**Assignment-3**

1. **Explain Cisco Wireless Technology ?**

Cisco Wireless Technology encompasses a range of wireless networking solutions designed for businesses, enterprises, and service providers. It includes wireless access points (APs), controllers, and network management tools that ensure secure, scalable, and high-performance wireless connectivity.

### Key Components of Cisco Wireless Technology

#### 1. Cisco Wireless Access Points (APs)

* Cisco offers a variety of indoor and outdoor APs that support Wi-Fi 6 (802.11ax) and older standards like Wi-Fi 5 (802.11ac).
* Examples: Cisco Catalyst 9100 Series, Aironet Series.
* Features include:
  + High-density support for multiple devices.
  + Integrated security features like Cisco Umbrella.
  + AI/ML-driven analytics for performance optimization.

#### 2. Cisco Wireless Controllers

* Manage multiple APs to provide centralized configuration, security, and performance optimization.
* Types:
  + On-Premises Controllers: Catalyst 9800 Series (hardware-based).
  + Cloud-Based Management: Cisco Meraki (cloud-managed solutions).
  + Embedded Controllers: Controllers built into APs for small-scale deployments.
* Features include:
  + Automated RF management.
  + Seamless roaming for users.
  + Integration with Cisco DNA Center for AI-driven analytics.

#### 3. Cisco Wireless Security

* Cisco ensures wireless security using multiple layers of protection, including:
  + WPA3 Encryption for secure wireless communication.
  + Cisco Identity Services Engine (ISE) for network access control.
  + Cisco Umbrella for cloud-based security.
  + Rogue AP detection and wireless intrusion prevention systems (WIPS).

#### 4. Cisco DNA (Digital Network Architecture) for Wireless

* Cisco DNA Center provides centralized network automation, assurance, and analytics.
* AI/ML-driven optimization for proactive troubleshooting.
* Application visibility and policy enforcement.

#### 5. Cisco Meraki Wireless (Cloud-Managed)

* Cloud-based dashboard for managing wireless networks.
* Zero-touch deployment for easy setup.
* Advanced analytics and security features.
* Ideal for organizations looking for simplified IT operations.

### Benefits of Cisco Wireless Technology

* High Performance & Reliability: Advanced RF management, seamless roaming, and AI-driven optimizations.
* Security & Compliance: End-to-end encryption, identity-based access control, and integrated threat defense.
* Scalability: Supports small businesses to large enterprises with modular and cloud-based solutions.
* Ease of Management: Centralized control through Cisco DNA Center or Meraki Dashboard.

Cisco Wireless Technology is widely used in enterprises, healthcare, education, and public sector environments to provide secure and efficient wireless connectivity. Would you like a deeper dive into any specific aspect?

1. **List of IEEE standards ?**

IEEE (Institute of Electrical and Electronics Engineers) has established various standards for networking, communication, and technology. Below is a list of key IEEE standards categorized based on their application:

### 1. IEEE 802 Standards (Networking & Communication)

These standards define networking technologies, including Ethernet, Wi-Fi, and Bluetooth.

#### A. IEEE 802.3 (Ethernet Standards)

* 802.3 – Ethernet (10 Mbps, CSMA/CD)
* 802.3u – Fast Ethernet (100 Mbps)
* 802.3ab – Gigabit Ethernet (1 Gbps over twisted pair)
* 802.3ae – 10 Gigabit Ethernet
* 802.3ba – 40/100 Gigabit Ethernet
* 802.3by – 25 Gigabit Ethernet
* 802.3bs – 200/400 Gigabit Ethernet

#### B. IEEE 802.11 (Wi-Fi Standards)

* 802.11 – Original Wi-Fi standard (2 Mbps, 2.4 GHz)
* 802.11a – 5 GHz, 54 Mbps
* 802.11b – 2.4 GHz, 11 Mbps
* 802.11g – 2.4 GHz, 54 Mbps
* 802.11n (Wi-Fi 4) – 2.4/5 GHz, MIMO support, up to 600 Mbps
* 802.11ac (Wi-Fi 5) – 5 GHz, MU-MIMO, up to 6.9 Gbps
* 802.11ax (Wi-Fi 6 & Wi-Fi 6E) – 2.4/5/6 GHz, OFDMA, up to 9.6 Gbps
* 802.11be (Wi-Fi 7, upcoming) – 6 GHz, ultra-high speed, up to 30 Gbps

#### C. IEEE 802.15 (Wireless Personal Area Networks - WPAN)

* 802.15.1 – Bluetooth (short-range wireless)
* 802.15.4 – Zigbee (IoT, low-power networks)

#### D. IEEE 802.16 (WiMAX)

* 802.16d – Fixed WiMAX (broadband wireless)
* 802.16e – Mobile WiMAX (for mobile broadband)

#### E. IEEE 802.20 (Mobile Broadband Wireless Access - MBWA)

* Designed for high-speed wireless Internet access in mobile environments.

