CCIE HUB

CCNA
200-301 (v2.0)

TALK TO US :

- +91 96502 72078
- +91 70111 33431
- info@cciehub.in

1.0 NETWORK FUNDAMENTAL 20%

Explain the role and function of network components

- 1.1.a Routers
- 1.1.b Layer 2 and Layer 3 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
- 1.1.h PoE

Describe characteristics of network topology architectures

- Two-tier
- Three-tier
- Spine-leaf
- WAN
- Small office/home office (SOHO)
- On-premise and cloud

- **Compare physical interface and cabling types**
  - Single-mode fiber, multimode fiber, copper
  - Connections (Ethernet shared media and point-to-point)

- **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**

Describe IPv6 address types

- Unicast (global, unique local, and link local)
- Anycast
- Multicast
- 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 (server virtualization, containers, and VRFs)

Explain virtualization fundamentals (server virtualization, containers, and VRFs)

- Describe switching concepts
- MAC learning and aging
- Frame switching
- Frame flooding
- MAC address table

2.0 NETWORK ACCESS (20%)

Configure and verify VLANs (normal range) spanning multiple switches

- Access ports (data and voice)
- Default VLAN
- InterVLAN 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)**
- **Interpret basic operations of Rapid PVST+ Spanning Tree Protocol**
  - 2.5.a Root port, root bridge (primary/secondary), and other port names
  - 2.5.b Port states (forwarding/blocking)
  - 2.5.c PortFast
  - 2.5.d Root guard, loop guard, BPDU filter, and BPDU guard

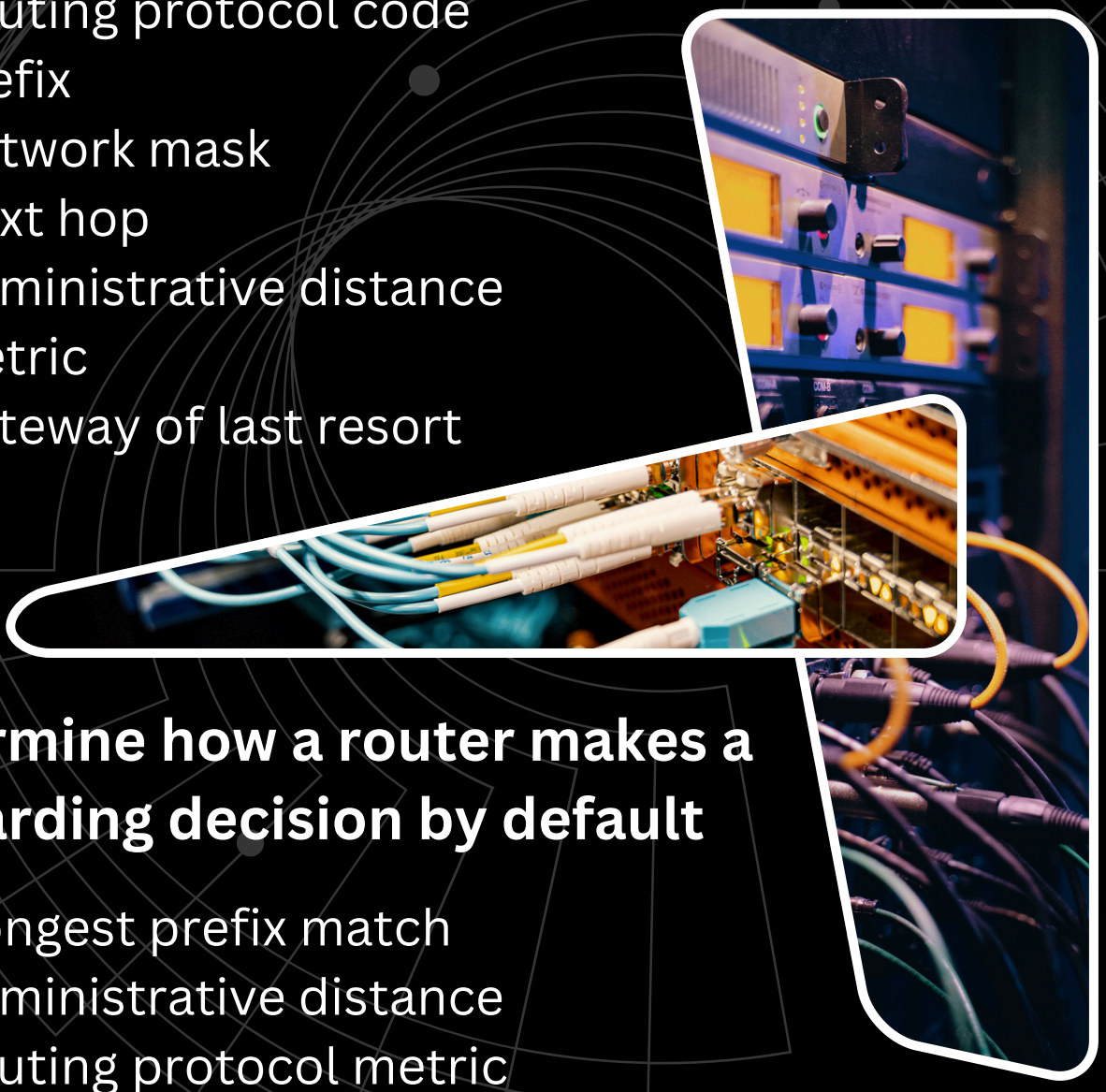
- **Describe Cisco Wireless Architectures and AP modes**
- **Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)**
- **Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)**

- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

3.0 IP CONNECTIVITY (25%)

Interpret the components of routing table

- Routing protocol code
- Prefix
- Network mask
- Next hop
- Administrative distance
- Metric
- Gateway of last resort



Determine how a router makes a forwarding decision by default

- Longest prefix match
- Administrative distance
- Routing protocol metric

- **Configure and verify IPv4 and IPv6 static routing**
  - Default route
  - Network route
  - Host route
  - Floating static
- **Configure and verify single area OSPFv2**
  - Neighbor adjacencies
  - Point-to-point
  - Broadcast (DR/BDR selection)
  - Router ID
- **Describe the purpose, functions, and concepts of first hop redundancy protocols**

4.0 IP SERVICES (10%)

- 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 behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping

- Configure network devices for remote access using SSH
- Describe the capabilities and function of TFTP/FTP in the network

5.0 SECURITY FUNDAMENTAL (15%)

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords

- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

- Describe IPsec 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 and verify WLAN within the GUI using WPA2 PSK

6.0 AUTOMATION AND PROGRAMMABILITY (10%)

- **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

- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)

- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data

CCIE HUB

Thank You

TALK TO US :

- 📞 +91 96502 72078
- 📞 +91 70111 33431
- 📧 info@cciehub.in