

(d-5332) CCDE Written Exam Topics v2.0

CCDE Written Exam Topics v2.0

The Cisco CCDE written exam topic areas listed are general guidelines for the type of content that is likely to appear on the exam. Please note, however, that other relevant or related topic areas may also appear on the CCDE written exam.

Exam Sections and Sub-task Objectives

1.00	Layer 2 control plane
1.01	Describe fast convergence techniques and mechanisms
1.01.1	Down detection
1.01.2	Interface dampening
1.02	Describe loop detection and mitigation protocols
1.02.1	Spanning tree types
1.02.2	Spanning tree tuning techniques
1.03	Describe mechanisms that are available for creating loop-free topologies
1.03.1	REP
1.03.2	Multipath
1.03.3	Switch clustering
1.03.4	Flex links
1.03.5	Loop detection and mitigation
1.04	Describe the impact of transport mechanisms and their interaction with routing protocols over different types of links
1.05	Describe multicast routing concepts
1.06	Describe the impact of fault isolation and resiliency on network design

1.06.1	Fault isolation
1.06.2	Fate sharing
1.06.3	Redundancy
1.06.4	Virtualization
1.06.5	Segmentation
2.00	Layer 3 control plane
2.01	Describe route aggregation concepts and techniques
2.01.1	Purpose of route aggregation
2.01.2	When to leak routes/avoid suboptimal routing
2.01.3	Determining aggregation location and techniques
2.02	Describe the theory and application of network topology layering
2.02.1	Layers and their purposes in various environments
2.03	Describe the theory and application of network topology abstraction
2.03.1	Purpose of link state topology summarization
2.03.2	Use of link state topology summarization
2.04	Describe the impact of fault isolation and resiliency on network design or network reliability
2.04.1	Fault isolation
2.04.2	Fate sharing
2.04.3	Redundancy
2.05	Describe metric-based traffic flow and modification
2.05.1	Metrics to modify traffic flow
2.05.2	Third-party next hop

2.06	Describe fast convergence techniques and mechanisms
2.06.1	Protocol timers
2.06.2	Loop-free alternates
2.07	Describe factors affecting convergence
2.07.1	Recursion
2.07.2	Microloops
2.07.3	Transport
2.08	Describe unicast routing protocol operation (OSPF, EIGRP, IS-IS, BGP, and RIP) in relation to network design
2.08.1	Neighbor relationships
2.08.2	Loop-free paths
2.08.3	Flooding domains and stubs
2.08.4	iBGP scalability
2.09	Analyze operational costs and complexity
2.09.1	Routing policy
2.09.2	Redistribution methods
2.10	Describe the interaction between routing protocols and topologies
2.11	Describe generic routing and addressing concepts
2.11.1	Policy-based routing
2.11.2	NAT
2.11.3	Subnetting
2.11.4	RIB-FIB relationships
2.12	Describe multicast routing concepts
2.12.1	General multicast concepts
2.12.2	Source specific
2.12.3	MSDP/anycast
2.12.4	PIM

2.12.5	mVPN
2.13	Describe IPv6 concepts and operation
2.13.1	General IPv6 concepts
2.13.2	IPv6 security
2.13.3	IPv6 transition techniques
3.00	Network virtualization
3.01	Describe Layer 2 and Layer 3 tunneling technologies
3.01.1	Tunneling for security
3.01.2	Tunneling for network extension
3.01.3	Tunneling for resiliency
3.01.4	Tunneling for protocol integration
3.01.5	Tunneling for traffic optimization
3.02	Analyze the implementation of tunneling
3.02.1	Tunneling technology selection
3.02.2	Tunneling endpoint selection
3.02.3	Tunneling parameter optimization of end-user applications
3.02.4	Effects of tunneling on routing
3.02.5	Routing protocol selection and tuning for tunnels
4.00	Design considerations
4.01	Analyze various Quality of Service (QoS) performance metrics
4.01.1	Application requirements
4.01.2	Performance metrics
4.02	Describe types of QoS techniques
4.02.1	Classification and marking
4.02.2	Shaping
4.02.3	Policing

4.02.4	Queuing
4.03	Identify QoS strategies based on customer requirements
4.03.1	DiffServ
4.03.2	IntServ
4.04	Identify network management requirements
4.05	Identify network application reporting requirements
4.06	Describe technologies, tools, and protocols used for network management
4.07	Describe the reference models and processes used in network management, such as FCAPS, ITIL, and TOGAF
4.08	Describe best practices for protecting network infrastructure
4.08.1	Secure administrative access
4.08.2	Control plane protection
4.09	Describe best practices for protecting network services
4.09.1	Deep packet inspection
4.09.2	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

- end-