Designing Cisco Network Service Architectures (300-320)

Exam Description: The Designing Cisco Network Service Architectures (ARCH) exam (300-320) is a 75-minute assessment with 60 – 70 questions associated with the Cisco Certified Design Professional certification. This exam tests a candidate's knowledge of the latest development in network design and technologies, including L2 and L3 infrastructures for the enterprise, WAN technologies, data center integration, network security and network services.

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.

22% 1.0 Advanced Addressing and Routing Solutions for Enterprise Networks

1.1 Create structured addressing designs to facilitate summarization
- 1.1.a Hierarchy
- 1.1.b Efficiency
- 1.1.c Scalability
- 1.1.d NAT

1.2 Create stable, secure, and scalable routing designs for IS-IS

1.3 Create stable, secure, and scalable routing designs for EIGRP

1.4 Create stable, secure, and scalable routing designs for OSPF

1.5 Create stable, secure, and scalable routing designs for BGP
- 1.5.a Transit prevention
- 1.5.b Basic route filtering
- 1.5.c Authentication
- 1.5.d Communities
- 1.5.e Basic traffic engineering (load distribution, creating path symmetry)
- 1.5.f Route reflectors

1.6 Determine IPv6 migration strategies
- 1.6.a Overlay (tunneling)
- 1.6.b Native (dual-stacking)
- 1.6.c Boundaries (IPv4/IPv6 translations)

20% 2.0 Advanced Enterprise Campus Networks

2.1 Design for high availability

2.1.a First Hop Redundancy Protocols
2.1.b Device virtualization

2.2 Design campus Layer 2 infrastructures
2.2.a STP scalability
2.2.b Fast convergence
2.2.c Loop-free technologies

2.3 Design multicampus Layer 3 infrastructures
2.3.a Convergence
2.3.b Load sharing
2.3.c Route summarization
2.3.d Route filtering
2.3.e VRFs
2.3.f Optimal topologies

2.4 Design a network to support network programmability
2.4.a Describe Application Centric Infrastructures (ACI)
2.4.b Select appropriate controller to meet requirements
2.4.c Identify and address key security issues with network programmability

17% 3.0 WANs for Enterprise Networks

3.1 Compare and contrast WAN connectivity options
3.1.a Dynamic Multipoint VPN (DMVPN)
3.1.b Layer 2 VPN
3.1.c MPLS Layer 3 VPN
3.1.d IPsec
3.1.e Generic Routing Encapsulation (GRE)
3.1.f Private lines

3.2 Design site-to-site VPNs
3.2.a DMVPN
3.2.b Layer 2 VPN
3.2.c MPLS Layer 3 VPN
3.2.d IPSec
3.2.e Group Encrypted Transport VPN (GETVPN)

3.3 Design for a resilient WAN strategy
3.3.a Single-homed
3.3.b Multi-homed
3.3.c Backup connectivity
3.3.d Failover

3.4 Design Extranet connectivity
3.4.a VPN
3.4.b Private lines
3.4.c Multitenant segmentation

3.5 Design Internet edge connectivity
- 3.5.a DMZ
- 3.5.b NAT
- 3.5.c Proxy functionality
- 3.5.d Resiliency
- 3.5.e Basic traffic engineering techniques (outbound/inbound load distribution, active/failover, symmetric outbound traffic flows)

17% 4.0 Enterprise Data Center Integration

4.1 Describe a modular and scalable data center network
- 4.1.a Top-of-rack
- 4.1.b End-of-row
- 4.1.c Multitenant environments
- 4.1.d Multitier topologies

4.2 Describe network virtualization technologies for the data center
- 4.2.a VPC
- 4.2.b VSS
- 4.2.c VDCs
- 4.2.d VRFs
- 4.2.e Multichassis EtherChannel
- 4.2.f VXLAN
- 4.2.g TRILL / Fabric Path

4.3 Describe high availability in a data center network
- 4.3.a VPC
- 4.3.b VSS
- 4.3.c Multichassis EtherChannel

4.4 Design data center interconnectivity
- 4.4.a OTV
- 4.4.b Private Line
- 4.4.c L2 vs. L3
- 4.4.d VPLS
- 4.4.e A-VPLS

4.5 Design data center and network integration
- 4.5.a Traffic flow
- 4.5.b Bandwidth
- 4.5.c Security
- 4.5.d Resiliency

13% 5.0 Security Services

5.1 Design firewall and IPS solutions
- 5.1.a Modes of operation
- 5.1.b Clustering
- 5.1.c High availability techniques
- 5.1.d IPS functionality and placement

5.1.e Multiple contexts

5.2 Design network access control solutions
- 5.2.a 802.1x
- 5.2.b TrustSec
- 5.2.c EAP
- 5.2.d Authentication services
- 5.2.e RBAC
- 5.2.f Basic denial of service mitigation techniques

5.3 Design infrastructure protection
- 5.3.a Infra structure ACLs
- 5.3.b CoPP
- 5.3.c Layer 2 / Layer 3 security considerations

11% 6.0 Network Services

6.1 Select appropriate QoS strategies to meet customer requirements
- 6.1.a DiffServ
- 6.1.b IntServ

6.2 Design end-to-end QoS policies
- 6.2.a Classification and marking
- 6.2.b Shaping
- 6.2.c Policing
- 6.2.d Queuing

6.3 Describe network management techniques
- 6.3.a In-band vs. out-of-band
- 6.3.b Segmented management networks
- 6.3.c Prioritizing network management traffic

6.4 Describe multicast routing concepts
- 6.4.a Source trees, shared trees
- 6.4.b RPF
- 6.4.c Rendezvous points

6.5 Design multicast services
- 6.5.a SSM
- 6.5.b PIM bidirectional
- 6.5.c MSDP