CCDE Written and Practical Exam v3.1

Core Technology List

Description: The following technologies are associated with the CCDE Written Exam v3.1 and the CCDE Practical Exam v3.1. Candidates are expected to have a deep understanding of the listed technologies and solutions and be able to integrate them while applying design considerations as described in the CCDE Exam Topics. Each of these technologies may appear in any delivery of the exam. If applicable for the technology, candidates must expect content that is dual-stack by nature.

1.0 Transport Technologies

- 1.1 Ethernet
- 1.2 CWDM/DWDM
- 1.3 Frame Relay (migration only)
- 1.4 Cellular and broadband (as transport methods)
- 1.5 Wireless
- 1.6 Physical mediums, such as fiber and copper

2.0 Layer 2 Control Plane

- 2.1 Physical media considerations
  - 2.1.a Down detection
  - 2.1.b Interface convergence characteristics
- 2.2 Loop detection protocols and loop-free topology mechanisms
  - 2.2.a Spanning tree types
  - 2.2.b Spanning tree tuning techniques
  - 2.2.c Multipath
  - 2.2.d Switch clustering
- 2.3 Loop detection and mitigation
- 2.4 Multicast switching
  - 2.4.a IGMPv2, IGMPv3, MLDv1, MLDv2
  - 2.4.b IGMP/MLD snooping
  - 2.4.c IGMP/MLD querier
- 2.5 Fault isolation and resiliency
  - 2.5.a Fate sharing
  - 2.5.b Redundancy
  - 2.5.c Virtualization
  - 2.5.d Segmentation

3.0 Layer 3 Control Plane

- 3.1 Network hierarchy and topologies
  - 3.1.a Layers and their purposes in various environments
  - 3.1.b Network topology hiding

- 3.2 Unicast routing protocols (OSPF, EIGRP, ISIS, BGP, and RIP)
  - 3.2.a Neighbor relationships
  - 3.2.b Loop-free paths
  - 3.2.c Flooding domains
  - 3.2.d Scalability
  - 3.2.e Routing policy
  - 3.2.f Redistribution methods
  - 3.2.g Securing routing protocols
  - 3.2.h Aggregation

- 3.3 Fast convergence techniques and mechanisms
  - 3.3.a Protocols
  - 3.3.b Timers
  - 3.3.c Topologies
  - 3.3.d Loop-free alternates

- 3.4 Factors affecting convergence
  - 3.4.a Recursion
  - 3.4.b Microloops
  - 3.4.c Micro-bursts
  - 3.4.d Physical failures

- 3.5 Route aggregation
  - 3.5.a When to leak routes and avoid suboptimal routing
  - 3.5.b When to include more specific routes (up to and including host routes)
  - 3.5.c Aggregation location and techniques

- 3.6 Fault isolation and resiliency
  - 3.6.a Fate sharing
  - 3.6.b Redundancy

- 3.7 Metric-based traffic flow and modification
  - 3.7.a Metrics to modify traffic flow
  - 3.7.b Third-party next hop

- 3.8 Generic routing and addressing concepts
  - 3.8.a Policy-based routing
  - 3.8.b NAT
  - 3.8.c Subnetting
  - 3.8.d RIB-FIB relationships

- 3.9 Multicast routing concepts
  - 3.9.a General multicast concepts
  - 3.9.b Intra- and interdomain multicast

- 3.9.c MSDP, anycast, and priority cast
- 3.9.d PIM flavors
- 3.9.e RP selection and placement

4.0 Data Plane Transport Protocols (such as TCP, UDP, and QUIC)

- 4.1 Areas of application and deployment
- 4.2 Characteristics and properties
- 4.3 Security

5.0 Network and network virtualization

- 5.1 Multiprotocol Label Switching
  - 5.1.a MPLS forwarding and control plane mechanisms
  - 5.1.b MP-BGP and related address families
  - 5.1.c Label distribution protocols, such as LDP, RSVP, and BGP+label
  - 5.1.d Segment routing

- 5.2 Layer 2/3 VPN and tunneling technologies
  - 5.2.a Tunneling technology selection, such as DMVPN, GETVPN, IPsec, MPLS, and GRE
  - 5.2.b Tunneling endpoint selection
  - 5.2.c Tunneling parameter optimization of end-user applications
  - 5.2.d Effects of tunneling on routing
  - 5.2.e Routing protocol selection and tuning for tunnels
  - 5.2.f Route path selection
  - 5.2.g Overlay encapsulation and control plane protocols (such as VXLAN, LISP, and MP-BGP)
  - 5.2.h BGP EVPN
  - 5.2.i Infrastructure segmentation methods
    - 5.2.i.i VLAN
    - 5.2.i.ii PVLAN
    - 5.2.i.iii VRF-Lite
    - 5.2.i.iv SGT

