IT Certification Guru PVT.LTD

Cisco Certified Network Associate (200-125)

Exam Description: The Cisco Certified Network Associate (CCNA) Routing and Switching composite exam (200-125) is a 90-minute, 50–60 question assessment that is associated with the CCNA Routing and Switching certification. This exam tests a candidate's knowledge and skills related to network fundamentals, LAN switching technologies, IPv4 and IPv6 routing technologies, WAN technologies, infrastructure services, infrastructure security, and infrastructure management. 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 Network Fundamentals

21% 2.0 LAN Switching Technologies

23% 3.0 Routing Technologies

10% 4.0 WAN Technologies

10% 5.0 Infrastructure Services

11% 6.0 Infrastructure Security

10% 7.0 Infrastructure Management

1.0 Network Fundamentals

1.1. Compare and contrast OSI and TCP/IP models

1.2. Compare and contrast TCP and UDP protocols

1.3. Describe the impact of infrastructure components in an enterprise network

- 1.3.1. Firewalls
- 1.3.2. Access points
- 1.3.3. Wireless controllers

1.4. Describe the effects of cloud resources on enterprise network architecture

- 1.4.1. Traffic path to internal and external cloud services
- 1.4.2. Virtual services
- 1.4.3. Basic virtual network infrastructure

1.5. Compare and contrast collapsed core and three-tier architectures

1.6. Compare and contrast network topologies

- 1.6.1. Star
- 1.6.2. Mesh
- 1.6.3. Hybrid

1.7. Select the appropriate cabling type based on implementation requirements

1.8. Apply troubleshooting methodologies to resolve problems

- 1.8.1. Perform and document fault isolation
- 1.8.2. Resolve or escalate
- 1.8.3. Verify and monitor resolution

1.9. Configure, verify, and troubleshoot IPv4 addressing and subnetting

1.10. Compare and contrast IPv4 address types

- 1.10.1. Unicast
- 1.10.2. Broadcast
- 1.10.3. Multicast

1.11. Describe the need for private IPv4 addressing

1.12. Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

1.13. Configure, verify, and troubleshoot IPv6 addressing

1.14. Configure and verify IPv6 Stateless Address Auto Configuration

1.15. Compare and contrast IPv6 address types

- 1.15.1. Global unicast
- 1.15.2. Unique local
- 1.15.3. Link local
- 1.15.4. Multicast
- 1.15.5. Modified EUI 64
- 1.15.6. Autoconfiguration
- 1.15.7. Anycast

2.0 LAN Switching Technologies

2.1. Describe and verify switching concepts

- 2.1.1. MAC learning and aging
- 2.1.2. Frame switching
- 2.1.3. Frame flooding
- 2.1.4. MAC address table

2.2. Interpret Ethernet frame format

2.3. Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

2.4. Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

- 2.4.1. Access ports (data and voice)
- 2.4.2. Default VLAN

2.5. Configure, verify, and troubleshoot interswitch connectivity

- 2.5.1. Trunk ports
- 2.5.2. Add and remove VLANs on a trunk
- 2.5.3. DTP, VTP (v1&v2), and 802.1Q
- 2.5.4. Native VLAN

2.6. Configure, verify, and troubleshoot STP protocols

- 2.6.1. STP mode (PVST+ and RPVST+)
- 2.6.2. STP root bridge selection

2.7. Configure, verify and troubleshoot STP related optional features

- 2.7.1. PortFast
- 2.7.2. BPDU guard

2.8. Configure and verify Layer 2 protocols

- 2.8.1. Cisco Discovery Protocol
- 2.8.2. LLDP

2.9. Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

- 2.9.1. Static
- 2.9.2. PAGP
- 2.9.3. LACP

2.10. Describe the benefits of switch stacking and chassis aggregation

3.0 Routing Technologies

3.1. Describe the routing concepts

- 3.1.1. Packet handling along the path through a network
- 3.1.2. Forwarding decision based on route lookup
- 3.1.3. Frame rewrite

3.2. Interpret the components of a routing table

- 3.2.1. Prefix
- 3.2.2. Network mask
- 3.2.3. Next hop
- 3.2.4. Routing protocol code

