CCNA

MODULE 1 – NETWORK FUNDAMENTALS

- Explain the role and function of network components
  - ✓ 1.1.a Routers
  - ✓ 1.1.b L2 and L3 switches
  - ✓ 1.1.c Next-generation firewalls and IPS
  - ✓ 1.1.d Access points
  - ✓ 1.1.e Controllers (Cisco DNA Center and WLC)
  - ✓ 1.1.f Endpoints
  - ✓ 1.1.g Servers
- Describe characteristics of network topology architectures
  - ✓ 1.2.a 2 tier
  - ✓ 1.2.b 3 tier
  - ✓ 1.2.c Spine-leaf
  - ✓ 1.2.d WAN
  - ✓ 1.2.e Small office/home office (SOHO)
  - ✓ 1.2.f On-premises and cloud
- Compare physical interface and cabling types
  - ✓ 1.3.a Single-mode fiber, multimode fiber, copper
  - ✓ 1.3.b Connections (Ethernet shared media and point-to-point)
  - ✓ 1.3.c Concepts of PoE
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- 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
- Compare IPv6 address types
  - ✓ 1.9.a Global unicast
  - ✓ 1.9.b Unique local
  - ✓ 1.9.c Link local
  - ✓ 1.9.d Anycast
  - ✓ 1.9.e Multicast
  - ✓ 1.9.f Modified EUI 64
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
  - ✓ 1.11.a Nonoverlapping Wi-Fi channels
  - ✓ 1.11.b SSID
  - ✓ 1.11.c RF
  - ✓ 1.11.d Encryption
- Explain virtualization fundamentals (virtual machines)
- Describe switching concepts
  - ✓ 1.13.a MAC learning and aging
  - ✓ 1.13.b Frame switching
  - ✓ 1.13.c Frame flooding
  - ✓ 1.13.d MAC address table

MODULE 2 – NETWORK ACCESS

- Configure and verify VLANs (normal range) spanning multiple switches
  - ✓ Access ports (data and voice)
  - ✓ Default VLAN
  - ✓ Connectivity
- Configure and verify interswitch connectivity
  - ✓ Trunk ports
  - ✓ 802.1Q
  - ✓ Native VLAN
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
  - ✓ Root port, root bridge (primary/secondary), and other port names
  - ✓ Port states (forwarding/blocking)
  - ✓ PortFast benefits
- Compare Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)
- Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)
- Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

MODULE 3 – IP CONNECTIVITY

- Interpret the components of routing table
  - ✓ a Routing protocol code
  - ✓ b Prefix
  - ✓ c Network mask
  - ✓ d Next hop
  - ✓ e Administrative distance
  - ✓ f Metric
  - ✓ g Gateway of last resort
- Determine how a router makes a forwarding decision by default
  - ✓ a Longest match
  - ✓ b Administrative distance
  - ✓ c Routing protocol metric
- Configure and verify IPv4 and IPv6 static routing
  - ✓ a Default route
  - ✓ b Network route
  - ✓ c Host route
  - ✓ d Floating static
- Configure and verify single area OSPFv2
  - ✓ a Neighbor adjacencies
  - ✓ b Point-to-point

- ✓ c Broadcast (DR/BDR selection)
- ✓ d Router ID

- Describe the purpose of first hop redundancy protocol

MODULE 4 – IP SERVICES

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

MODULE 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

MODULE 6 – AUTOMATION AND PROGRAMMABILITY
• Explain how automation impacts network management • Compare traditional networks with controller-based networking • Describe controller-based and software defined architectures (overlay, underlay, and fabric) ✓ Separation of control plane and data plane ✓ North-bound and south-bound APIs • Compare traditional campus device management with Cisco DNA Center enabled device management • Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding) • Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible • Interpret JSON encoded data

BOOST YOUR CAREER

TechnoKraft
TRAINING & SOLUTION PVT. LTD

Give your skills a new shape, join TechnoKraft now
Learn from most experienced team in the city.
Choose from various IT courses and become industry ready.

For More Details

www.tts.net.in

9371044424
9371044428

TechnoKraft Training & Solution Pvt. Ltd.
First Floor Kanchwala Avenue,
Above Viju's Dabeli, Thatte Nagar Marg,
College Road, Nashik,
Maharashtra 422005.