### 2. IEEE Electrical & Power Standards

* IEEE 1547 – Standard for Interconnecting Distributed Energy Resources with Power Systems.
* IEEE 519 – Harmonic control in electrical power systems.
* IEEE 1100 – Power system grounding.

### 3. IEEE Computer Standards

* IEEE 488 (GPIB) – General Purpose Interface Bus for communication between instruments.
* IEEE 1394 (FireWire) – High-speed data transfer, similar to USB.

### 4. IEEE Security Standards

* IEEE 802.1X – Port-based network access control (used in Wi-Fi security).
* IEEE 802.11i – Wireless security (WPA2 encryption).

1. **Explain Wireless Topologies ?**

### Wireless Topologies: Types and Applications

Wireless network topologies define how devices (nodes) are arranged and communicate in a wireless network. The choice of topology depends on factors like network size, data traffic, coverage, and reliability. Below are the main types of wireless topologies:

## 1. Point-to-Point (P2P) Topology

Description:

* A direct wireless link between two devices.
* Often used for long-distance communication.

Example Use Cases:

* Connecting two buildings wirelessly (e.g., corporate offices, warehouses).
* Backhaul links for cellular networks.

Advantages:  
 High security and reliability.  
 Low interference.  
 Efficient for dedicated connections.

Disadvantages:  
 Limited scalability (only two devices).  
 Requires precise alignment for directional antennas.

## 2. Point-to-Multipoint (P2MP) Topology

Description:

* A single central node (e.g., a base station) connects to multiple client nodes.
* Common in Wi-Fi networks, where an access point connects multiple devices.

Example Use Cases:

* Wi-Fi networks in homes, offices, and public areas.
* Wireless Internet Service Providers (WISPs).

Advantages:  
 Supports multiple clients.  
 Cost-effective compared to wired solutions.  
 Easy to scale.

Disadvantages:  
 Increased network congestion with too many clients.  
 Performance degrades with distance.

## 3. Mesh Topology

Description:

* Each device (node) connects to multiple other nodes, forming a web-like structure.
* Nodes can relay data dynamically, improving redundancy.

Example Use Cases:

* Smart cities and IoT networks.
* Military and disaster recovery networks.
* Large-scale enterprise Wi-Fi networks.

Advantages:  
 Highly resilient and fault-tolerant.  
 Extends coverage without requiring more infrastructure.  
 Automatic rerouting if a node fails.

Disadvantages:  
 High setup complexity.  
 Increased latency due to multiple hops.

## 4. Infrastructure Topology

Description:

* Uses access points (APs) to manage communication between devices.
* Commonly found in enterprise and public Wi-Fi networks.

Example Use Cases:

* Office and campus Wi-Fi.
* Airports, hotels, and public hotspots.

Advantages:  
 Centralized management and security.  
 Scalable for large networks.  
 Better control over bandwidth and performance.

Disadvantages:  
 AP failure can disrupt the network.  
 More expensive than ad-hoc networks.

## 5. Ad-Hoc (Peer-to-Peer) Topology

Description:

* Devices connect directly without a central access point.
* A temporary and decentralized network.

Example Use Cases:

* Military or emergency networks.
* IoT and sensor-based communication.
* File-sharing between devices without a router.

Advantages:  
 Quick deployment with minimal setup.  
 No need for extra infrastructure.  
 Useful in remote or emergency situations.

Disadvantages:  
 Less secure than infrastructure-based networks.  
 Not scalable for large networks.

1. **Explain Wireless security protocol and Encryption method type ?**

## Wireless Security Protocols and Encryption Methods

Wireless security is crucial to protect data from unauthorized access, interception, and attacks. Various wireless security protocols and encryption methods ensure secure communication in Wi-Fi networks.

