352-001

CCDE Design Written Exam

NWExam.com

SUCCESS GUIDE TO CISCO CERTIFICATION

Exam Summary – Syllabus – Questions

Table of Contents

Introduction to 352-001 Exam on CCDE Design Written Exam

A great way to start the Cisco Certified Design Expert (CCDE) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Cisco 352-001 certification exam. This study guide is an instrument to get you on the same page with Cisco and understand the nature of the Cisco Design Expert exam.

Our team of experts has composed this Cisco 352-001 exam preparation guide to provide the overview about Cisco CCDE Design Written Exam exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Cisco CCDE exam by identifying prerequisite areas of knowledge. We recommend you to refer the simulation questions and practice test listed in this guide to determine what type of questions will be asked and the level of difficulty that could be tested in the Cisco Design Expert certification exam.

Cisco 352-001 Certification Details:

Exam Name	CCDE Design Written Exam
Exam Number	352-001 CCDE
Exam Price	$300 USD
Duration	120 minutes
Number of Questions	90-110
Passing Score	Variable (750-850 / 1000 Approx.)
Exam Registration	PEARSON VUE
Sample Questions	Cisco 352-001 Sample Questions
Practice Exam	**Cisco Certified Design Expert Practice Test**

Cisco 352-001 Exam Syllabus:

Section	Weight	Objectives
Layer 2 Control Plane	24%	1 Describe fast convergence techniques and mechanisms a) Down detection b) Interface dampening 2 Describe loop detection and mitigation protocols a) Spanning tree types b) Spanning tree tuning techniques 3 Describe mechanisms that are available for creating loop-free topologies a) REP b) Multipath c) Switch clustering d) Flex links e) Loop detection and mitigation 4 Describe the effect of transport mechanisms and their interaction with routing protocols over different types of links 5 Describe multicast routing concepts 6 Describe the effect of fault isolation and resiliency on network design a) Fault isolation b) Fate sharing c) Redundancy

Section	Weight	Objectives
		d) Virtualization e) Segmentation
Layer 3 Control Plane	33%	1 Describe route aggregation concepts and techniques a) Purpose of route aggregation b) When to leak routes / avoid suboptimal routing c) Determine aggregation location and techniques 2 Describe the theory and application of network topology layering a) Layers and their purposes in various environments 3 Describe the theory and application of network topology abstraction a) Purpose of link state topology summarization b) Use of link state topology summarization 4 Describe the effect of fault isolation and resiliency on network design or network reliability a) Fault isolation b) Fate sharing c) Redundancy 5 Describe metric-based traffic flow and modification a) Metrics to modify traffic flow b) Third-party next hop

Section	Weight	Objectives
		6 Describe fast convergence techniques and mechanisms a) Protocol timers b) Loop-free alternates 7 Describe factors affecting convergence a) Recursion b) Microloops c) Transport 8 Describe unicast routing protocol operation [OSPF, EIGRP, ISIS, BGP, and RIP] in relation to network design a) Neighbor relationships b) Loop-free paths c) Flooding domains and stubs d) iBGP scalability 9 Analyze operational costs and complexity a) Routing policy b) Redistribution methods 10 Describe the interaction between routing protocols and topologies 11 Describe generic routing and addressing concepts a) Policy-based routing b) NAT c) Subnetting

Section	Weight	Objectives
		d) RIB-FIB relationships 12 Describe multicast routing concepts a) General multicast concepts b) Source specific c) MSDP/anycast d) PIM e) mVPN 13 Describe IPv6 concepts and operation a) General IPv6 concepts b) IPv6 security c) IPv6 transition techniques
Network Virtualization	15%	1 Describe Layer 2 and Layer 3 tunnelling technologies a) Tunnelling for security b) Tunnelling for network extension c) Tunnelling for resiliency d) Tunnelling for protocol integration e) Tunnelling for traffic optimization 2 Analyze the implementation of tunnelling a) Tunnelling technology selection b) Tunnelling endpoint selection c) Tunnelling parameter optimization of end-user applications d) Effects of tunnelling on routing e) Routing protocol selection and tuning for tunnels

