**Module 8 Network Access**

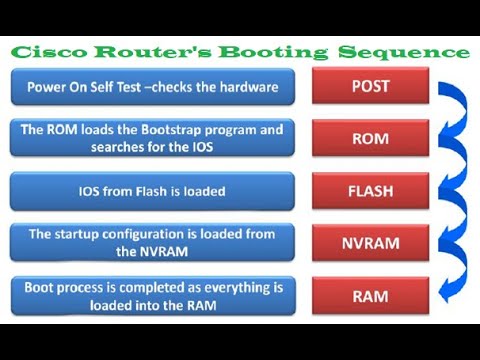
**Explain Switch**

* + A switch is a networking device that operates at the Data Link layer (Layer 2) of the OSI model. It connects multiple devices within a local area network (LAN) and uses MAC addresses to forward data frames to their intended destinations.
  + Switches use MAC address tables to make forwarding decisions, allowing them to send data only to the specific port where the destination device is connected, thus reducing network traffic and improving efficiency compared to hubs.



Explain Switch Boot Sequence:

* + The boot sequence of a switch involves several steps:
    - Power-On Self-Test (POST): The switch performs a self-diagnostic test to check hardware components such as CPU, RAM, and interfaces.
    - Load the bootstrap program: The switch loads the bootstrap program from its ROM (Read-Only Memory) into RAM (Random Access Memory).
    - Locate and load the operating system: The switch locates the operating system image stored in flash memory or other storage media and loads it into RAM.
    - Initialize interfaces and configurations: The switch initializes its interfaces, applies any configured settings, and establishes connections to the network.



Explain Three Methods to Access Switch Command Line Interface (CLI):

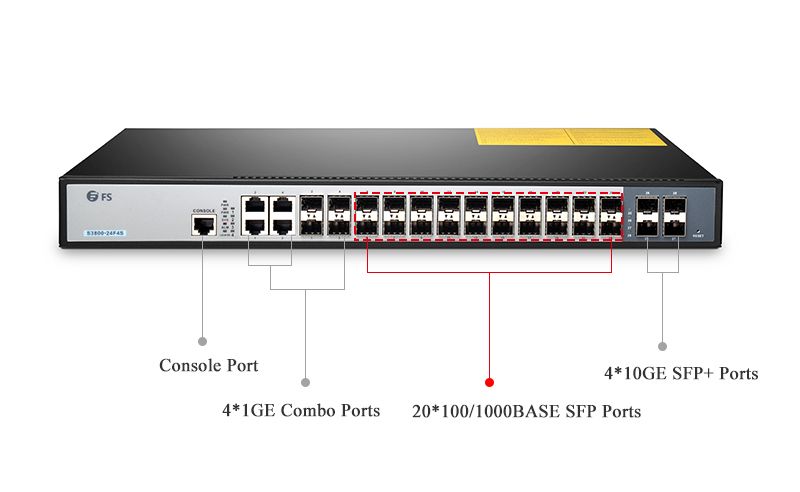
* + Console port: Connect to the switch using a console cable and terminal emulation software (e.g., PuTTY) through the console port.
  + Telnet: Access the switch remotely over a network using Telnet protocol. Telnet requires IP connectivity to the switch and can be enabled on the switch.
  + SSH (Secure Shell): Similar to Telnet, SSH provides secure remote access to the switch over a network. SSH encrypts the data transmitted between the client and the switch, offering better security compared to Telnet.

Explain Switch Port

1. **Console Port:**
   * **The console port is a special type of port found on network switches and routers. It provides direct access to the device's command-line interface (CLI) for configuration and management purposes.**
   * **Administrators typically connect to the console port using a console cable, which is often equipped with an RJ-45 connector on one end and a serial connector (DB-9 or USB) on the other.**
   * **Through the console port, administrators can perform initial device configuration, troubleshoot network issues, and recover the device in case of network connectivity issues.**
2. **Ethernet Ports:**
   * **Ethernet ports are the most common type of switch ports and are used to connect end-user devices, such as computers, printers, servers, and other network devices, to the network.**
   * **These ports support Ethernet cables, typically with RJ-45 connectors, and facilitate the transmission of data packets between devices within the local area network (LAN).**
3. **Auxiliary Ports:**
   * **Auxiliary ports, also known as AUX ports, are additional serial ports found on some network devices, including switches and routers.**
   * **These ports are used for out-of-band management, allowing administrators to access the device remotely for configuration and troubleshooting purposes.**
   * **Auxiliary ports are often used in conjunction with modems or terminal servers to establish remote access to the device's CLI.**

**Managed vs. Unmanaged Ports**: In managed switches, administrators have granular control over individual ports through a centralized management interface. This allows for configuration changes, monitoring of port performance, and implementation of advanced networking features such as Quality of Service (QoS) and port mirroring. On the other hand, unmanaged switches have fixed settings and operate in a plug-and-play manner without the need for configuration.

Switch ports are fundamental components of modern network infrastructures, enabling the seamless exchange of data between devices and supporting the efficient operation of LAN environments. Their configurability, performance, and reliability make them essential building blocks for creating scalable and resilient network architectures.



**Configure Basic Password Settings on a switch**:

*enable*

*configure terminal*

*enable password <password>*

*enable secret <secret-password>*

enable configure terminal enable password <password> enable secret <secret-password>

* **enable**: Enters privileged EXEC mode.
* **configure terminal**: Enters global configuration mode.
* **enable password <password>**: Sets an unencrypted password for accessing privileged EXEC mode.
* **enable secret <secret-password>**: Sets an encrypted password for accessing privileged EXEC mode.