## 1. Wireless Security Protocols

### A. WEP (Wired Equivalent Privacy)

* Introduced: 1997 (IEEE 802.11 standard).
* Encryption: RC4 with 64-bit or 128-bit key.
* Weakness:
  + Easily cracked using modern hacking tools.
  + Uses weak key management.
  + Vulnerable to IV (Initialization Vector) attacks.
* Status: Obsolete and not recommended for use.

### B. WPA (Wi-Fi Protected Access)

* Introduced: 2003 as a temporary replacement for WEP.
* Encryption: TKIP (Temporal Key Integrity Protocol).
* Weakness:
  + Still vulnerable to attacks like dictionary attacks.
  + TKIP is not fully secure.
* Status: Outdated but better than WEP.

### C. WPA2 (Wi-Fi Protected Access 2)

* Introduced: 2004, based on IEEE 802.11i standard.
* Encryption: AES-CCMP (Advanced Encryption Standard – Counter Mode CBC-MAC Protocol).
* Improvements:
  + Stronger encryption compared to WPA.
  + No TKIP vulnerabilities.
* Weakness:
  + Vulnerable to brute-force attacks if a weak password is used.
  + The KRACK attack (Key Reinstallation Attack) can exploit weaknesses in WPA2 but is mitigated through updates.
* Status: Widely used but replaced by WPA3 in new networks.

### D. WPA3 (Wi-Fi Protected Access 3)

* Introduced: 2018 as the latest security standard.
* Encryption: AES-GCMP-256 (stronger than WPA2).
* Improvements:
  + SAE (Simultaneous Authentication of Equals): Protects against dictionary attacks.
  + Forward Secrecy: Prevents past communications from being decrypted if the key is compromised.
  + Stronger encryption for open networks: Uses OWE (Opportunistic Wireless Encryption).
  + Protection against brute-force attacks: Limits the number of authentication attempts.
* Weakness:
  + Some older devices do not support WPA3.
* Status: Most secure and recommended standard.

## 2. Encryption Methods Used in Wireless Security

Encryption ensures that data transmitted over a wireless network is unreadable to unauthorized users.

### A. RC4 (Rivest Cipher 4)

* Used in WEP and WPA (with TKIP).
* Weakness: Vulnerable to attacks, leading to deprecation.

### B. TKIP (Temporal Key Integrity Protocol)

* Used in WPA (Wi-Fi Protected Access).
* Dynamically changes encryption keys to enhance security.
* Weakness:
  + Still uses RC4, which is insecure.
  + Susceptible to replay attacks.
* Status: Deprecated, replaced by AES.

### C. AES (Advanced Encryption Standard)

* Used in WPA2 and WPA3 with CCMP or GCMP modes.
* Encryption Strength:
  + 128-bit, 192-bit, or 256-bit keys.
* Modes:
  + AES-CCMP (Counter Mode CBC-MAC Protocol) – Used in WPA2.
  + AES-GCMP (Galois/Counter Mode Protocol) – Used in WPA3, offering better performance and security.
* Status: Highly secure and widely used.

### D. SAE (Simultaneous Authentication of Equals)

* Used in WPA3 instead of PSK (Pre-Shared Key).
* Prevents dictionary attacks by securely exchanging authentication keys.
* Provides Forward Secrecy (previous data remains secure even if the password is compromised).

### Comparison of Wireless Security Protocols & Encryption Methods

| Security Protocol | Encryption Method | Strength | Vulnerabilities |
| --- | --- | --- | --- |
| WEP | RC4 | Weak | Easily cracked, IV attacks |
| WPA | TKIP (RC4-based) | Medium | Susceptible to dictionary and replay attacks |
| WPA2 | AES-CCMP | Strong | Vulnerable to KRACK if not patched |
| WPA3 | AES-GCMP + SAE | Very Strong | Backward compatibility issues |

## Best Practices for Wireless Security

1. Use WPA3 whenever possible (or WPA2 with strong passwords if WPA3 is unavailable).
2. Disable WEP and WPA (they are insecure).
3. Use AES encryption (avoid TKIP).
4. Use strong, unique passwords to prevent brute-force attacks.
5. Enable MAC address filtering to allow only authorized devices.
6. Regularly update router firmware to patch security vulnerabilities.
7. Use a VPN (Virtual Private Network) for additional encryption on public Wi-Fi.
8. **Example of DHCP configuration ?**

### Example of DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network. Below are examples of DHCP configurations for different environments.

## 1. DHCP Configuration on a Cisco Router

This example configures a DHCP server on a Cisco router.

