INFOSECTRAIN

CISCO CERTIFIED NETWORK ASSOCIATE (CCNA 200-301)

COURSE CONTENT

Course Content

1. **Network Fundamentals**
2. **Network Access**
3. **IP connectivit**
4. **IP Services**
5. **Security Fundamentals**
6. **Automation and programmability**

1. Network Fundamentals

- Role and function of network components
- characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe the need for private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- IPV6 address types
- Defining Wireless principles
- Virtualization fundamentals and switching concepts

2. Network Access

- Configure and verify VLANs
- Configure and verify Interswitch connectivity
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- The requirement of basic operations of Rapid PVST+ Spanning Tree Protocol
- Comparison of Cisco Wireless Architectures and AP modes
- Explanation of physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Description of AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
- Configuration of the components of a wireless LAN access for client connectivity

3. IP connectivity

- Explanation of the components of the routing table
- How a router makes a forwarding decision by default
- Configuration and verification of IPv4 and IPv6 static routing
- Configuration and verification of single area OSPFv2
- Description of the purpose of first-hop redundancy protocol

4. IP Services

- Configuration and verification of inside source NAT using static and pools
- Configuration and verification of NTP operating in a client and server mode
- The role of DHCP and DNS within the network
- The function of SNMP in network operations
- Explanation of the use of Syslog features, including facilities and levels
- Configuration and verification DHCP client and relay
- Explanation of the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
- Configuration of network devices for remote access using SSH
- Explanation of the capabilities and function of TFTP/FTP in the network

5. Security Fundamentals

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Differentiate authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure WLAN using WPA2 PSK using the GUI

6. Automation and programmability

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Differentiate authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure WLAN using WPA2 PSK using the GUI

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com