- 5.3 SD-WAN
  - 5.3.a Orchestration plane
  - 5.3.b Management plane
  - 5.3.c Control plane
  - 5.3.d Data plane
  - 5.3.e Segmentation
  - 5.3.f Policy
    - 5.3.f.i Security
    - 5.3.f.ii Topologies
    - 5.3.f.iii Application-based routing

- 5.4 Migration techniques

- 5.5 Design considerations

- 5.6 QoS techniques and strategies

- 5.6.a Application requirements
- 5.6.b Infrastructure requirements

5.7 Network management techniques
- 5.7.a Traditional (such as SNMP and SYSLOG)
- 5.7.b Model-driven (such as NETCONF, RESTCONF, gNMI, and streaming telemetry)

5.8 Reference models and paradigms that are used in network management (such as FCAPS, ITIL®, TOGAF, and DevOps)

6.0 Security

6.1 Infrastructure security
- 6.1.a Device hardening techniques and control plane protection methods
- 6.1.b Management plane protection techniques
  - 6.1.b.i CPU
  - 6.1.b.ii Memory thresholding
  - 6.1.b.iii Securing device access
- 6.1.c Data plane protection techniques
  - 6.1.c.i QoS
- 6.1.d Policy plane signaling
  - 6.1.d.i RADIUS
  - 6.1.d.ii TACACS+
  - 6.1.d.iii pxGrid
  - 6.1.d.iv SXP
- 6.1.e Layer 2 security techniques
  - 6.1.e.i Dynamic ARP inspection
  - 6.1.e.ii IPDT
  - 6.1.e.iii STP security
  - 6.1.e.iv Port security
  - 6.1.e.v DHCP snooping
  - 6.1.e.vi IPv6-specific security mechanisms
  - 6.1.e.vii VACL
  - 6.1.e.viii MACsec (802.1AE)
  - 6.1.e.ix MACsec in WAN environments
- 6.1.f Wireless security technologies
  - 6.1.f.i WPA
  - 6.1.f.ii WPA2
  - 6.1.f.iii WPA3
  - 6.1.f.iv TKIP
  - 6.1.f.v AES
  - 6.1.f.vi OWE

6.2 Protecting network services
- 6.2.a Deep packet inspection
- 6.2.b Data plane protection

6.3 Perimeter security and intrusion prevention
- 6.3.a Firewall deployment modes

- 6.3.a.i Routed
- 6.3.a.ii Transparent
- 6.3.a.iii Virtualization
- 6.3.a.iv Clustering and high availability

6.3.b Firewall features
- 6.3.b.i NAT
- 6.3.b.ii Application inspection
- 6.3.b.iii Traffic zones
- 6.3.b.iv Policy-based routing
- 6.3.b.v TLS inspection
- 6.3.b.vi User identity
- 6.3.b.vii Geolocation

6.3.c IPS/IDS deployment modes
- 6.3.c.i In-line
- 6.3.c.ii Passive
- 6.3.c.iii TAP

6.3.d Detect and mitigate common types of attacks
- 6.3.d.i DoS/DDoS
- 6.3.d.ii Evasion techniques
- 6.3.d.iii Spoofing
- 6.3.d.iv Man-in-the-middle
- 6.3.d.v Botnet

6.4 Zero trust
- 6.4.a ZTNA
- 6.4.b Build policies using tools such as AI/ML
- 6.4.c Use cases, principles, and architecture
- 6.4.d Migration from classic deployments

6.5 Network control and identity management
- 6.5.a Wired and wireless network access control
- 6.5.b AAA for network access with 802.1X and MAB
- 6.5.c Guest and BYOD considerations
- 6.5.d Internal and external identity sources
- 6.5.e User- and certificate-based authentication
- 6.5.f EAP Chaining authentication method
- 6.5.g Integration with multifactor authentication

7.0 Wireless

7.1 IEEE 802.11 Standards and Protocols (up to and including Wi-Fi 7)

7.1.a Indoor and outdoor RF deployments
- 7.1.a.i Coverage
- 7.1.a.ii Throughput
- 7.1.a.iii Voice
- 7.1.a.iv Location
- 7.1.a.v High density / very high density

7.2 Enterprise wireless network

- 7.2.a High availability, redundancy, and resiliency
- 7.2.b Controller-based mobility and controller placement
- 7.2.c L2/L3 roaming
- 7.2.d Tunnel traffic optimization
- 7.2.e AP groups
- 7.2.f AP modes

8.0 Automation

- 8.1 Zero-touch provisioning
- 8.2 Infrastructure as Code (tools, awareness, and when to use)
  - 8.2.a CI/CD and automation platforms (such as Jenkins, GitLab, and GitHub)
  - 8.2.b Configuration management tools (such as Ansible)
  - 8.2.c Provisioning tools (such as Ansible and Terraform)
  - 8.2.d Orchestration platforms
  - 8.2.e Programming languages (such as Python)