### Steps to Configure DHCP on Cisco Router

1. Enable the DHCP service
2. Define the IP address pool
3. Exclude specific addresses
4. Set the default gateway and DNS server
5. Activate the DHCP service

### Configuration:

Router(config)# service dhcp ! Enable DHCP service

Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10 ! Exclude IPs (e.g., reserved for static devices)

Router(config)# ip dhcp pool MY-DHCP-POOL ! Create a DHCP pool

Router(dhcp-config)# network 192.168.1.0 255.255.255.0 ! Define network range

Router(dhcp-config)# default-router 192.168.1.1 ! Set default gateway

Router(dhcp-config)# dns-server 8.8.8.8 8.8.4.4 ! Set DNS servers

Router(dhcp-config)# lease 7 ! Lease time (7 days)

Router(dhcp-config)# exit ! Exit configuration

### Verification Commands

Router# show ip dhcp binding ! View assigned IPs

Router# show ip dhcp pool ! View DHCP pool status

Router# show ip dhcp server statistics ! View DHCP statistics

## 2. DHCP Configuration on a Linux Server (dhcpd.conf - ISC DHCP Server)

The ISC DHCP Server is widely used on Linux-based servers.

### Configuration File (/etc/dhcp/dhcpd.conf):

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.100 192.168.1.200; # DHCP address pool

option routers 192.168.1.1; # Default gateway

option domain-name-servers 8.8.8.8, 8.8.4.4; # DNS servers

option domain-name "example.com"; # Domain name

default-lease-time 600; # Default lease time (10 minutes)

max-lease-time 7200; # Maximum lease time (2 hours)

}

### Restart DHCP Service:

sudo systemctl restart isc-dhcp-server

### Check DHCP Leases:

cat /var/lib/dhcp/dhcpd.leases

## 3. DHCP Configuration on Windows Server

Using Windows Server DHCP Role:

1. Open Server Manager → Add Roles → Install DHCP Server role.
2. Open DHCP Management Console (dhcpmgmt.msc).
3. Right-click on the server name → Select New Scope.
4. Configure:
   * Scope Name: Example\_Scope
   * IP Range: 192.168.1.100 - 192.168.1.200
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.1.1
   * DNS Server: 8.8.8.8
   * Lease Duration: Default or custom

### Verify DHCP Leases:

Run the following command in PowerShell:

Get-DhcpServerv4Scope | Get-DhcpServerv4Lease

### Summary of DHCP Configurations

| Environment | DHCP Service | Configuration File/Command |
| --- | --- | --- |
| Cisco Router | Built-in DHCP | ip dhcp pool, show ip dhcp binding |
| Linux Server | ISC DHCP Server | /etc/dhcp/dhcpd.conf |
| Windows Server | DHCP Role | DHCP Management Console (dhcpmgmt.msc) |

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

### What is ACL?

An Access Control List (ACL) is a set of rules applied to a network device (such as a router or firewall) to permit or deny traffic based on IP addresses, protocols, or ports. ACLs enhance security by controlling which packets are allowed or blocked in a network.

## Types of ACL in Cisco Devices

ACLs are classified into two main types:

### 1. Standard ACL

* Filters traffic based only on the source IP address.
* Applied close to the destination (on the interface receiving the traffic).
* Uses ACL numbers 1-99 and 1300-1999 (extended range).

Example of a Standard ACL:

Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip access-group 10 in

Router(config-if)# exit

This configuration allows only traffic from 192.168.1.0/24 on interface GigabitEthernet0/1.

### 2. Extended ACL

* Filters traffic based on multiple criteria:
  + Source & Destination IP
  + Protocol (TCP, UDP, ICMP, etc.)
  + Port numbers (e.g., HTTP, FTP, SSH)
* Applied close to the source (on the interface where traffic originates).
* Uses ACL numbers 100-199 and 2000-2699 (extended range).

## Example of an Extended ACL

Scenario: Block all HTTP traffic from 192.168.1.0/24 going to 192.168.2.0/24, but allow everything else.

### Configuration:

Router(config)# access-list 110 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80

Router(config)# access-list 110 permit ip any any ! Allow all other traffic

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip access-group 110 in

Router(config-if)# exit

### Explanation:

1. deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
   * Blocks HTTP (port 80) traffic from 192.168.1.0/24 to 192.168.2.0/24.
2. permit ip any any
   * Allows all other traffic.
3. Applied on the incoming interface (GigabitEthernet0/1) to stop restricted traffic at the source.

