CCIE Enterprise Infrastructure v1.1

Exam Description: The CCIE Enterprise Infrastructure (v1.1) Lab Exam is an eight-hour, hands-on exam that requires that a candidate plan, design, operate, and optimize dual-stack solutions (IPv4 and IPv6) for complex enterprise networks.

Candidates are expected to program and automate the network within their exam, as per exam topics below.

The following topics are general guidelines for the content likely to be included on the exam. Your knowledge, skills, and abilities on these topics will be tested throughout the entire network lifecycle, unless explicitly specified otherwise within this document.

30% 1.0 Network Infrastructure

- 1.1 Switched campus
  - 1.1.a Switch administration
    - 1.1.a (i) Managing MAC address table
    - 1.1.a (ii) Errdisable recovery
    - 1.1.a (iii) L2 MTU
  - 1.1.b Layer 2 protocols
    - 1.1.b (i) CDP, LLDP
    - 1.1.b (ii) UDLD
  - 1.1.c VLAN technologies
    - 1.1.c (i) Access ports
    - 1.1.c (ii) Trunk ports (802.1Q)
    - 1.1.c (iii) Native VLAN
    - 1.1.c (iv) Manual VLAN pruning
    - 1.1.c (v) Normal range and extended range VLANs
    - 1.1.c (vi) Voice VLAN
  - 1.1.d EtherChannel
    - 1.1.d (i) LACP, static
    - 1.1.d (ii) Layer 2, Layer 3
    - 1.1.d (iii) Load balancing
    - 1.1.d (iv) EtherChannel misconfiguration guard
    - 1.1.d (v) Identify multichassis EtherChannel use cases
  - 1.1.e Spanning Tree Protocol
    - 1.1.e (i) PVST+, Rapid PVST+, MST
    - 1.1.e (ii) Switch priority, port priority, tuning port/path cost, STP timers
    - 1.1.e (iii) PortFast, BPDU guard, BPDU filter
    - 1.1.e (iv) Loop guard, root guard

- 1.2 Routing concepts
  - 1.2.a Administrative distance
  - 1.2.b Static routing (unicast, multicast)
  - 1.2.c Policy-based routing
  - 1.2.d VRF-Lite
  - 1.2.e VRF-aware routing with BGP, EIGRP, OSPF, and static

- 1.2.f Route leaking between VRFs using route maps and VASI
- 1.2.g Route filtering with BGP, EIGRP, OSPF, and static
- 1.2.h Redistribution between BGP, EIGRP, OSPF, and static
- 1.2.i Routing protocol authentication
- 1.2.j Bidirectional Forwarding Detection
- 1.2.k L3 MTU

1.3 EIGRP
- 1.3.a Adjacencies
- 1.3.b Best path selection
  - 1.3.b (i) Reported distance, computed distance, feasible distance, feasibility condition, successor, feasible successor
  - 1.3.b (ii) Classic metrics and wide metrics
- 1.3.c Operations
  - 1.3.c (i) General operations
  - 1.3.c (ii) Topology table
  - 1.3.c (iii) Packet types
  - 1.3.c (iv) Stuck-in-active
  - 1.3.c (v) Graceful shutdown
- 1.3.d EIGRP named mode
- 1.3.e Optimization, convergence, and scalability
  - 1.3.e (i) Query propagation boundaries
  - 1.3.e (ii) Leak-map with summary routes
  - 1.3.e (iii) EIGRP stub with leak map

1.4 OSPF (v2 and v3)
- 1.4.a Adjacencies
- 1.4.b OSPFv3 address family support
- 1.4.c Network types, area types
- 1.4.d Path preference
- 1.4.e Operations
  - 1.4.e (i) General operations
  - 1.4.e (ii) Graceful shutdown
  - 1.4.e (iii) GTSM (Generic TTL Security Mechanism)
- 1.4.f Optimization, convergence, and scalability
  - 1.4.f (i) Metrics
  - 1.4.f (ii) LSA throttling, SPF tuning
  - 1.4.f (iii) Stub router
  - 1.4.f (iv) Prefix suppression

1.5 BGP
- 1.5.a IBGP and EBGP peer relations
  - 1.5.a (i) Peer groups, templates
  - 1.5.a (ii) Active, passive
  - 1.5.a (iii) Timers
  - 1.5.a (iv) Dynamic neighbors
  - 1.5.a (v) 4-byte AS numbers
  - 1.5.a (vi) Private AS numbers
- 1.5.b Path selection
  - 1.5.b (i) Attributes
  - 1.5.b (ii) Best path selection algorithm

