CCDE Written Exam

Blueprint

The following blueprint provides general guidelines for the content to be included on the CCDE Written exam (#352-001). Please note, however, that other relevant or related topic areas may also appear.

1 IP Routing
1.1 Explain route aggregation concepts and techniques
1.1.1 Purpose of route aggregation
a. Scalability
b. Fault isolation
1.1.2 How to aggregate
1.2 Explain the theory and application of network topology abstraction and layering
1.2.1 Layers and their purpose
a. Core, aggregation, distribution, access
1.2.2 Purpose of Link State Topology Summarization
a. What is the purpose of Link State topology summarization (not how it works)
1.2.3 Use of Link State Topology Summarization
a. Where and how to build a flooding domain border
1.3 Explain the impact of fault isolation and resiliency on network design
1.3.1 What is the impact of fault isolation on network reliability
a. Separating rapid and/or massive changes from the remainder of the network, how to create fault isolation
1.3.2 What is fate sharing, and what is its impact
1.3.3 What is the impact of redundancy on convergence times
1.4 Explain metric based traffic flow and modification
1.4.1 How to engineer metrics to modify traffic flow
a. MPLS versus IGP Traffic Engineering
b. Modifying IGP Metrics to Engineer Traffic Flow
1.4.2 Understanding Traffic Flow & Metrics
1.4.3 Third Party Next Hop
a. Impact on redistribution design
1.5 Explain fast convergence techniques and mechanisms
1.5.1 Layer 2 Down Detection
a. For all media types
1.5.2 Fast hello timers
a. OSPF, EIGRP, IS-IS, BGP
1.5.3 Fast SPF Timers
a. OSPF, IS-IS

1.5.4 Recursion and Convergence
a. Impact of Third Party Next Hop & BGP recursion
1.6 Explain routing protocol operation
1.6.1 Neighbor Relationships
a. OSPF, EIGRP, IS-IS, BGP
1.6.2 Determining Loop Free Paths
a. OSPF, EIGRP, IS-IS, BGP, MPLS Constrained SPF
1.6.3 General Operation
a. OSPF, EIGRP, IS-IS, BGP; How each protocol operates
1.6.4 Flooding Domains and Stubs
a. OSPF/IS-IS flooding domains, EIGRP stubs
1.6.5 iBGP Mesh
a. Next hop mechanisms in BGP, RR's, etc.
1.7 Select lower operational costs and complexity
1.7.1 Route Filters
a. Simple versus complex
1.7.2 General
1.7.3 Redistribution
a. Simple designs, tags, route filters, etc.
1.8 Explain transport mechanisms and interaction with routing protocols
1.8.1 Link Characteristics
a. Point-to-point, point-to-multipoint, broadcast, etc.
1.8.2 RP Implementation on Various Links
a. OSPF on each link type
b. IS-IS on each link type
c. EIGRP considerations for point-to-multipoint
1.8.3 Topology Characteristics
a. Full mesh, partial mesh, ring, etc.
1.8.4 RP Implementation on Various Topologies
a. OSPF/IS-IS flood blocking, etc.
1.9 Explain generic routing and addressing concepts
1.9.1 Policy Based Routing
1.9.2 IPv6 Basics
1.10 Explain multicast routing concepts
1.10.1 General Multicast concepts

2 Tunneling
2.1 Explain how tunneling affects end service applications
2.1.1 Identify and select tunneling technologies appropriate to meet network design objectives
2.1.2 Identify where and when tunneling parameters must be tuned to optimize the operation of end user applications
2.1.3 Knowledge of issues related to Layer 2 tunneling: packet ordering, MTU, etc.
2.1.4 What technologies support Layer 2 and Layer 3 tunneling: L2TPv3, GRE, ATOM, IPsec, etc.
2.1.5 How to implement tunneling given a specific situation: tunneling Novel IPX over a Layer 3 service provider core, etc.
2.1.6 Understanding of issues related to tunneling L3(IP) in L2(ATM, MPLS)
2.2 Explain, recognize, and select tunneling techniques appropriate to the size and scale of the network requirements
2.2.1 What is the impact of different tunneling technologies on scalability (Selection of a tunneling technology with scalability as a criteria)
2.2.2 How scalability is affected based on type of tunnels (point-to-point, point-to-multipoint)
2.3 Explain how L3 routing is affected by tunneling technologies and select L3 routing protocols appropriate to implement tunneling and as passenger traffic in tunnels
2.3.1 How L3 routing is overlaid on a given tunneling technologies
2.3.2 What L3 Routing Protocol would suit a given tunneling technology, topology and scalability
2.4 Explain, recognize, and select logical and physical topologies required to meet network design requirements
2.4.1 What are the best points/nodes in network to initiate and terminate tunnels
2.4.2 Which model would fulfill the requirements (full mesh, partial mesh, hierarchical)
2.5 Explain, recognize, and select methods for interconnecting tunneling environments across one or more service provider networks
2.5.1 Describe different inter-provider tunneling models (2547, GRE, IPsec, etc.)
2.6 Explain, recognize, and select methods for steering traffic with tunnels and into tunnels
2.6.1 Class Based Tunnel Selection
2.6.2 Traffic Engineering

