Interconnecting Cisco Networking Devices Part 2 (200-105)

Exam Description: The Interconnecting Cisco Networking Devices Part 2 exam (200-105) is a 90-minute, 45–55 question assessment that is associated with the CCNA Routing and Switching certification. This exam tests a candidate's knowledge and skills related to LAN switching technologies, IPv4 and IPv6 routing technologies, WAN technologies, infrastructure services, and infrastructure maintenance.

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.

26%   **1.0**   **LAN Switching Technologies**

1.1   Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches
  1.1.a   Access ports (data and voice)
  1.1.b   Default VLAN

1.2   Configure, verify, and troubleshoot interswitch connectivity
  1.2.a   Add and remove VLANs on a trunk
  1.2.b   DTP and VTP (v1&v2)

1.3   Configure, verify, and troubleshoot STP protocols
  1.3.a   STP mode (PVST+ and RPVST+)
  1.3.b   STP root bridge selection

1.4   Configure, verify, and troubleshoot STP-related optional features
  1.4.a   PortFast
  1.4.b   BPDU guard

1.5   Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel
  1.5.a   Static
  1.5.b   PAGP
  1.5.c   LACP

1.6   Describe the benefits of switch stacking and chassis aggregation

1.7   Describe common access layer threat mitigation techniques
  1.7.a   802.1x
  1.7.b   DHCP snooping
  1.7.c   Nondefault native VLAN

29%   **2.0**   **Routing Technologies**

2.1   Configure, verify, and troubleshoot Inter-VLAN routing

     2.1.a   Router on a stick

     2.1.b   SVI

2.2   Compare and contrast distance vector and link-state routing protocols

2.3   Compare and contrast interior and exterior routing protocols

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

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

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

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

16%   **3.0**   **WAN Technologies**

3.1   Configure and verify PPP and MLPPP on WAN interfaces using local authentication

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

3.3   Configure, verify, and troubleshoot GRE tunnel connectivity

3.4   Describe WAN topology options

     3.4.a   Point-to-point

     3.4.b   Hub and spoke

     3.4.c   Full mesh

     3.4.d   Single vs dual-homed

3.5   Describe WAN access connectivity options

     3.5.a   MPLS

     3.5.b   MetroEthernet

     3.5.c   Broadband PPPoE

     3.5.d   Internet VPN (DMVPN, site-to-site VPN, client VPN)

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

14% **4.0** **Infrastructure Services**

4.1   Configure, verify, and troubleshoot basic HSRP
   4.1.a   Priority
   4.1.b   Preemption
   4.1.c   Version

4.2   Describe the effects of cloud resources on enterprise network architecture
   4.2.a   Traffic path to internal and external cloud services
   4.2.b   Virtual services
   4.2.c   Basic virtual network infrastructure

4.3   Describe basic QoS concepts
   4.3.a   Marking
   4.3.b   Device trust
   4.3.c   Prioritization
           4.3.c. (i)   Voice
           4.3.c. (ii) Video
           4.3.c. (iii) Data
   4.3.d   Shaping
   4.3.e   Policing
   4.3.f   Congestion management

4.4   Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering
   4.4.a   Standard
   4.4.b   Extended
   4.4.c   Named

4.5   Verify ACLs using the APIC-EM Path Trace ACL analysis tool

15% **5.0** **Infrastructure Maintenance**

5.1   Configure and verify device-monitoring protocols
   5.1.a   SNMPv2
   5.1.b   SNMPv3

5.2   Troubleshoot network connectivity issues using ICMP echo-based IP SLA

5.3   Use local SPAN to troubleshoot and resolve problems

5.4   Describe device management using AAA with TACACS+ and RADIUS

5.5   Describe network programmability in enterprise network architecture
   5.5.a   Function of a controller
   5.5.b   Separation of control plane and data plane
   5.5.c   Northbound and southbound APIs

5.6   Troubleshoot basic Layer 3 end-to-end connectivity issues