 5.2.a (ii) Device programmability (gRPC, NETCONF and RESTCONF)
  - 5.2.a (iii) Controller based network design (policy driven configuration and northbound/ southbound APIs)
  - 5.2.a (iv) Configuration management tools (agent and agentless) and version control systems (Git and SVN)

5.3 Internet of things (IoT)

- 5.3.a Describe architectural framework and deployment considerations for IoT
  - 5.3.a (i) IoT technology stack (IoT Network Hierarchy, data acquisition and flow)
  - 5.3.a (ii) IoT standards and protocols (characteristics within IT and OT environment)
  - 5.3.a (iii) IoT security (network segmentation, device profiling, and secure remote access)
  - 5.3.a (iv) IoT edge and fog computing (data aggregation and edge intelligence)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.