Module-3

CCNA - Ip connectivity and IP services

* Explain cisco wireless Technology.

Cisco Wireless Technology helps you connect to the internet without using cables. It's like the Wi-Fi you use at home, but stronger and more secure. It's used in offices, schools, hospitals, and public places like coffee shops and airports.

* + List of IEEE standard.

1. IEEE 802.3 - Ethernet

2. IEEE 802.11 - Wi-Fi

3. IEEE 802.15 - Bluetooth, Zigbee

4. IEEE 754 - Floating-Point Arithmetic

5. IEEE 1284 - Parallel Interface

6. IEEE 1394 - FireWire

* + Explain Wireless Topologies.

**1. Ad-Hoc:** Devices connect directly to each other.

**2. Infrastructure:** Devices connect to a central access point (AP).

**3. Mesh:** Devices connect to each other and to APs, forming a network.

**4. Point-to-Point:** Two devices connect directly, often for long-range links.

**5. Point-to-Multi-Point:** One device connects to multiple devices.

* + Explain Wireless security protocol and Encryption method type.

Wireless Security Protocols:

**1. WEP (Wired Equivalent Privacy):** Oldest protocol, uses static keys, vulnerable to hacking.

**2. WPA (Wi-Fi Protected Access):** Introduced TKIP encryption, improved security, but still vulnerable.

**3. WPA2 (Wi-Fi Protected Access 2):** Uses AES encryption, more secure than WPA, but vulnerable to KRACK attack.

**4. WPA3 (Wi-Fi Protected Access 3):** Latest protocol, uses individualized data encryption, more secure than WPA2.

Encryption Methods:

**1. AES (Advanced Encryption Standard):** Symmetric-key block cipher, widely used, secure.

**2. TKIP (Temporal Key Integrity Protocol):** Used in WPA, provides per-packet key mixing, less secure than AES.

**3. CCMP (Counter Mode CBC-MAC Protocol):** Used in WPA2, provides data confidentiality, integrity, and authentication.

Best Practices:

- Use WPA3 protocol

- Use AES encryption

- Set strong passwords

- Regularly update firmware and software

- Use a firewall and antivirus software

* + Example of DHCP configuration.

Here's an example of DHCP configuration:

DHCP Server Configuration:

- IP address: 192.168.1.1

- Subnet mask: 255.255.255.0

- DHCP scope: 192.168.1.100 to 192.168.1.200

- Lease duration: 1 day

- Default gateway: 192.168.1.1

- DNS server: 8.8.8.8

DHCP Client Configuration:

- Obtain IP address automatically: Yes

- Obtain DNS server address automatically: Yes

Example of DHCP configuration in Cisco IOS:

Router(config)# ip dhcp pool MYPOOL

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

Router(dhcp-config)# dns-server 8.8.8.8

Router(dhcp-config)# lease 1

This is just a basic example, and actual DHCP configurations may vary depending on the specific requirements and network architecture.

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

ACL (Access Control List) is a set of rules that controls network traffic by filtering incoming and outgoing packets based on source/destination IP addresses, ports, and protocols.

Types of ACL:

1. Standard ACL

2. Extended ACL

3. Named ACL

4. Numbered ACL

5. Dynamic ACL

6. Reflexive ACL

Example of an extended ACL:

Router(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.10.10.10 eq 80

Explanation:

- 101 is the ACL number

- permit allows traffic

- tcp specifies the protocol

- 192.168.1.0 0.0.0.255 specifies the source IP address range

- host 10.10.10.10 specifies the destination IP address

- eq 80 specifies the destination port (HTTP)

* + Example of Port security in Switch.

Example of port security configuration on switch:

Switch(config)# interface FastEthernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security mac-address 0001.0001.0001

Switch(config-if)# switchport port-security maximum 1

Switch(config-if)# switchport port-security violation shutdown

Explanation:

- Enable port security on interface FastEthernet0/1

- Set the MAC address allowed on the port

- Limit the number of MAC addresses to 1

- Shutdown the port if a security violation occurs

* + List Of WAN connection with protocol.

1. Leased Line - HDLC, PPP

2. Frame Relay - LMI, DLCI

3. ISDN (Integrated Services Digital Network) - PPP, HDLC

4. DSL (Digital Subscriber Line) - PPPoE, PPPoA

5. Cable Modem - DOCSIS

6. MPLS (Multiprotocol Label Switching) - LDP, RSVP

7. VPN (Virtual Private Network) - IPSec, L2TP, PPTP

8. ATM (Asynchronous Transfer Mode) - LANE, MPOA

* + Explain Frame-Relay and PPP.

**Frame Relay**

- WAN protocol (Layer 2)

- Packet-switching technology

- Uses virtual circuits (PVCs/SVCs)

- Supports multiple protocols

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

- WAN protocol (Layer 2)

- Connects two devices over a serial link

- Supports multiple protocols

- Provides error detection, authentication, and encryption

* + What is NAT? explain with one example.

NAT (Network Address Translation) allows multiple devices on a private network to share a single public IP address when accessing the Internet.

**NAT example:**

A home network with 3 devices (laptops) uses private IP addresses (192.168.1.1, 192.168.1.2, 192.168.1.3). The router uses NAT to share a single public IP address (e.g., 202.123.123.1) when accessing the Internet.

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

HDLC (High-Level Data Link Control) is a data link layer protocol that provides error-free transfer of data between devices over point-to-point or multipoint networks.

To show HDLC configuration and status, you can use the following command in Cisco IOS software:

show running-config | include hdlc

or

show interfaces | include hdlc

* + What is Encapsulation? example of GRE Tunnel.

Encapsulation is the process of wrapping data from a higher layer (e.g., IP) with a header and possibly a trailer from a lower layer (e.g., Ethernet), creating a new packet.

Example of configuring a GRE (Generic Routing Encapsulation) tunnel between two routers:

Router A (10.1.1.1):

- Tunnel source: 10.1.1.1

- Tunnel destination: 10.2.2.2

- Tunnel mode: GRE

Router B (10.2.2.2):

- Tunnel source: 10.2.2.2

- Tunnel destination: 10.1.1.1

- Tunnel mode: GRE

Traffic between the two routers is encapsulated in GRE packets and transmitted over the tunnel.