COURSE AGENDA:

CCIE Enterprise Infrastructure Certification Training Syllabus

Qualifying Exam - Implementing Cisco Enterprise Network Core Technologies v1.0 (350-401)

Architecture - 15%

1.1 Explain the different design principles used in an enterprise network

1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning

1.1.b High availability techniques such as redundancy, FHRP, and SSO

1.2 Analyze design principles of a WLAN deployment

1.2.a Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)

1.2.b Location services in a WLAN design

1.3 Differentiate between on-premises and cloud infrastructure deployments

1.4 Explain the working principles of the Cisco SD-WAN solution

1.4.a SD-WAN control and data planes elements

1.4.b Traditional WAN and SD-WAN solutions

1.5 Explain the working principles of the Cisco SD-Access solution

1.5.a SD-Access control and data planes elements

1.5.b Traditional campus interoperating with SD-Access

1.6 Describe concepts of wired and wireless QoS

1.6.a QoS components

1.6.b QoS policy

1.7 Differentiate hardware and software switching mechanisms

1.7.a Process and CEF

1.7.b MAC address table and TCAM

1.7.c FIB vs. RIB

Virtualization – 10%

2.1 Describe device virtualization technologies

2.1.a Hypervisor type 1 and 2

2.1.b Virtual machine

2.1.c Virtual switching

2.2 Configure and verify data path virtualization technologies

2.2.a VRF

2.2.b GRE and IPsec tunneling

2.3 Describe network virtualization concepts

2.3.a LISP

2.3.b VXLAN

Infrastructure – 30%

3.1 Layer 2

3.1.a Troubleshoot static and dynamic 802.1q trunking protocols

3.1.b Troubleshoot static and dynamic EtherChannels

3.1.c Configure and verify common Spanning Tree Protocols (RSTP and MST)

3.2 Layer 3

3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics)

3.2.b Configure and verify simple OSPF environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point and broadcast network types, and passive interface)

3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)

3.3 Wireless

3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise, band and channels, and wireless client devices capabilities

3.3.b Describe AP modes and antenna types

3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)

3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming

3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues

3.4 IP Services

3.4.a Describe Network Time Protocol (NTP)

3.4.b Configure and verify NAT/PAT

3.4.c Configure first hop redundancy protocols, such as HSRP and VRRP

3.4.d Describe multicast protocols, such as PIM and IGMP v2/v3

Network Assurance – 10%

4.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog

4.2 Configure and verify device monitoring using syslog for remote logging

Cisco Systems, Inc. This document is Cisco Page

4.3 Configure and verify NetFlow and Flexible NetFlow

4.4 Configure and verify SPAN/RSPAN/ERSPAN

4.5 Configure and verify IPSLA

4.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management

4.7 Configure and verify NETCONF and RESTCONF

Security – 20%

5.1 Configure and verify device access control

5.1.a Lines and password protection

5.1.b Authentication and authorization using AAA

5.2 Configure and verify infrastructure security features
5.2.a ACLs

5.2.b CoPP

5.3 Describe REST API security

5.4 Configure and verify wireless security features

5.4.a EAP

5.4.b WebAuth

5.4.c PSK

5.5 Describe the components of network security design

5.5.a Threat defense

5.5.b Endpoint security

5.5.c Next-generation firewall

5.5.d TrustSec, MACsec

5.5.e Network access control with 802.1X, MAB, and WebAuth

Automation – 15%

6.1 Interpret basic Python components and scripts

6.2 Construct valid JSON encoded file

6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG

6.4 Describe APIs for Cisco DNA Center and vManage

6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF

6.6 Construct EEM applet to automate configuration, troubleshooting, or data collection

6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

Lab Exam - Cisco CCIE Enterprise Infrastructure (v1.0) Practical Exam

1. Network Infrastructure (30%)

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 VLAN database

1.1.c vi Normal range and extended range VLANs

1.1.c vii Voice VLAN

1.1.c viii VTP

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.e Spanning Tree Protocol

1.1.e i PVST+, Rapid PVST+, MST

1.1.e ii Switch priority, port priority, 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 VRF-lite

1.2.c Static routing

1.2.d Policy Based Routing

1.2.e VRF-aware routing with any routing protocol

1.2.f Route filtering with any routing protocol

1.2.g Manual summarization with any routing protocol

1.2.h Redistribution between any pair of routing protocols

1.2.i Routing protocol authentication

1.2.j Bidirectional Forwarding Detection

1.3 EIGRP

1.3.a Adjacencies

1.3.b Best path selection

1.3.b i RD, FD, FC, 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 load balancing

1.3.d i Equal-cost

1.3.d ii Unequal-cost

1.3.d iii Add-path

1.3.e EIGRP Named Mode

1.3.f Optimization, convergence and scalability

1.3.f i Fast convergence requirements

1.3.f ii Query propagation boundaries

1.3.f iii IP FRR (single hop)

1.3.f iv Leak-map with summary routes

1.3.f v EIGRP stub with leak map

1.4 OSPF (v2 and v3)

1.4.a Adjacencies

1.4.b Network types, area types

1.4.c Path preference

1.4.d Operations

1.4.d i General operations

1.4.d ii Graceful shutdown

1.4.d iii GTSM (Generic TTL Security Mechanism)

1.4.e Optimization, convergence and scalability

1.4.e i Metrics

1.4.e ii LSA throttling, SPF tuning, fast hello

1.4.e iii LSA propagation control (area types)