Section	Weight	Objectives
Design Considerations	18%	1 Analyze various QoS performance metrics a) Application requirements b) Performance metrics 2 Describe types of QoS techniques a) Classification and marking b) Shaping c) Policing d) Queuing 3 Identify QoS strategies based on customer requirements a) DiffServ b) IntServ 4 Identify network management requirements 5 Identify network application reporting requirements 6 Describe technologies, tools, and protocols that are used for network management 7 Describe the reference models and processes that are used in network management, such as FCAPS, ITIL®, and TOGAF 8 Describe best practices for protecting network infrastructure a) Secure administrative access b) Control plane protection

Section	Weight	Objectives
		9 Describe best practices for protecting network services a) Deep packet inspection b) Data plane protection 10 Describe tools and technologies for identity management 11 Describe tools and technologies for IEEE 802.11 wireless deployment 12 Describe tools and technologies for optical deployment 13 Describe tools and technologies for SAN fabric deployment
Evolving Technologies	10%	1 Cloud a) Compare and contrast Cloud deployment models a) [i] Infrastructure, platform, and software services [XaaS] a) [ii] Performance and reliability a) [iii] Security and privacy a) [iv] Scalability and interoperability b) Describe Cloud implementations and operations b) [i] Automation and orchestration b) [ii] Workload mobility b) [iii] Troubleshooting and management b) [iv] OpenStack components

Section	Weight	Objectives
		2 Network programmability [SDN] a) Describe functional elements of network programmability [SDN] and how they interact a) [i] Controllers a) [ii] APIs a) [iii] Scripting a) [iv] Agents a) [v] Northbound vs. Southbound protocols b) Describe aspects of virtualization and automation in network environments b) [i] DevOps methodologies, tools and workflows b) [ii] Network/application function virtualization [NFV, AFV] b) [iii] Service function chaining b) [iv] Performance, availability, and scaling considerations 3 Internet of Things a) Describe architectural framework and deployment considerations for Internet of Things [IoT] a) [i] Performance, reliability and scalability a) [ii] Mobility a) [iii] Security and privacy a) [iv] Standards and compliance a) [v] Migration a) [vi] Environmental impacts on the network

352-001 Sample Questions:

01. Which two steps can be taken by the sinkhole technique?
(Choose two.)
a) Reverse the direction of an attack
b) Redirect an attack away from its target
c) Monitor attack noise, scans, and other activity
d) Delay an attack from reaching its target

02. Which resource will be targeted by a TCP SYN flood attack?

a) Connection tables on the target host
b) Syn cookies on the target host
c) Send buffers on transit routers
d) Shared memory on the routers closest to the target

03. When is the site-to-site remote access model appropriate?
a) For multiple ISDN connections
b) For modem concentrated dial-up connections
c) For a group of users in the same vicinity sharing a connection
d) For use by mobile users

04. What are two considerations to using IP Multicast delivery?
(Choose two.)
a) No congestion avoidance
b) Not for bandwidth intensive applications
c) No guaranteed delivery mechanism
d) Source sends multiple data streams out each interface

05. You are the Cisco Network Designer in Company.com. You are designing an e-Commerce module, which routing statement is correct?
a) Routing is mostly static.
b) Hardcoded IP addresses are used to support failover.
c) Inbound servers use the CSM or ACE as the default gateway.
d) VLANs between the access layer switches are used for FHRP protocols.

06. Which item will be attacked by a DoS attack?
a) Availability
b) Correlation
c) Integrity
d) Confidentiality

07. IS-IS supports which two network or interface types?
(Choose two.)
a) Point-to-point
b) Non-Broadcast Multiple Access
c) Broadcast network
d) Broadcast Multiple Access

08. Which two benefits does VoFR provide?
(Choose two.)
a) Bandwidth efficiency
b) Cell-switching
c) Congestion notification
d) Heterogeneous network

09. During periods of congestion, which two impacts are of traffic shaping on traffic flows?

(Choose two.)
a) Increased delay
b) Fewer packets dropped
c) Less bandwidth consumption
d) More packets dropped

10. In secure IP multicast, which protocol handles group key management?
a) GDOI
b) MD5
c) IPsec
d) SHA-256

Answers to 352-001Exam Questions:

Question: 01 Answer: b, c	Question: 02 Answer: a	Question: 03 Answer: c	Question: 04 Answer: a, c	Question: 05 Answer: a
Question: 06 Answer: a	Question: 07 Answer: a, c	Question: 08 Answer: a, c	Question: 09 Answer: a, b	Question: 10 Answer: a

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@nwexam.com