Designing for Cisco Internetwork Solutions (200-310)

Exam Description: The Designing for Cisco Internetwork Solutions (DESGN) exam (200-310) is a 75-minute assessment with 55–65 questions that are associated with the Cisco CCDA® Design certification. This exam requires a foundation or apprentice knowledge of network design for Cisco enterprise network architectures. CCDA certified professionals can design routed and switched network infrastructures and services involving LAN/WAN technologies for SMB or basic enterprise campus and branch networks.

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.

15% 1.0 Design Methodologies
  1.1 Describe the Cisco Design lifecycle – PBM (plan, build, manage)
  1.2 Describe the information required to characterize an existing network as part of the planning for a design change
  1.3 Describe the use cases and benefits of network characterization tools (SNMP, NBAR, NetFlow)
  1.4 Compare and contrast the top-down and bottom-up design approaches

20% 2.0 Design Objectives
  2.1 Describe the importance and application of modularity in a network
  2.2 Describe the importance and application of hierarchy in a network
  2.3 Describe the importance and application of scalability in a network
  2.4 Describe the importance and application of resiliency in a network
  2.5 Describe the importance and application of concept of fault domains in a network

20% 3.0 Addressing and Routing Protocols in an Existing Network
  3.1 Describe the concept of scalable addressing
    3.1.a Hierarchy
    3.1.b Summarization
    3.1.c Efficiency

  3.2 Design an effective IP addressing scheme
    3.2.a Subnetting
    3.2.b Summarization
    3.2.c Scalability
    3.2.d NAT

3.3   Identify routing protocol scalability considerations
        3.3.a   Number of peers
        3.3.b   Convergence requirements
        3.3.c   Summarization boundaries and techniques
        3.3.d   Number of routing entries
        3.3.e   Impact of routing table of performance
        3.3.f   Size of the flooding domain
        3.3.g   Topology

3.4   Design a routing protocol expansion
        3.4.a   IGP protocols (EIGRP, OSPF, ISIS)
        3.4.b   BGP (eBGP peering, iBGP peering

20%   4.0   Enterprise Network Design
4.1   Design a basic campus
        4.1.a   Layer 2/Layer 3 demarcation
        4.1.b   Spanning tree
        4.1.c   Ether channels
        4.1.d   First Hop Redundancy Protocols (FHRP)
        4.1.e   Chassis virtualization

4.2   Design a basic enterprise network
        4.2.a   Layer 3 protocols and redistribution
        4.2.b   WAN connectivity
                4.2.b(i)   Topologies (hub and spoke, spoke to spoke, point to point, full/partial mesh)
                4.2.b(ii)   Connectivity methods (DMVPN, get VPN, MPLS Layer 3 VPN, Layer 2 VPN, static IPsec, GRE,VTI)
                4.2.b(iii)   Resiliency (SLAs, backup links, QoS)
        4.2.c   Connections to the data center
        4.2.d   Edge connectivity
                4.2.d(i)   Internet connectivity
                4.2.d(ii)   ACLs and firewall placements
                4.2.d(iii)   NAT placement

4.3   Design a basic branch network
        4.3.a   Redundancy
                4.3.a(i)   Connectivity
                4.3.a(ii)   Hardware
                4.3.a(iii)   Service provider
        4.3.b   Link capacity
                4.3.b(i)   Bandwidth
                4.3.b(ii)   Delay

25%   5.0   Considerations for Expanding an Existing Network
5.1   Describe design considerations for wireless network architectures
        5.1.a   Physical and virtual controllers
        5.1.b   Centralized and decentralized designs

5.2   Identify integration considerations and requirements for controller-based wireless networks
    5.2.a   Traffic flows
    5.2.b   Bandwidth consumption
    5.2.c   AP and controller connectivity
    5.2.d   QoS

5.3   Describe security controls integration considerations
    5.3.a   Traffic filtering and inspection
    5.3.b   Firewall and IPS placement and functionality

5.4   Identify traffic flow implications as a result of security controls
    5.4.a   Client access methods
    5.4.b   Network access control

5.5   Identify high-level considerations for collaboration (voice, streaming video, interactive video) applications
    5.5.a   QoS (shaping vs. policing, trust boundaries, jitter, delay, loss)
    5.5.b   Capacity
    5.5.c   Convergence time
    5.5.d   Service placement

5.6   Describe the concepts of virtualization within a network design

5.7   Identify network elements that can be virtualized
    5.7.a   Physical elements (chassis, VSS, VDC, contexts)
    5.7.b   Logical elements (routing elements, tunneling, VRFs, VLANs)

5.8   Describe the concepts of network programmability within a network design
    5.8.a   APIs
    5.8.b   Controllers
    5.8.c   Application Centric Infrastructure (ACI)

5.9   Describe data center components
    5.9.a   Server load balancing basics
    5.9.b   Blocking vs. non-blocking Layer 2
    5.9.c   Layer 2 extension