2.7 Explain, recognize, and select methods for providing network failover and redundancy to meet network availability requirements
2.7.1 Restoration versus Protection (IGP Fast Convergence, FRR)
2.7.2 Non-stop Forwarding versus Restoration (at the IP routing layer)
2.8 Explain, recognize, and select methods for interconnecting different types of attachment media on tunnel endpoints. Recognize and explain the differences in mapping different L2 technologies onto an L3 tunneling environment
2.8.1 Interworking
2.8.2 Mapping Layer 2 service onto Layer 3 at the edge
2.9 Explain, recognize, and select methods to manage the size and scale of broadcast domains in tunneled L2VPN environments
2.9.1 VPLS scaling issues
2.9.2 Spanning Tree issues
2.9.3 Broadcast issues across various topologies

3 QoS
3.1 Measure and interpret different QoS performance metrics
3.1.1 Correlate performance metrics to application performance
3.1.2 Knowledge of the different QoS performance metrics: one-way delay, round-trip delay, jitter, etc.
3.1.3 How to measure and interpret QoS performance metrics
3.1.4 How QoS performance metrics relate to user applications: impact of QoS metrics on application performance, etc.
3.2 Determine why, where and how to implement traffic classification, traffic conditioning and PHB
3.2.1 Explain how DiffServ QoS tools work
3.2.2 What DiffServ Terminology means (DS codepoint, Meter, DS ingress/egress node, Remark, DS domain, etc.)
3.2.3 Where to do Traffic Classification (edge and core of DS Domain)
3.2.4 What is Traffic Conditioning and where is it applied? (metering, marking, shaping and policing)
3.2.5 What are traffic profiles and meaning of in/out of profile (Token bucket)
3.2.6 What is the difference between micro-flow and DS behavior aggregate (PHB)
3.2.7 What is the impact on non-DS-compliant nodes within a DS domain on SLAs
3.2.8 What is the issue with MF Classifier and Fragmentation
3.2.9 What is the issue with re-marking and OoO packets
3.2.10 What is the purpose of shapers and droppers
3.2.11 What are different PHB models (x% minimal resources and proportional remaining link capacity, etc.)
3.2.12 What are issues with Different number/type of PHBs in different part of the network
3.2.13 What are the benefits of MF classification on edge and DS classification in the core
3.2.14 Understanding Classification/conditioning/PHB on a per customer basis or few number of templates
3.2.15 What are ways of DS Field Mapping to PHB: 1->1 or N->1 or both
3.2.16 What are tools for PHB Queue management and bounding delay, jitter, packet loss (TS, WRED, WFQ, etc.)
3.2.17 Understanding QoS provides differentiated services only when there is contention for resources

3.3 Explain operations of RSVP
3.3.1 How RSVP Application does CAC and resource reservation
3.4 Explain generic QoS requirements for common application (VoIP, Video, TCP, UDP, control plane traffic)
3.4.1 Explain QoS requirements for control plane traffic
3.4.2 What are generic VoIP Requirements
3.4.3 What are generic Video Requirements
3.4.4 What are generic TCP Requirements
3.4.5 What are generic UDP Requirements
3.4.6 Understanding of differentiation of control traffic versus data traffic
3.4.7 Where and how to define marking/conditioning of Control Traffic
3.5 Explain the techniques to avoid Class starvation when multiple classes are used (EF and non-EF)
3.5.1 How EF with a policer and MDRR/Priority Queue solves the problem
3.5.2 How minimum BW assignment per class or proportional BW assignment among all classes solves the problem
3.5.3 What is the impact of applications' traffic within a given queue with same DS or different DS codepoint
3.5.4 What is the impact of applications' traffic riding on the same node/link in case of failure
3.6 Explain the interaction of IP DSCP with other marking schemes (IP Prec, .1P, MPLS EXP, ATM, Frame Relay)
3.6.1 Interaction between DSCP and other technologies (understanding/issues/concerns)
a. Ethernet
b. ATM
c. Frame Relay
d. MPLS
e. RPR
f. IP Prec
f.1. In case of tunneling layers of marking: Differentiation between tunnel marking and data packet marking