1.4.e iv Stub router

1.4.e v Loop-free alternate

1.4.e vi Prefix suppression

1.5 BGP

1.5.a IBGP and EBGP peer relationships

1.5.a i Peer-group/update-group, template

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

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 Multi-homing

1.5.d AS path manipulations

1.5.d i local-AS, allowas-in, remove-private-as

1.5.d ii Prepend

1.5.d iii Regexp

1.5.e Convergence and scalability

1.5.e i Route reflector

1.5.e ii Aggregation, as-set

1.5.f Other BGP features

1.5.f i Multipath, add-path

1.5.f ii Soft reconfiguration, 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, AutoRP

1.6.c iii Group to RP Mapping

1.6.c iv Bidirectional PIM

1.6.c v Source-Specific Multicast

1.6.c vi Multicast boundary, RP announcement filter

1.6.c vii PIMv6 Anycast RP

1.6.c viii IPv4 Anycast RP using MSDP

1.6.c ix Multicast multipath

2. Software Defined Infrastructure (25%)

2.1 Cisco SD Access

2.1.a Design a Cisco SD Access solution

2.1.a i Underlay network (IS-IS, manual/PnP)

2.1.a ii Overlay fabric design (LISP, VXLAN, Cisco TrustSec)

2.1.a iii Fabric domains (single-site and multi-site using SD-WAN transit)

2.1.b Cisco SD Access deployment

2.1.b i Cisco DNA Center device discovery and device management

2.1.b ii Add fabric node devices to an existing fabric

2.1.b iii Host onboarding (wired endpoints only)

2.1.b iv Fabric border handoff

2.1.c Segmentation

2.1.c i Macro-level segmentation using VNs

2.1.c ii Micro-level segmentation using SGTs (using Cisco ISE)

2.1.d Assurance

2.1.d i Network and client health (360)

2.1.d ii Monitoring and troubleshooting

2.2 Cisco SD-WAN

2.2.a Design a Cisco SD-WAN solution

2.2.a i Orchestration plane (vBond, NAT)

2.2.a ii Management plane (vManage)

2.2.a iii Control plane (vSmart, OMP)

2.2.a iv Data plane (vEdge/cEdge)

2.2.b WAN edge deployment

2.2.b i Onboarding new edge routers

2.2.b ii Orchestration with zero-touch provisioning/Plug-And-Play

2.2.b iii OMP

2.2.b iv TLOC

2.2.c Configuration templates

2.2.d Localized policies

2.2.e Centralized policies

3. Transport Technologies and Solutions (15%)

3.1 MPLS

3.1.a Operations

3.1.a i Label stack, LSR, LSP

3.1.a ii LDP

3.1.a iii MPLS ping, MPLS traceroute

3.1.b L3VPN

3.1.b i PE-CE routing

3.1.b ii MP-BGP VPNv4/VPNv6

3.1.b iii Extranet (route leaking)

3.2 DMVPN

3.2.a Troubleshoot DMVPN Phase 3 with dual-hub

3.2.a i NHRP

3.2.a ii IPsec/IKEv2 using pre-shared key

3.2.a iii Per-Tunnel QoS

3.2.b Identify use cases for FlexVPN

3.2.b i Site-to-site, Server, Client, Spoke-to-Spoke

3.2.b ii IPsec/IKEv2 using pre-shared key

3.2.b iii MPLS over FlexVPN

4. Infrastructure Security and Services (15%)

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.a vii Private VLAN

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

4.2.d IEEE 802.1X Port-Based Authentication

4.2.d i Device roles, port states

4.2.d ii Authentication process

4.2.d iii Host modes

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

4.3.b i v2c

4.3.b ii v3

4.3.c Logging

4.3.c i Local logging, syslog, debugs, conditional debugs

4.3.c ii Timestamps

4.4 Quality of Service

4.4.a End to end L3 QoS using MQC

4.4.a i DiffServ

4.4.a ii CoS and DSCP Mapping

4.4.a iii Classification

4.4.a iv Network Based Application Recognition (NBAR)

4.4.a v Marking using IP Precedence, DSCP, CoS

4.4.a vi Policing, shaping

4.4.a vii Congestion management and avoidance

4.4.a viii HQoS, Sub-rate Ethernet Link

4.5 Network Services

4.5.a First Hop Redundancy Protocols

4.5.a i HSRP, GLBP, VRRP

4.5.a ii Redundancy using IPv6 RS/RA

4.5.b Network Time Protocol

4.5.b i Master, client

4.5.b ii Authentication

4.5.c DHCP on Cisco IOS

4.5.c i Client, server, relay

4.5.c ii Options

4.5.c iii SLAAC/DHCPv6 interaction

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 IOS-XE VRF-Aware Software Infrastructure (VASI) NAT

4.6 Network optimization

4.6.a IP SLA

4.6.a i ICMP probes

4.6.a ii UDP probes

4.6.a iii TCP probes

4.6.b Tracking object

4.6.c Flexible NetFlow

4.7 Network operations

4.7.a Traffic capture

4.7.a i SPAN

4.7.a ii RSPAN

4.7.a iii ERSPAN

4.7.a iv Embedded Packet Capture

4.7.b Cisco IOS-XE troubleshooting tools

4.7.b i Packet Trace

4.7.b ii Conditional debugger (debug platform condition)

5. Infrastructure Automation and Programmability (15%)

5.1 Data encoding formats

5.1.a JSON

5.1.b XML

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

5.3.b i HTTP request (GET, PUT, POST) via Python requests library and Postman

5.3.c Interaction with Cisco IOS XE API

5.3.c i Via NETCONF/YANG using Python ncclient library

5.3.c ii Via RESTCONF/YANG using Python requests library and Postman

5.3.d Deploy and verify model-driven telemetry

5.3.d i Configure on-change subscription using gRPC