- 1.5.b (iii) Load balancing
- 1.5.c Routing policies
  - 1.5.c (i) Attribute manipulation
  - 1.5.c (ii) Conditional advertisement
  - 1.5.c (iii) Outbound route filtering
  - 1.5.c (iv) Standard and extended communities
  - 1.5.c (v) Multihoming
- 1.5.d AS path manipulations
  - 1.5.d (i) local-as, allowas-in, remove-private-as
  - 1.5.d (ii) AS path prepending
  - 1.5.d (iii) Regular expressions
- 1.5.e Convergence and scalability
  - 1.5.e (i) Route reflectors
  - 1.5.e (ii) Aggregation, as-set
- 1.5.f Other BGP features such as soft reconfiguration and route refresh

1.6 Multicast

- 1.6.a Layer 2 multicast
  - 1.6.a (i) IGMPv2, IGMPv3
  - 1.6.a (ii) IGMP snooping, PIM snooping
  - 1.6.a (iii) IGMP querier
  - 1.6.a (iv) IGMP filter
  - 1.6.a (v) MLD
- 1.6.b Reverse path forwarding check
- 1.6.c PIM
  - 1.6.c (i) Sparse mode
  - 1.6.c (ii) Static RP, BSR, Auto-RP
  - 1.6.c (iii) Group-to-RP mapping
  - 1.6.c (iv) Source Specific Multicast
  - 1.6.c (v) Multicast boundary, RP announcement filter
  - 1.6.c (vi) PIMv6 anycast RP
  - 1.6.c (vii) IPv4 anycast RP using MSDP
  - 1.6.c (viii) Multicast multipath

25% 2.0 Software-Defined Infrastructure

2.1 Cisco SD-Access

- 2.1.a Underlay
  - 2.1.a (i) Manual
  - 2.1.a (ii) LAN automation / PnP
  - 2.1.a (iii) Device discovery and device management
  - 2.1.a (iv) Extended nodes / policy extended nodes
- 2.1.b Overlay
  - 2.1.b (i) LISP, BGP control planes
  - 2.1.b (ii) VXLAN data plane
  - 2.1.b (iii) Cisco TrustSec policy plane
  - 2.1.b (iv) L2 flooding
  - 2.1.b (v) Native multicast
- 2.1.c Fabric design
  - 2.1.c (i) Single-site campus
  - 2.1.c (ii) Multisite
  - 2.1.c (iii) Fabric in a box

- 2.1.d Fabric deployment
  - 2.1.d (i) Host onboarding
  - 2.1.d (ii) Authentication templates
  - 2.1.d (iii) Port configuration
  - 2.1.d (iv) Multisite remote border
  - 2.1.d (v) Border priority
  - 2.1.d (vi) Adding devices to fabric
- 2.1.e Fabric border handoff
  - 2.1.e (i) SDA, SDWAN, IP transits
  - 2.1.e (ii) Peer device (Fusion router)
  - 2.1.e (iii) Layer 2 border handoff
- 2.1.f Segmentation
  - 2.1.f (i) Macro segmentation using virtual networks
  - 2.1.f (ii) Micro-level segmentation using SGTs and SGACLs

2.2 Cisco SD-WAN

- 2.2.a Controller architecture
  - 2.2.a (i) Management plane (vManage)
  - 2.2.a (ii) Orchestration plane (vBond)
  - 2.2.a (iii) Control plane (vSmart)
- 2.2.b SD-WAN underlay
  - 2.2.b (i) WAN Cloud Edge deployment (AWS, Azure, Google Cloud)
  - 2.2.b (ii) WAN Edge deployment (hardware)
  - 2.2.b (iii) Greenfield, brownfield, and hybrid deployments
  - 2.2.b (iv) System configuration (system IP, site ID, org name, vBond address)
  - 2.2.b (v) Transport configuration (underlay and tunnel interfaces, allowed services, TLOC extension)
- 2.2.c Overlay Management Protocol (OMP)
  - 2.2.c (i) OMP attributes
  - 2.2.c (ii) IPsec key management
  - 2.2.c (iii) Route aggregation
  - 2.2.c (iv) Redistribution
  - 2.2.c (v) Additional features (BGP AS path propagation, SDA integration)
- 2.2.d Configuration templates
  - 2.2.d (i) CLI templates
  - 2.2.d (ii) Feature templates
  - 2.2.d (iii) Device templates
- 2.2.e Centralized policies
  - 2.2.e (i) Data policies
  - 2.2.e (ii) Application-aware routing policies
  - 2.2.e (iii) Control policies
- 2.2.f Localized policies
  - 2.2.f (i) Access lists
  - 2.2.f (ii) Route policies

15% 3.0 Transport Technologies and Solutions

3.1 Static point-to-point GRE tunnels

3.2 MPLS

- 3.2.a Operations
  - 3.2.a (i) Label stack, LSR, LSP
  - 3.2.a (ii) LDP

- 3.2.a (iii) MPLS ping, MPLS traceroute
- 3.2.b L3VPN
  - 3.2.b (i) PE-CE routing using BGP
  - 3.2.b (ii) Basic MP-BGP VPNv4/VPNv6
- 3.3 DMVPN
  - 3.3.a Troubleshoot DMVPN Phase 3 with dual hub
    - 3.3.a (i) NHRP
    - 3.3.a (ii) IPsec/IKEv2 using preshared key