### Comparison: Standard vs Extended ACL

| Feature | Standard ACL | Extended ACL |
| --- | --- | --- |
| Filters by | Source IP only | Source & Destination IP, Protocol, Port |
| Control Level | Basic | Granular |
| Number Range | 1-99, 1300-1999 | 100-199, 2000-2699 |
| Placement | Near destination | Near source |
| Example Use Case | Allow/block entire subnets | Allow/block specific services (HTTP, SSH, etc.) |

### Best Practices for ACL Configuration

Place standard ACLs near the destination (to prevent unnecessary blocking).  
 Place extended ACLs near the source (to filter traffic before it enters the network).  
 Always end ACLs with permit ip any any if needed to allow traffic.  
 Use descriptive names (ip access-list extended NAME) instead of just numbers for better readability.

1. **Example of Port security in Switch ?**

## Example of Port Security on a Cisco Switch

Port Security is a feature on Cisco switches that helps restrict and control access to a port based on MAC addresses. It prevents unauthorized devices from connecting to the network and mitigates attacks like MAC flooding.

### 🔹 Steps to Configure Port Security on a Cisco Switch

1. Enable port security on an interface
2. Set the maximum number of MAC addresses allowed
3. Define violation actions (Shutdown, Restrict, or Protect)
4. (Optional) Configure sticky MAC addresses

## 🔸 Example: Basic Port Security Configuration

Scenario:

* Allow only one MAC address on interface FastEthernet 0/1.
* If an unauthorized MAC address is detected, the port will be shut down.

### 🔹 Configuration:

Switch(config)# interface FastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

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

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

Switch(config-if)# switchport port-security mac-address 00A1.B2C3.D4E5

Switch(config-if)# exit

### 🔹 Explanation:

1. switchport mode access → Sets the port as an access port.
2. switchport port-security → Enables port security.
3. switchport port-security maximum 1 → Allows only one MAC address on the port.
4. switchport port-security violation shutdown → If an unauthorized MAC address is detected, the port shuts down.
5. switchport port-security mac-address 00A1.B2C3.D4E5 → Manually assigns the allowed MAC address.

## 🔸 Example: Sticky MAC Address (Dynamic Learning)

Instead of manually setting a MAC address, the switch can dynamically learn and store it.

Switch(config)# interface FastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 2

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

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

Switch(config-if)# exit

### 🔹 Explanation:

1. switchport port-security mac-address sticky → Learns and stores MAC addresses dynamically.
2. switchport port-security maximum 2 → Allows up to two devices.
3. switchport port-security violation restrict → Logs unauthorized MAC attempts but does not shut down the port.

## 🔸 Port Security Violation Modes

| Mode | Action When Violation Occurs |
| --- | --- |
| Shutdown | Default mode, port disables itself until manually re-enabled (shutdown & no shutdown). |
| Restrict | Drops unauthorized traffic and logs a violation message but keeps the port active. |
| Protect | Drops unauthorized traffic without logging or disabling the port. |

## 🔸 Verify and Monitor Port Security

### Check Port Security Status:

Switch# show port-security interface FastEthernet 0/1

### Check Violation Statistics:

Switch# show port-security address

### Reactivate a Disabled Port:

Switch(config)# interface FastEthernet 0/1

Switch(config-if)# shutdown

Switch(config-if)# no shutdown

### Best Practices for Port Security

Use Sticky MAC Addresses for ease of management.  
 Set a maximum limit on allowed MAC addresses per port.  
 Choose violation mode based on security needs.  
 Regularly monitor violations using show port-security.  
 Secure unused ports by disabling them (shutdown command).

1. **List Of WAN connections with protocol ?**

Wide Area Networks (WANs) connect networks across large geographical areas using various technologies and protocols. Below is a list of WAN connection types and their associated protocols.

