

Course Name: CCDE
Version: v2.0
Course Time: 80 Hrs.
Course Prerequisites: CCNP Routing & Switching
Course Outline:
<ul style="list-style-type: none"> ➤ Layer 2 control plane <ul style="list-style-type: none"> ❖ Describe fast convergence techniques and mechanisms <ul style="list-style-type: none"> • Down detection • Interface dampening ❖ Describe loop detection and mitigation protocols <ul style="list-style-type: none"> • Spanning tree types • Spanning tree tuning techniques ❖ Describe mechanisms that are available for creating loop-free topologies <ul style="list-style-type: none"> • REP • Multipath • Switch clustering • Flex links • Loop detection and mitigation ❖ Describe the impact of transport mechanisms and their interaction with routing protocols over different types of links ❖ Describe multicast routing concepts ❖ Describe the impact of fault isolation and resiliency on network design <ul style="list-style-type: none"> • Fault isolation • Fate sharing • Redundancy • Virtualization • Segmentation ➤ Layer 3 control plane <ul style="list-style-type: none"> ❖ Describe route aggregation concepts and techniques <ul style="list-style-type: none"> • Purpose of route aggregation • When to leak routes/avoid suboptimal routing • Determining aggregation location and techniques ❖ Describe the theory and application of network topology layering <ul style="list-style-type: none"> • Layers and their purposes in various environments ❖ Describe the theory and application of network topology abstraction <ul style="list-style-type: none"> • Purpose of link state topology summarization • Use of link state topology summarization ❖ Describe the impact of fault isolation and resiliency on network design or network reliability <ul style="list-style-type: none"> • Fault isolation • Fate sharing • Redundancy ❖ Describe metric-based traffic flow and modification <ul style="list-style-type: none"> • Metrics to modify traffic flow • Third-party next hop ❖ Describe fast convergence techniques and mechanisms <ul style="list-style-type: none"> • Protocol timers • Loop-free alternates ❖ Describe factors affecting convergence <ul style="list-style-type: none"> • Recursion • Microloops • Transport

- ❖ Describe unicast routing protocol operation (OSPF, EIGRP, IS-IS, BGP, and RIP) in relation to network design
 - Neighbor relationships
 - Loop-free paths
 - Flooding domains and stubs
 - iBGP scalability
- ❖ Analyze operational costs and complexity
 - Routing policy
 - Redistribution methods
- ❖ Describe the interaction between routing protocols and topologies
- ❖ Describe generic routing and addressing concepts
 - Policy-based routing
 - NAT
 - Subnetting
 - RIB-FIB relationships
- ❖ Describe multicast routing concepts
 - General multicast concepts
 - Source specific
 - MSDP/anycast
 - PIM
 - mVPN
- ❖ Describe IPv6 concepts and operation
 - General IPv6 concepts
 - IPv6 security
 - IPv6 transition techniques
- **Network virtualization**
 - ❖ Describe Layer 2 and Layer 3 tunneling technologies
 - Tunneling for security
 - Tunneling for network extension
 - Tunneling for resiliency
 - Tunneling for protocol integration
 - Tunneling for traffic optimization
 - ❖ Analyze the implementation of tunneling
 - Tunneling technology selection
 - Tunneling endpoint selection
 - Tunneling parameter optimization of end-user applications
 - Effects of tunneling on routing
 - Routing protocol selection and tuning for tunnels
- **Design considerations**
 - ❖ Analyze various Quality of Service (QoS) performance metrics
 - Application requirements
 - Performance metrics
 - ❖ Describe types of QoS techniques
 - Classification and marking
 - Shaping
 - Policing
 - Queuing
 - ❖ Identify QoS strategies based on customer requirements
 - DiffServ
 - IntServ
 - ❖ Identify network management requirements

- ❖ Identify network application reporting requirements
- ❖ Describe technologies, tools, and protocols used for network management
- ❖ Describe the reference models and processes used in network management, such as FCAPS, ITIL, and TOGA
- ❖ Describe best practices for protecting network infrastructure
 - Secure administrative access
 - Control plane protection
- ❖ Describe best practices for protecting network services
 - Deep packet inspection
 - Data plane protection
- ❖ Describe tools and technologies for identity management
- ❖ Describe tools and technologies for 802.11 wireless deployment
- ❖ Describe tools and technologies for optical deployment
- ❖ Describe tools and technologies for SAN fabric deployment

NOORAN
telecommunication