15% 4.0 Infrastructure Security and Services

- 4.1 Device security on Cisco IOS XE
  - 4.1.a Control plane policing and protection
  - 4.1.b AAA
- 4.2 Network security
  - 4.2.a Switch security features
    - 4.2.a (i) VACL, PACL
    - 4.2.a (ii) Storm control
    - 4.2.a (iii) DHCP snooping, DHCP option 82
    - 4.2.a (iv) IP Source Guard
    - 4.2.a (v) Dynamic ARP Inspection
    - 4.2.a (vi) Port security
  - 4.2.b Router security features
    - 4.2.b (i) IPv6 traffic filters
    - 4.2.b (ii) IPv4 access control lists
    - 4.2.b (iii) Unicast Reverse Path Forwarding
  - 4.2.c IPv6 infrastructure security features
    - 4.2.c (i) RA Guard
    - 4.2.c (ii) DHCP Guard
    - 4.2.c (iii) Binding table
    - 4.2.c (iv) Device tracking
    - 4.2.c (v) ND Inspection/Snooping
    - 4.2.c (vi) Source Guard
- 4.3 System management
  - 4.3.a Device management
    - 4.3.a (i) Console and VTY
    - 4.3.a (ii) SSH, SCP
    - 4.3.a (iii) RESTCONF, NETCONF
  - 4.3.b SNMP (v2c, v3)
  - 4.3.c Logging
    - 4.3.c (i) Local logging, syslog, debugs, conditional debugs
    - 4.3.c (ii) Configuration change notification and logging
    - 4.3.c (iii) Timestamps
- 4.4 Quality of Service
  - 4.4.a Differentiated Services architecture
  - 4.4.b Classification, trust boundary
  - 4.4.c Network Based Application Recognition (NBAR)
  - 4.4.d Marking DSCP values in IPv4 and IPv6 headers
  - 4.4.e Policing, shaping

- 4.4.f Congestion management and avoidance
- 4.4.g HQoS
- 4.4.h End-to-end Layer 3 QoS using MQC

4.5 Network services
- 4.5.a First-Hop Redundancy Protocols
  - 4.5.a (i) HSRP, VRRP
  - 4.5.a (ii) Redundancy using IPv6 RS/RA
- 4.5.b Time synchronization protocols
  - 4.5.b (i) NTP as a client
  - 4.5.b (ii) PTP design considerations
- 4.5.c DHCP on Cisco devices
  - 4.5.c (i) Client, server, relay
  - 4.5.c (ii) Options
  - 4.5.c (iii) SLAAC/DHCPv6 integration
  - 4.5.c (iv) Stateful, stateless DHCPv6
  - 4.5.c (v) DHCPv6 Prefix Delegation
- 4.5.d IPv4 Network Address Translation
  - 4.5.d (i) Static NAT, PAT
  - 4.5.d (ii) Dynamic NAT, PAT
  - 4.5.d (iii) Policy-based NAT, PAT
  - 4.5.d (iv) VRF-aware NAT, PAT
  - 4.5.d (v) VRF-aware Software Infrastructure (VASI) NAT

4.6 Network optimization
- 4.6.a IP SLA (ICMP, UDP, TCP probes)
- 4.6.b Tracking objects and lists
- 4.6.c Flexible NetFlow

4.7 Network operations
- 4.7.a Traffic capture
  - 4.7.a (i) SPAN, RSPAN, ERSPAN
  - 4.7.a (ii) Embedded packet capture
- 4.7.b Troubleshooting tools
  - 4.7.b (i) Data path packet trace
  - 4.7.b (ii) Conditional debugger (debug platform condition)

15% 5.0 Infrastructure Automation and Programmability

5.1 Data encoding formats
- 5.1.a JSON
- 5.1.b XML
- 5.1.c YAML
- 5.1.d Jinja

5.2 Automation and scripting
- 5.2.a EEM applets
- 5.2.b Guest shell
  - 5.2.b (i) Linux environment
  - 5.2.b (ii) CLI Python module
  - 5.2.b (iii) EEM Python module

- 5.3 Programmability
  - 5.3.a Interaction with vManage API
    - 5.3.a (i) Python requests library and Postman
    - 5.3.a (ii) Monitoring endpoints
    - 5.3.a (iii) Configuration endpoints
  - 5.3.b Interaction with Cisco DNA Center API using HTTP requests (GET, PUT, POST) via Python requests library and Postman
  - 5.3.c Deploy and verify model-driven telemetry
    - 5.3.c (i) Configure on-change subscription using gRPC