### 1. Leased Line

* Description: A dedicated point-to-point connection between two locations.
* Protocols Used:
  + PPP (Point-to-Point Protocol)
  + HDLC (High-Level Data Link Control)
  + Frame Relay (Legacy)
* Speed Range: 64 Kbps – 10 Gbps

### 2. DSL (Digital Subscriber Line)

* Description: Uses telephone lines for high-speed internet.
* Protocols Used:
  + PPP over Ethernet (PPPoE)
  + PPP over ATM (PPPoA)
* Speed Range: 256 Kbps – 100 Mbps

### 3. Cable Broadband

* Description: Uses coaxial cable for internet access.
* Protocols Used:
  + DOCSIS (Data Over Cable Service Interface Specification)
  + IP (Internet Protocol)
* Speed Range: 10 Mbps – 1 Gbps

### 4. Fiber Optic (FTTH, FTTP, Metro Ethernet)

* Description: High-speed internet using fiber-optic cables.
* Protocols Used:
  + Ethernet over MPLS (EoMPLS)
  + Gigabit Passive Optical Network (GPON)
  + 10-Gigabit Ethernet (10GE)
* Speed Range: 100 Mbps – 10 Gbps

### 5. MPLS (Multiprotocol Label Switching)

* Description: High-performance, label-based routing for WAN networks.
* Protocols Used:
  + MPLS (Multiprotocol Label Switching)
  + IP/MPLS (for VPNs)
* Speed Range: 1 Mbps – 100 Gbps

### 6. Metro Ethernet

* Description: Ethernet-based WAN used in metropolitan areas.
* Protocols Used:
  + Ethernet over MPLS (EoMPLS)
  + Carrier Ethernet (CE)
* Speed Range: 10 Mbps – 100 Gbps

### 7. ISDN (Integrated Services Digital Network)

* Description: Circuit-switched telephone network for voice and data.
* Protocols Used:
  + PPP (Point-to-Point Protocol)
  + ISDN PRI (Primary Rate Interface)
* Speed Range: 64 Kbps – 128 Kbps (Basic Rate Interface)

### 8. Frame Relay (Legacy)

* Description: Packet-switched technology for WAN links (now replaced by MPLS).
* Protocols Used:
  + Frame Relay
* Speed Range: 56 Kbps – 45 Mbps

### 9. ATM (Asynchronous Transfer Mode)

* Description: High-speed networking technology for voice and data (obsolete).
* Protocols Used:
  + ATM (Asynchronous Transfer Mode)
  + PPP over ATM (PPPoA)
* Speed Range: 155 Mbps – 622 Mbps

### 10. Satellite Internet

* Description: Uses satellite communication for remote locations.
* Protocols Used:
  + IP over DVB-S (Digital Video Broadcasting – Satellite)
  + TCP/IP with acceleration techniques
* Speed Range: 512 Kbps – 100 Mbps

### 11. Wireless WAN (4G, 5G, LTE)

* Description: Cellular networks used for mobile and remote connectivity.
* Protocols Used:
  + LTE (Long-Term Evolution)
  + 5G NR (New Radio)
  + CDMA/GSM (for older networks)
* Speed Range: 1 Mbps – 10 Gbps

### 12. SD-WAN (Software-Defined WAN)

* Description: Uses software-based control to optimize WAN traffic.
* Protocols Used:
  + IPsec VPN (for secure tunneling)
  + BGP (Border Gateway Protocol)
* Speed Range: Varies (depends on the underlying network)

## 🔹 Summary Table of WAN Connections & Protocols

| WAN Connection Type | Protocols Used | Speed Range |
| --- | --- | --- |
| Leased Line | PPP, HDLC, Frame Relay | 64 Kbps – 10 Gbps |
| DSL | PPPoE, PPPoA | 256 Kbps – 100 Mbps |
| Cable Broadband | DOCSIS, IP | 10 Mbps – 1 Gbps |
| Fiber Optic | GPON, 10GE, EoMPLS | 100 Mbps – 10 Gbps |
| MPLS | MPLS, IP/MPLS | 1 Mbps – 100 Gbps |
| Metro Ethernet | Ethernet over MPLS | 10 Mbps – 100 Gbps |
| ISDN | PPP, ISDN PRI | 64 Kbps – 128 Kbps |
| Frame Relay (Legacy) | Frame Relay | 56 Kbps – 45 Mbps |
| ATM (Legacy) | ATM, PPPoA | 155 Mbps – 622 Mbps |
| Satellite | IP over DVB-S, TCP/IP | 512 Kbps – 100 Mbps |
| Wireless WAN (4G/5G) | LTE, 5G NR, CDMA/GSM | 1 Mbps – 10 Gbps |
| SD-WAN | IPsec VPN, BGP | Varies |

### Key Takeaways

MPLS, Fiber Optic, and SD-WAN are the most common modern WAN technologies.  
 Leased Lines (PPP, HDLC) are still used for dedicated high-security connections.  
 4G/5G Wireless WAN is useful for mobile and remote locations.  
 Legacy technologies (Frame Relay, ATM, ISDN) are obsolete but may still exist in older networks.

