CCDE v3.0 Core Technology List

Description: The following is a list of technologies associated with both the CCDE Written Exam v3.0 and the CCDE Practical Exam v3.0. Candidates are expected to have a deep understanding of these technologies. Each of these technologies may appear in any delivery of the exam.

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 protocol operation (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
- 3.3 Fast convergence techniques and mechanism
  - 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 Micro-loops
- 3.5 Route aggregation
  - 3.5.a When to leak routes / 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 MSDP/anycast
  - 3.9.c PIM

4.0 Network Virtualization

- 4.1 Multiprotocol Label Switching
  - 4.1.a MPLS forwarding and control plane mechanisms
  - 4.1.b MP-BGP and related address families
  - 4.1.c LDP
- 4.2 Layer 2 and 3 VPN and tunneling technologies

4.2.a Tunneling technology selection (such as DMVPN, GETVPN, IPsec, MPLS, GRE)
4.2.b Tunneling endpoint selection
4.2.c Tunneling parameter optimization of end-user applications
4.2.d Effects of tunneling on routing
4.2.e Routing protocol selection and tuning for tunnels
4.2.f Route path selection
4.2.g MACsec (802.1ae)
4.2.h Infrastructure segmentation methods
4.2.h.i VLAN
4.2.h.ii PVLAN
4.2.h.iii VRF-Lite

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

4.4 Migration techniques

4.5 Design considerations

4.6 QOS techniques and strategies
4.6.a Application requirements
4.6.b Infrastructure requirements

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

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

5.0 Security

5.1 Infrastructure security
5.1.a Device hardening techniques and control plane protection methods
5.1.b Management plane protection techniques
5.1.b.i CPU
5.1.b.ii Memory thresholding
5.1.b.iii Securing device access
5.1.c Data plane protection techniques
5.1.c.i QoS
5.1.d Layer 2 security techniques

- 5.1.d.i Dynamic ARP inspection
- 5.1.d.ii IPDT
- 5.1.d.iii STP security
- 5.1.d.iv Port security
- 5.1.d.v DHCP snooping
- 5.1.d.vi IPv6-specific security mechanisms
- 5.1.d.vii VACL

- 5.1.e Wireless security technologies
  - 5.1.e.i WPA
  - 5.1.e.ii WPA2
  - 5.1.e.iii WPA3
  - 5.1.e.iv TKIP
  - 5.1.e.v AES

- 5.2 Protecting network services
  - 5.2.a Deep packet inspection
  - 5.2.b Data plane protection
- 5.3 Perimeter security and intrusion prevention
  - 5.3.a Firewall deployment modes
    - 5.3.a.i Routed
    - 5.3.a.ii Transparent
    - 5.3.a.iii Virtualization
    - 5.3.a.iv Clustering and high availability
  - 5.3.b Firewall features
    - 5.3.b.i NAT
    - 5.3.b.ii Application inspection
    - 5.3.b.iii Traffic zones
    - 5.3.b.iv Policy-based routing
    - 5.3.b.v TLS inspection
    - 5.3.b.vi User identity
    - 5.3.b.vii Geolocation
  - 5.3.c IPS/IDS deployment modes
    - 5.3.c.i In-line
    - 5.3.c.ii Passive
    - 5.3.c.iii TAP
  - 5.3.d Detect and mitigate common types of attacks
    - 5.3.d.i DoS/DDoS
    - 5.3.d.ii Evasion techniques
    - 5.3.d.iii Spoofing
    - 5.3.d.iv Man-in-the-middle
    - 5.3.d.v Botnet
- 5.4 Network control and identity Management
  - 5.4.a Wired and wireless network access control

- 5.4.b AAA for network access with 802.1X and MAB
- 5.4.c Guest and BYOD considerations
- 5.4.d Internal and external identity sources
- 5.4.e Certificate-based authentication
- 5.4.f EAP Chaining authentication method
- 5.4.g Integration with multifactor authentication

6.0 Wireless

- 6.1 IEEE 802.11 Standards and Protocols
  - 6.1.a Indoor and outdoor RF deployments
    - 6.1.a.i Coverage
    - 6.1.a.ii Throughput
    - 6.1.a.iii Voice
    - 6.1.a.iv Location
    - 6.1.a.v High density / very high density
- 6.2 Enterprise wireless network
  - 6.2.a High availability, redundancy, and resiliency
  - 6.2.b Controller-based mobility and controller placement
  - 6.2.c L2/L3 roaming
  - 6.2.d Tunnel traffic optimization
  - 6.2.e AP groups
  - 6.2.f AP modes

7.0 Automation

- 7.1 Zero-touch provisioning
- 7.2 Infrastructure as Code (tools, awareness, and when to use)
  - 7.2.a Automation tools (i.e. Ansible)
  - 7.2.b Orchestration platforms
  - 7.2.c Programming Language (e.g. Python)
- 7.3 CI/CD Pipeline