**Assignment**

**CCNA Assignment**

**By**

**Himanshu Kalambe**

**Guided by**

**Rohit Sir**

**MODULE 3**

1, Explain Cisco Wireless Technology.

Ans; Cisco Wireless Technology refers to the systems and devices developed by Cisco to create and manage wireless networks. These technologies enable devices like smartphones, laptops, and IoT devices to connect to the internet without needing physical cables.

**Wireless Access Points (APs)**

Function: These are devices that act as communication hubs for wireless devices to connect to a network.

Example: Think of an AP like a Wi-Fi hotspot in your home or office.

**Wireless Controllers**

Function: These manage multiple APs within a network, ensuring they work together efficiently.

Example: Imagine a conductor coordinating an orchestra; the controller ensures all APs work in harmony.

**Wireless LAN (WLAN)**

Function: A Wireless Local Area Network connects devices within a specific area using wireless communication.

Example: This is like having a local radio station in your building that only your devices can tune into.

2, List of IEEE standard.

Ans; IEEE 802.11: Standards for wireless LAN (Wi-Fi)

IEEE 802.11a: 5 GHz band, up to 54 Mbps

IEEE 802.11b: 2.4 GHz band, up to 11 Mbps

IEEE 802.11g: 2.4 GHz band, up to 54 Mbps

IEEE 802.11n: 2.4/5 GHz bands, up to 600 Mbps

IEEE 802.11ac: 5 GHz band, up to 1.3 Gbps

IEEE 802.11ax: Also known as Wi-Fi 6, operates in 2.4/5 GHz bands, up to 10 Gbps.

3, Explain Wireless Topologies.

Ans, Wireless topologies refer to the various ways wireless network devices can be arranged and connected to communicate with each other.

Ad-Hoc Topology

Description: Devices connect directly to each other without any central device or router.

Simple Example: Imagine a group of friends at a park sharing files directly from phone to phone without needing a Wi-Fi hotspot.

4, Explain Wireless security protocol and Encryption method type.

Ans; **Wireless Protocol**

WEP (Wired Equivalent Privacy)

Description: An older security protocol designed to provide a wireless network with security similar to a wired network.

Example: Think of it as an old lock on a door. It provides some security, but it's not very strong and can be easily broken into.

WPA (Wi-Fi Protected Access)

Description: An improvement over WEP with stronger security measures.

Example: Like upgrading to a better lock on your door that is harder to pick.

Note: WPA is more secure than WEP but has been replaced by WPA2 and WPA3 for better protection.

WPA2 (Wi-Fi Protected Access II)

Description: An enhanced version of WPA with even stronger security features, including advanced encryption.

Example: Imagine adding a deadbolt to your door lock, making it much harder for intruders to get in.

WPA3 (Wi-Fi Protected Access III)

Description: The latest security protocol, offering the strongest security features, including protections against brute-force attacks and better security for public networks.

Example: Like having a state-of-the-art security system with multiple layers of protection.

**ENCRYPTION Method**

TKIP (Temporal Key Integrity Protocol)

Description: Used in WPA, TKIP provides dynamic key changes to improve security over WEP.

Example: Like changing your lock’s combination every day to keep it secure.

**AES (Advanced Encryption Standard)**

Description: A very strong encryption method used in WPA2 and WPA3. AES encrypts data with robust security.

Example: Imagine putting your valuables in a safe with a complex code that is extremely difficult to crack.

5, Example of DHCP configuration.

Ans; take 1 router and switch

Connect 5 pc to the switch

Assign ip to router not on pc becoz we get it by dhcp .

In Router go to configure terminal mode

Ip dhcp pool Yashdhcp

Network 192.168.10.0 255.255.255.0

Default router : Assign router ip

Dns-server ip

6, What is ACL? Types of ACL and Example of Extended ACL.

Ans; ACL stands for Access Control List. It is a set of rules used to control the incoming and outgoing traffic on a network. ACLs are typically used in network devices such as routers and switches to provide security by filtering packets based on various criteria like IP address, protocol, port number, etc.

Types of ACL

There are mainly two types of ACLs:

**Standard ACL**

Description: Standard ACLs filter traffic based solely on the source IP address.

Use Case: Used for basic filtering, such as allowing or denying traffic from specific IP addresses.

