**CCNA - IP connectivity and IP services**

**Module – 3**

**• Explain Cisco Wireless Technology.**

**Ans.** Cisco wireless technology enables the connectivity of devices to networks using radio waves, much like a walkie-talkie or a cell phone. It serves as a digital communication pathway between devices such as smartphones, tablets, and laptops, and the main network infrastructure.

Imagine you are at home with several devices connected to the internet. Cisco wireless technology uses a central wireless router to distribute signals across your space. This router acts as a hub, sending and receiving data over radio waves to and from your devices. This is similar to how a telephone network connects different homes through physical lines, but with radio waves instead of wires.

Cisco offers a range of wireless networking solutions to improve signal strength, stability, and security. For instance:

1. **Wireless Access Points (WAPs**): These devices serve as relay points for wireless signals, enhancing coverage in large or complex spaces.
2. **Wireless Controllers:** These manage multiple access points, optimizing network performance and providing better control over devices.
3. **Security:** Cisco wireless technology integrates various security protocols to protect your data from unauthorized access.
4. **Network Management:** Cisco provides tools for monitoring and managing the wireless network, ensuring efficient and reliable performance.

**• List of IEEE standard.**

**Ans.** IEEE standards are guidelines and specifications developed by the institute of Electrical and Electronics Engineers for various technologies and industries. In the context of wireless networking and communication, some of the key IEEE standards include.

1. IEEE 802.11: wi-fi, covering different generation like 802.11a/b/g/n/ac/ax.
2. IEEE 802.3: Ethernet, for wired networks.
3. IEEE 802.15: Personal area networks, including Bluetooth.
4. IEEE 802.16: WiMAX, for wireless broadband.
5. IEEE 802.1: Bridging and network management for secure and efficient networking.

**• Explain Wireless Topologies.**

**Ans.** Wireless topologies in a wireless network are connected and communication with each. There are Three main types of wireless topologies.

1. **Star Topology:** In a star topology, each device is connected to a central device (like a router or access point). The central device manages communication and data flow between devices.
2. **Mesh Topology:** In a mesh topology, devices connect directly to each other, creating multiple paths for data to travel. This allows for efficient data transfer and provides redundancy if a connection fails.
3. **Ad-hoc Topology:** In an ad-hoc topology, devices connect directly to each other without a central device. This type of network is flexible and can be quickly set up, but may have limited range and performance.

**• Explain Wireless security protocol and Encryption method type.**

**Ans.** The Wireless security protocol is protect wireless networks from unauthorized access. There are several main types:

1. WPA (Wi-Fi Protected Access): Improve over WEP with stronger encryption. WPA uses TKIP (Temporal Key Integrity Protocol) for encryption.
2. WPA2: A more secure version of WPA. It uses AES (Advanced Encryption Standard) encryption, providing much stronger security and performance.
3. WPA3: The latest protocol, offers the stronger security with advanced encryption methods.

**• Example of DHCP configuration.**

**Ans.** A DHCP (Dynamic Host Configuration Protocol) configuration allow network devices to automatically receive IP addresses and network settings. Here’s an example of how to set up DHCP in a network.

1. **Configuration the DHCP server:**

* Specify the IP address range: Define the range of IP address that the server can assign to devices.
* For ex.: 10.0.0.100 to 10.0.0.200
* Set the lease time: Determine how long devices can keep their assigned IP address.
* For Ex. 24 hours
* Define the default gateway: Specify the IP address of the router that devices will use to access other networks.
* For Ex. 10.0.0.1
* Set DNS server: Define the IP addresses of the DNS servers for domain name resolution.
* For Ex. 8.8.8.8 and 8.8.4.4

1. **Example configuration snippet (in a DHCP Server configuration file):**

subnet 10.0.0.0 netmask 255.255.255.0 {

range 10.0.0.100 10.0.0.200;

option routers 10.0.0.1;

option domain-name-servers 8.8.8.8, 8.8.4.4;

default-lease-time 86400;

max-lease-time 172800;

}

**• What is ACL? Types of ACL and Example of Extended ACL.**

**Ans.** ACL stand for Access Control list, a set of rules used to filter and control network traffic.

**Types of ACL:**

* **Standard ACL:** Filter traffic based on source IP addresses.
* **Extended ACL:** Filter traffic based on source and destination IP addresses, protocol, and ports.
* **Ex. Of Extended ACL:**
  + access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.1 eq 80
  + access-list 100 deny ip any any