1. **Explain Frame-Relay and PPP ?**

Both Frame Relay and PPP (Point-to-Point Protocol) are WAN technologies used for communication between remote networks. However, they serve different purposes and operate in different ways.

### 🔹 What is Frame Relay?

* Frame Relay is a packet-switched WAN technology that enables multiple sites to connect using a shared network infrastructure.
* It is a layer 2 protocol that operates on virtual circuits (VCs) instead of dedicated physical links.
* It was widely used before MPLS and Metro Ethernet, but it is now considered legacy technology.

### 🔹 Features of Frame Relay

✔ Cost-Effective – Uses a shared network instead of dedicated lines.  
 ✔ Packet-Switched – Sends data in small frames with variable sizes.  
 ✔ Uses Virtual Circuits (PVCs & SVCs) – Logical connections instead of dedicated links.  
 ✔ No Error Correction – Frame Relay relies on higher-layer protocols (TCP/IP) for error handling.

### 🔹 Frame Relay Virtual Circuits

Frame Relay uses two types of virtual circuits for communication:

1. Permanent Virtual Circuit (PVC) – Always active, pre-configured by the provider.
2. Switched Virtual Circuit (SVC) – Temporary, established on demand.

Each VC is identified by a Data Link Connection Identifier (DLCI), which acts like a local address.

### 🔹 Basic Frame Relay Configuration

Scenario: A router is connected to a Frame Relay network using DLCI 102.

Router(config)# interface Serial0/0

Router(config-if)# encapsulation frame-relay

Router(config-if)# frame-relay interface-dlci 102

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

### 🔹 Advantages & Disadvantages of Frame Relay

| Advantages | Disadvantages |
| --- | --- |
| Cost-effective for multiple remote sites | No built-in error correction |
| More efficient than older technologies like X.25 | Being phased out by MPLS |
| Supports multiple logical connections (PVCs) over one physical link | Performance depends on service provider |

# 

### 🔹 What is PPP?

* PPP (Point-to-Point Protocol) is a layer 2 WAN protocol used to establish direct connections between two nodes.
* It supports authentication, compression, and error detection.
* Unlike Frame Relay (which is a packet-switched network), PPP is used for dedicated point-to-point connections.

### 🔹 Features of PPP

✔ Works with synchronous and asynchronous links  
 ✔ Supports Authentication (PAP, CHAP)  
 ✔ Error detection using CRC  
 ✔ Multilink PPP (MLPPP) for bandwidth aggregation

### 🔹 PPP Authentication Methods

PPP supports two types of authentication:

1. PAP (Password Authentication Protocol) – Sends passwords in plain text (less secure).
2. CHAP (Challenge Handshake Authentication Protocol) – Uses a hashed authentication method (more secure).

### 🔹 Basic PPP Configuration

Scenario: Configure PPP on a serial link between two routers.

Router(config)# interface Serial0/0

Router(config-if)# encapsulation ppp

Router(config-if)# ip address 10.1.1.1 255.255.255.0

Router(config-if)# ppp authentication chap

Router(config-if)# no shutdown

For CHAP authentication, configure the username and password:

Router(config)# username R2 password cisco123

🔹 Advantages & Disadvantages of PPP

| Advantages | Disadvantages |
| --- | --- |
| Supports authentication (PAP/CHAP) | Works only for point-to-point links |
| Supports compression for efficient transmission | Less scalable than Frame Relay |
| Supports error detection (CRC) | Requires dedicated physical links |

# Frame Relay vs. PPP – Key Differences

| Feature | Frame Relay | PPP |
| --- | --- | --- |
| Type | Packet-switched WAN | Point-to-point WAN |
| Topology | Supports multiple remote sites | Only works for two directly connected devices |
| Encapsulation | Frame Relay encapsulation | PPP encapsulation |
| Authentication | No built-in authentication | Supports PAP/CHAP authentication |
| Error Detection | Relies on TCP/IP for error handling | Uses CRC for error checking |
| Use Case | Used for multiple remote sites over a shared WAN | Used for dedicated connections like leased lines |

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

## 🔹 What is NAT (Network Address Translation)?

NAT (Network Address Translation) is a process used in routers to modify IP addresses in packet headers as they pass through the device. It allows multiple devices in a private network to access the internet using a single public IP address. NAT is essential for conserving IPv4 addresses and improving security by hiding internal IP addresses.

