CCNP_ENARSI
Implementing Cisco Enterprise Advanced Routing and Services

35% 1.0 Layer 3 Technologies

- 1.1 Troubleshoot administrative distance (all routing protocols)
- 1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)
- 1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)
- 1.4 Troubleshoot redistribution between any routing protocols or routing sources
- 1.5 Troubleshoot manual and auto-summarization with any routing protocol
- 1.6 Configure and verify policy-based routing
- 1.7 Configure and verify VRF-Lite
- 1.8 Describe Bidirectional Forwarding Detection
- 1.9 Troubleshoot EIGRP (classic and named mode)
  - 1.9.a Address families (IPv4, IPv6)
  - 1.9.b Neighbor relationship and authentication
  - 1.9.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)
  - 1.9.d Stubs
  - 1.9.e Load balancing (equal and unequal cost)
  - 1.9.f Metrics
- 1.10 Troubleshoot OSPF (v2/v3)
  - 1.10.a Address families (IPv4, IPv6)
  - 1.10.b Neighbor relationship and authentication
  - 1.10.c Network types, area types, and router types
    - 1.10.c (i) Point-to-point, multipoint, broadcast, nonbroadcast
    - 1.10.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub
    - 1.10.c (iii) Internal router, backbone router, ABR, ASBR
    - 1.10.c (iv) Virtual link
  - 1.10.d Path preference
- 1.11 Troubleshoot BGP (Internal and External)
  - 1.11.a Address families (IPv4, IPv6)
  - 1.11.b Neighbor relationship and authentication (next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)
  - 1.11.c Path preference (attributes and best-path)
  - 1.11.d Route reflector (excluding multiple route reflectors, confederations, dynamic peer)
  - 1.11.e Policies (inbound/outbound filtering, path manipulation)

20% 2.0 VPN Technologies

- 2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)
- 2.2 Describe MPLS Layer 3 VPN
- 2.3 Configure and verify DMVPN (single hub)
  - 2.3.a GRE/mGRE
  - 2.3.b NHRP
  - 2.3.c IPsec
  - 2.3.d Dynamic neighbor
  - 2.3.e Spoke-to-spoke

20% **3.0 Infrastructure Security**

- 3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)
- 3.2 Troubleshoot router security features
  - 3.2.a IPv4 access control lists (standard, extended, time-based)
  - 3.2.b IPv6 traffic filter
  - 3.2.c Unicast reverse path forwarding (uRPF)
- 3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)
- 3.4 Describe IPv6 First Hop security features (RA guard, DHCP guard, binding table, ND inspection/snooping, source guard)

25% **4.0 Infrastructure Services**

- 4.1 Troubleshoot device management
  - 4.1.a Console and VTY
  - 4.1.b Telnet, HTTP, HTTPS, SSH, SCP
  - 4.1.c (T)FTP
- 4.2 Troubleshoot SNMP (v2c, v3)
- 4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)
- 4.4 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)
- 4.5 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)
- 4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow)
- 4.7 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)