

## Syllabus for practical examination of Hardware/Network Engineer

### 1. Network Fundamentals

Role and function of network components, Layered architecture, routers, L2 and L3 switches, next-generation firewalls and IPS, access points, controllers, endpoints, servers, Flow and Error Control Techniques, Routing algorithms, Congestion control, Circuit Switching, Packet Switching, Multiple Access Techniques, Mobile IP.

### 2. Characteristics of network topology architectures

2 tier, 3 tier, Spine-leaf, WAN, Small office/home office (SOHO), On-premises and cloud, physical interface and cabling types, Single-mode fiber, multimode fiber, copper, Connections (Ethernet shared media and point-to-point), Concepts of PoE, Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed), Compare TCP to UDP, IPv4 addressing and subnetting, private IPv4 addressing.

### 3. Basic Networking Concepts

Configure and verify IPv6 addressing and prefix, Compare IPv6 address types, Global unicast, Unique local, Link local, Anycast, Multicast, Modified EUI 64, IP parameters for Client OS (Windows, Mac OS, Linux), wireless principles, Nonoverlapping Wi-Fi channels, SSID, RF, Encryption, virtualization fundamentals (virtual machines), switching concepts, MAC learning and aging, Frame switching, Frame flooding, MAC address table

### 4. Network Access concepts

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, Cisco Discovery Protocol and LLDP, Configure and verify (Layer 2/Layer 3) EtherChannel (LACP), Basic operations of Rapid PVST+ Spanning Tree Protocol, Root port, root bridge (primary/secondary), and other port names. Port states (forwarding/blocking), Cisco Wireless Architectures and AP modes, Physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG), AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS), Wireless LAN access for client connectivity using GUI only, security settings, QoS profiles, and advanced WLAN settings

### 5. IP Concepts

Routing table, Routing protocol code, Network prefix, Network mask, Next hop, Administrative distance, Gateway of last resort, Longest match, Routing protocol metric, IPv4 and IPv6 static routing, Default route, Network route, Host route, Floating static, OSPFv2, Neighbor adjacencies, Point-to-point, Broadcast (DR/BDR selection), Router ID, first hop redundancy protocol

  
Additional Director  
Sikkim Judicial Academy  
Gangtok

## **6. IP Services**

Source NAT using static and pools, NTP operating in a client and server mode, DHCP and DNS within the network, SNMP in network operations syslog features, DHCP client and relay, forwarding per-hop behavior (PHB) for QoS, queuing, congestion, policing, shaping, remote access using SSH, TFTP/FTP

## **7. Network Security Concepts**

Threats, vulnerabilities, exploits, and mitigation techniques; security program elements, Configuration of device access control using local passwords, security password policies elements, multifactor authentication, certificates, and biometrics, remote access and site-to-site VPNs, configure access control lists, DHCP snooping, dynamic ARP inspection, port security, authentication, authorization, accounting, WPA, WPA2, and WPA3, configuration of WLAN using WPA2 PSK using the GUI

## **8. Network Programming**

Impact of automation in network management, controller-based networking, software defined architectures, overlay, underlay, fabric, control plane, data plane, North-bound and south-bound APIs, Cisco DNA Center enabled device management REST-based APIs

  
Additional Director  
Sikkim Judicial Academy  
Gangtok