## 🔹 Types of NAT

1. Static NAT – Maps a private IP to a public IP one-to-one.
2. Dynamic NAT – Maps a private IP to a pool of public IPs.
3. PAT (Port Address Translation) / NAT Overload – Maps multiple private IPs to a single public IP using different port numbers.

## 🔹 Example: Configuring NAT Overload (PAT) on a Cisco Router

Scenario:

* Inside network: 192.168.1.0/24
* Outside network: The internet
* Public IP: 203.0.113.1

### 🔹 Step-by-Step Configuration

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)# interface FastEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# ip nat inside

Router(config-if)# exit

Router(config)# interface Serial0/0

Router(config-if)# ip address 203.0.113.1 255.255.255.252

Router(config-if)# ip nat outside

Router(config-if)# exit

Router(config)# ip nat inside source list 1 interface Serial0/0 overload

Router(config)# exit

### 🔹 How It Works

access-list 1 permit 192.168.1.0 0.0.0.255 → Allows internal traffic for NAT.  
 ip nat inside / ip nat outside → Defines inside (private) and outside (public) interfaces.  
 ip nat inside source list 1 interface Serial0/0 overload → Enables PAT (NAT overload), mapping multiple private IPs to one public IP.

### 🔹 Verifying NAT

Use the following commands to check the NAT translations:

Router# show ip nat translations

Router# show ip nat statistics

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

### HDLC (High-Level Data Link Control)

HDLC is a bit-oriented synchronous data link layer protocol used for communication over point-to-point and multipoint links. It provides error detection, flow control, and encapsulation of data for transmission. HDLC is widely used in serial communication and WAN connections.

### Commands to Show HDLC in Networking Software

#### On Cisco Devices (Routers/Switches)

To check the HDLC encapsulation on an interface:  
  
 show interfaces serial <interface-number>

Example:  
  
 show interfaces serial 0/0/0

1. This command displays the interface status, encapsulation type (HDLC), and other details.

To check HDLC encapsulation for all interfaces:  
  
 show interfaces

1. This will list details for all interfaces, including encapsulation type.

To configure HDLC on a Cisco interface:  
  
 configure terminal

interface serial 0/0/0

encapsulation hdlc

exit

1. This ensures the interface uses HDLC encapsulation.

### On Linux (PPP/HDLC over Serial)

To check if HDLC is enabled on a serial interface in Linux, use:

ifconfig

or

ip link show

For more advanced HDLC configurations, you may use:

hdlcstat

or

sethdlc -q

(if hdlc-utils package is installed)

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

### Encapsulation in Networking

Encapsulation is the process of wrapping data with protocol-specific headers and trailers as it moves through different layers of the OSI model. Each layer adds its own header information to ensure proper transmission and delivery.

For example, in WAN connections, encapsulation methods like HDLC, PPP, Frame Relay, or GRE are used to transport data between routers.

### Example: GRE Tunnel Encapsulation

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate various network layer protocols inside IP packets, enabling communication between remote networks.

#### GRE Tunnel Configuration (Cisco Example)

1 Configure the Tunnel on Router 1 (R1):

interface Tunnel0

ip address 10.1.1.1 255.255.255.0

tunnel source 192.168.1.1

tunnel destination 192.168.2.1

tunnel mode gre ip

2️ Configure the Tunnel on Router 2 (R2):

interface Tunnel0

ip address 10.1.1.2 255.255.255.0

tunnel source 192.168.2.1

tunnel destination 192.168.1.1

tunnel mode gre ip

### How GRE Encapsulation Works

1. Original Packet → Carries private IP (e.g., 10.0.0.1 → 10.0.0.2).
2. GRE Encapsulation → GRE header is added.
3. IP Encapsulation → An outer IP header is added (e.g., 192.168.1.1 → 192.168.2.1).
4. Transmission over the Internet → The packet travels through public networks while keeping the private network hidden.
5. Decapsulation at Destination → The receiving router removes the GRE and outer IP headers to reveal the original packet.

This is useful for site-to-site VPNs, dynamic routing over the internet, or carrying non-IP traffic over IP networks.

🔹 To verify the GRE tunnel:

show interface tunnel0

show ip route

show ip interface brief