Example Rule: Permit or deny traffic from the IP address 192.168.1.1.

**Extended ACL**

Description: Extended ACLs filter traffic based on multiple criteria, including source and destination IP addresses, protocol type, and port numbers.

Use Case: Used for more granular control over network traffic.

Example Rule: Permit HTTP traffic from 192.168.1.1 to 10.0.0.1.

7, List Of WAN connection with protocol

Ans; Wide Area Networks (WANs) connect devices across large geographic areas, such as cities, countries, or even globally. Various technologies and protocols are used to implement WAN connections.

**Point-to-Point Protocol (PPP)**

Description: A data link layer protocol used to establish a direct connection between two networking nodes.

Use Case: Dial-up connections, leased lines.

Protocol: PPP

**Integrated Services Digital Network (ISDN)**

Description: A circuit-switched telephone network system designed to allow digital transmission of voice and data over ordinary telephone copper wires.

Use Case: Voice and data transmission.

Protocols: BRI (Basic Rate Interface), PRI (Primary Rate Interface)

**Leased Line**

Description: A private bidirectional or symmetric telecommunications circuit between two or more locations provided according to a commercial contract.

Use Case: Dedicated internet access, private network interconnects.

Protocol: Various, often includes PPP, HDLC (High-Level Data Link Control)

**Digital Subscriber Line (DSL)**

Description: A family of technologies that provides digital data transmission over the wires of a local telephone network.

Use Case: High-speed internet access.

Protocols: ADSL (Asymmetric DSL), SDSL (Symmetric DSL), VDSL (Very high-bit-rate DSL)

8, Explain Frame-Relay and PPP.

Ans; **Frame Relay**

Frame Relay is a standardized wide area network technology that uses packet-switching methodology for transmitting data. It is designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in a wide area network (WAN).

Use Case:

Connecting LANs: Used to connect multiple LANs within an organization over a WAN.

Internet Backbone: Often used by ISPs to provide WAN connectivity.

**Point-to-Point Protocol (PPP)**

Point-to-Point Protocol (PPP) is a data link layer communication protocol used to establish a direct connection between two networking nodes. It provides a standard method for transporting multi-protocol datagrams over point-to-point links.

Use Case:

Dial-up Connections: Widely used in dial-up internet access.

Leased Lines: Commonly used on leased line connections, such as T1 or E1 links.

9, What is NAT? explain with one example.

Ans; NAT stands for Network Address Translation. It is a technique used in networking to translate private IP addresses within a local network into public IP addresses used on the Internet, and vice versa. NAT enables multiple devices within a local network to share a single public IP address.

Example of NAT:

Let's say you have a home network with several devices connected to a router that performs NAT.

Device IP Addresses: Your devices within the home network have private IP addresses assigned by the router, such as 192.168.1.10 for a laptop and 192.168.1.20 for a smartphone.

Public IP Address: Your ISP provides your router with a single public IP address, let's say 203.0.113.1.

Translation: When your laptop (192.168.1.10) sends a request to access a website, for example, www.google.com:

The router translates the source IP address of the outgoing packets from 192.168.1.10 to 203.0.113.1.

The website www.example.com sees incoming traffic from 203.0.113.1.

When the website responds, it sends the response to 203.0.113.1.

The router then uses its NAT table to forward the response back to the laptop 192.168.1.10.

10, What is HDLC? Which command using to show in software.

Ans; HDLC stands for High-Level Data Link Control. It is a bit-oriented data link protocol that is commonly used to encapsulate PPP (Point-to-Point Protocol) frames for transmission over synchronous serial lines.

**Protocol Type** HDLC is a Layer 2 protocol (Data Link Layer) that provides error detection and correction capabilities for data transmitted between devices over serial links

Command to Show HDLC in Software:

show interfaces serial <interface-id>

11, What is Encapsulation? example of GRE Tunnel.

Ans; Encapsulation in networking refers to the process of wrapping data with additional headers as it moves from one layer of the OSI (Open Systems Interconnection) model to another. This allows data to be transmitted over different types of networks and protocols.

GRE (Generic Routing Encapsulation) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links. It is often used to create a private, secure communication tunnel between two endpoints over a public network, such as the Internet.