**• Example of Port security in Switch.**

**Ans.** Port security is a feature on switches that control which devices can connect to specific switch ports.

**Example of port security configuration:**

Enable port security on a specific port:

switchport port-security

Set the maximum number of allowed MAC addresses:

switchport port-security maximum 2

Specify an action if a security violation occurs (e.g., protect, restrict, or shutdown):

switchport port-security violation shutdown

Optionally, restrict the port to specific MAC addresses:

switchport port-security mac-address 00:11:22: 33:44:55

switchport port-security mac-address 00:11:22: 33:44:66

**• List Of WAN connection with protocol.**

**Ans.**

1. **DSL (Digital Subscriber Line):** Uses PPPoE (Point-to-Point Protocol over Ethernet).
2. **Cable**: Often uses DHCP (Dynamic Host Configuration Protocol).
3. **Fiber Optic**: Typically uses IP-based protocols like DHCP.
4. **T1/E1:** Uses PPP (Point-to-Point Protocol) or HDLC (High-Level Data Link Control).
5. **MPLS (Multiprotocol Label Switching):** Uses its own MPLS protocol to manage data paths.
6. **Satellite:** Typically uses TCP/IP and other standard network protocols**.**
7. **Leased Line:** Can use PPP or HDLC protocols.

**• Explain Frame-Relay and PPP.**

**Ans**. Frame Relay and PPP (Point-to-Point Protocol) are two different protocols used in networking, especially for WAN connections.

**Frame Relay:**

* A WAN technology that provides fast, cost-effective data transmission.
* Uses a shared network to create virtual circuits, which are logical paths for data.
* Efficient for bursty traffic and is often used for connecting multiple sites.
* Data is transmitted in frames, which include headers with address information.
* Typically used for enterprise networking, especially in connecting branch offices.

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

* A protocol used to establish direct connections between two network points.
* Supports multiple protocols, including IP and IPv6.
* Provides features like error checking, data compression, and authentication.
* Can be used over various media types such as phone lines, DSL, and fiber optics.
* Often used in VPNs and internet connections, as it can carry multiple types of traffic.

**• What is NAT? explain with one example.**

**Ans.** NAT (Network Address Translation) is a method of modifying IP addresses as data packets pass through a network device, such as a router. It helps improve security and manage limited IP addresses.

**How NAT works:**

* A router translates internal private IP addresses (used within a local network) to a public IP address (used on the internet).
* This allows multiple devices in a local network to share a single public IP address.

**Example of NAT:**

1. **Private Network**: A computer with private IP address 192.168.1.100 sends a request to a web server on the internet.
2. **Router**: The router receives the request and translates the private IP address 192.168.1.100 to its public IP address (e.g., 203.0.113.1).
3. **Internet**: The request is sent to the web server with the public IP address.
4. **Response**: The web server responds to the public IP address, which the router receives and translates back to the private IP address 192.168.1.100.
5. **Delivery**: The response is then forwarded to the original computer.

**• What is HDLC? Which command using to show in software.**

**Ans.** HDLC (High-Level Data Link Control) is a link Layer Protocol Used for point-to-point communication in WAN connections. It provides error detection and can frame data for transmission.

In network devices like routers, HDLC is often used for serial connection.

To show HDLC configuration and information on a router, you can use the command:

‘show interfaces serial <interface number>’

This command display information about a specific serial interface, including whether HDLC is the protocol in use, and other detail such as IP address, encapsulation type, and status. Replace ‘<interface number>’ with the actual interface number you want to check. For ex.

‘show interface serial 0/0/0’

**• What is Encapsulation? example of GRE Tunnel.**

**Ans.**  Encapsulation is the process of wrapping data in a specific protocol format to be transmitted across a network. It involves adding headers (and sometimes trailers) to the data packet, allowing it to be routed through the network and interpreted correctly by different devices.

**Example of GRE Tunnel:**

1. **Purpose:** GRE (Generic Routing Encapsulation) creates a virtual point-to-point connection between two networks over the internet.
2. **Encapsulation:** GRE wraps data packets in its own header, allowing different protocols to be tunneled through the internet.
3. **Creation:**

* Source: Define the tunnel source IP address.
* Destination: Define the tunnel destination IP address.
* Tunnel interface: Create a virtual interface on the router for the GRE tunnel.

**GRE Tunnel configuration example on a router:**

1. Create a GRE tunnel interface:

* interface tunnel0

1. Configure the tunnel source and destination:

* tunnel source 192.168.1.1
* tunnel destination 10.0.0.1

1. Assign an IP address to the tunnel interface:

* ip address 172.16.1.1 255.255.255.0