3.2.5. Administrative distance
3.2.6. Metric
3.2.7. Gateway of last resort

3.3. Describe how a routing table is populated by different routing information sources
3.3.1. Admin distance

3.4. Configure, verify, and troubleshoot inter-VLAN routing
3.4.1. Router on a stick
3.4.2. SVI

3.5. Compare and contrast static routing and dynamic routing

3.6. Compare and contrast distance vector and link state routing protocols

3.7. Compare and contrast interior and exterior routing protocols

3.8. Configure, verify, and troubleshoot IPv4 and IPv6 static routing
3.8.1. Default route
3.8.2. Network route
3.8.3. Host route
3.8.4. Floating static

3.9. Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.10. Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.11. Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.12. Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.13. Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

3.14. Troubleshoot basic Layer 3 end-to-end connectivity issues

4.0 WAN Technologies

4.1. Configure and verify PPP and MLPPP on WAN interfaces using local authentication

4.2. Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication

4.3. Configure, verify, and troubleshoot GRE tunnel connectivity

4.4. Describe WAN topology options

- 4.4.1. Point-to-point
- 4.4.2. Hub and spoke
- 4.4.3. Full mesh
- 4.4.4. Single vs dual-homed

4.5. Describe WAN access connectivity options

- 4.5.1. MPLS
- 4.5.2. Metro Ethernet
- 4.5.3. Broadband PPPoE
- 4.5.4. Internet VPN (DMVPN, site-to-site VPN, client VPN)

4.6. Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)

4.7. Describe basic QoS concepts

- 4.7.1. Marking
- 4.7.2. Device trust
- 4.7.3. Prioritization
  - 4.7.3.1. Voice
  - 4.7.3.2. Video
  - 4.7.3.3. Data
- 4.7.4. Shaping
- 4.7.5. Policing
- 4.7.6. Congestion management

5.0 Infrastructure Services

5.1. Describe DNS lookup operation

5.2. Troubleshoot client connectivity issues involving DNS

5.3. Configure and verify DHCP on a router (excluding static reservations)

- 5.3.1. Server

5.3.2. Relay
5.3.3. Client
5.3.4. TFTP, DNS, and gateway options

5.4. Troubleshoot client- and router-based DHCP connectivity issues

5.5. Configure, verify, and troubleshoot basic HSRP
5.5.1. Priority
5.5.2. Preemption
5.5.3. Version

5.6. Configure, verify, and troubleshoot inside source NAT
5.6.1. Static
5.6.2. Pool
5.6.3. PAT

5.7. Configure and verify NTP operating in a client/server mode

6.0 Infrastructure Security

6.1. Configure, verify, and troubleshoot port security
6.1.1. Static
6.1.2. Dynamic
6.1.3. Sticky
6.1.4. Max MAC addresses
6.1.5. Violation actions
6.1.6. Err-disable recovery

6.2. Describe common access layer threat mitigation techniques
6.2.1. 802.1x
6.2.2. DHCP snooping
6.2.3. Nondefault native VLAN

6.3. Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering
6.3.1. Standard
6.3.2. Extended
6.3.3. Named

6.4. Verify ACLs using the APIC-EM Path Trace ACL Analysis tool

6.5. Configure, verify, and troubleshoot basic device hardening
6.5.1. Local authentication
6.5.2. Secure password

6.5.3. Access to device
6.5.3.1. Source address
6.5.3.2. Telnet/SSH

6.5.4. Login banner

6.5.5. Describe device security using AAA with TACACS+ and RADIUS

7.0 Infrastructure Management

7.1. Configure and verify device-monitoring protocols
7.1.1. SNMPv2
7.1.2. SNMPv3
7.1.3. Syslog

7.2. Troubleshoot network connectivity issues using ICMP echo-based IP SLA

7.3. Configure and verify device management
7.3.1. Backup and restore device configuration
7.3.2. Using Cisco Discovery Protocol or LLDP for device discovery
7.3.3. Licensing
7.3.4. Logging
7.3.5. Timezone
7.3.6. Loopback

7.4. Configure and verify initial device configuration

7.5. Perform device maintenance
7.5.1. Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
7.5.2. Password recovery and configuration register
7.5.3. File system management

7.6. Use Cisco IOS tools to troubleshoot and resolve problems
7.6.1. Ping and traceroute with extended option
7.6.2. Terminal monitor
7.6.3. Log events
7.6.4. Local SPAN

7.7. Describe network programmability in enterprise network architecture
7.7.1. Function of a controller
7.7.2. Separation of control plane and data plane
7.7.3. Northbound and southbound APIs