3.7 Explain QoS based routing (PBR)
3.7.1 Situations where one has to pick one or two of the following to solve a problem (and understanding of the following)
a. BGP QoS Propagation
b. MTR
c. OER
d. PBR
e. CBTS

4 Management
4.1 Analyze network conditions and behavior to determine potential degradation or failure conditions
4.1.1 Recognize conditions from SHOW output for data plane, control plane, hardware, etc.
4.1.2 Recognize conditions from DEBUG output for data plane, control plane, hardware, etc.
4.1.3 Recognize conditions from network behaviors for data plane, control plane, hardware, etc.
4.1.4 Recognize conditions from external monitoring and reporting systems
4.2 Explain the operation and advantages of different management access mechanisms
4.2.1 How to implement out of band access to all devices in a network
4.2.2 What should be considered when defining secure access to routers
4.2.3 Recognize when and where a design will result in failure
4.3 Explain the operation and use of network management protocols
4.3.1 Differences between the versions of SNMP
4.3.2 Knowledge of puts, gets, operations (read, write)
4.3.3 Use of SNMP in SLA management
4.3.4 Identify when use of CMIP is appropriate
4.3.5 Identify when use of TMN is appropriate
4.4 Identify network management tools and their uses
4.4.1 Recognize tools used for SLA management
4.4.2 Identify use of Generic On-Line Diagnostics (GOLD)
4.4.3 Identify and Classify tools for Event Management
4.4.4 State rules for use of Syslog
4.4.5 Knowledge of where to place Netflow Collectors
4.4.6 Identify Services required for flow collection
4.4.7 Recognize Port number for Netflow
4.4.8 Identify services required for event correlation
4.5 Identify auditable factors in a network
4.5.1 Identify auditable factors in a network
4.6 Explain traffic management concepts and actions based on traffic statistics
4.6.1 What is a traffic matrix
4.6.2 When to upgrade a link or re-route traffic
4.6.3 Interpretation of historical data to predict future growth and needs

4.7 Recognize configuration management tools and best practices
4.7.1 Recognize uses of templating tools
4.7.2 Identify best practices for configuration management (logging config changes, auditing "as running" versus "as configured," consistent feature application, etc.)
4.7.3 Describe role-based configuration access

5 Security
5.1 Explain the impact of security availability design in the characteristics of a network
5.1.1 OOB Access
5.1.2 Decoupling
5.1.3 Paul Baran Model
5.1.4 Compartmentalization
5.2 Use available tools in a network security design to address identity, monitoring and correlation aspects
5.2.1 SNMP
5.2.2 Netflow
5.2.3 Syslog
5.2.4 RMON
5.2.5 DNS
5.2.6 Radius/AAA
5.2.7 Full Packet Classifiers
5.3 Explain the impact of control plane design decisions on the security of a network; implement security mechanisms to protect the control plane
5.3.1 Use and impact of addressing
5.3.2 Use and impact of area (flooding domain/summary points) placement
5.3.3 Route/Topology/Link Hiding
5.3.4 Adjacency Protection (MD5, GTSM, etc.)
5.3.5 Route Validation
5.3.6 Route Filtering
5.3.7 Routing Plan
5.3.8 Other routing techniques
5.4 Explain the impact of data plane design decisions on the security of a network; implement security mechanisms to protect the data plane
5.4.1 Infrastructure Protection
5.4.2 Policy Enforcement (QoS, BCP38)
5.5 Prepare and explain security incident preparation and response strategies in a network
5.5.1 Reaction Tools (Identification and Classification)
5.5.2 Traceback Tools
5.5.3 Remotely-Triggered Black Holes (RTBH) (destination, source, rate limit, etc.)
5.5.4 Sink Holes
5.5.5 Reactive ACLs