**Configure Line Password Settings on a switch**:

enable

configure terminal

line console 0

password <password>

login

exit

enable configure terminal line console 0 password <password> login exit

* **line console 0**: Enters console line configuration mode.
* **password <password>**: Sets a password for accessing the console line.
* **login**: Enables password checking for console access.

**Configure Password Settings on a switch**:

enable

configure terminal

username <username> secret <password>

enable configure terminal username <username> secret <password>

* **username <username>**: Configures a username for user authentication.
* **secret <password>**: Sets an encrypted password for the configured username.

**Configure IPv4 on a switch**:

enable

configure terminal

interface <interface>

ip address <ip-address> <subnet-mask>

no shutdown

enable configure terminal interface <interface> ip address <ip-address> <subnet-mask> no shutdown

* **interface <interface>**: Enters interface configuration mode.
* **ip address <ip-address> <subnet-mask>**: Assigns an IP address and subnet mask to the interface.
* **no shutdown**: Enables the interface.

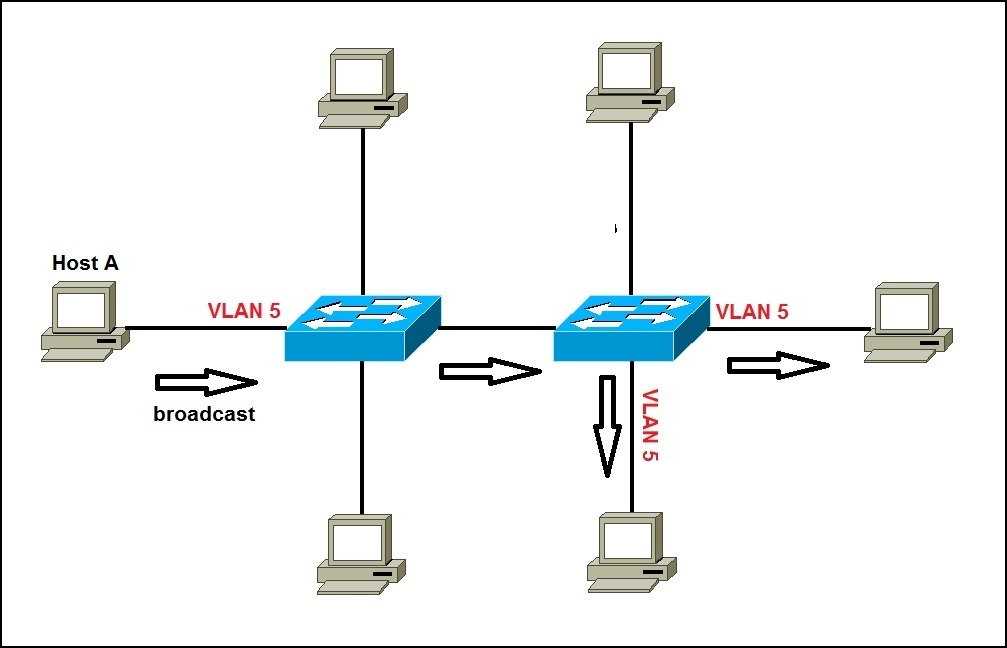
**Verifying IPv4 on a switch**:

show ip interface brief

* **show ip interface brief**: Displays the IPv4 configuration and status of all interfaces on the switch.

**Basic VLAN (Virtual Local Area Network)**:

* + VLANs divide a single physical network into multiple logical networks, allowing administrators to segment traffic, enhance security, and simplify network management.



**VTP (VLAN Trunking Protocol)**:

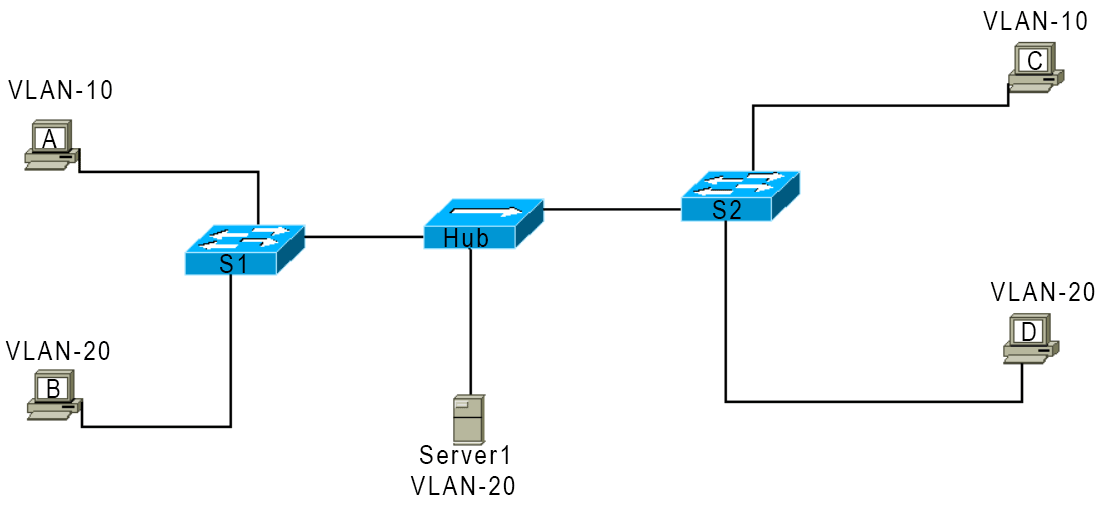
* + VTP is a Cisco proprietary protocol used to manage VLAN configurations across a network of interconnected switches. It enables switches to share and synchronize VLAN information automatically.

**CDP (Cisco Discovery Protocol)**:

* + CDP is a Cisco proprietary protocol used to discover and collect information about directly connected Cisco devices. It provides details such as device type, capabilities, and connected interfaces.

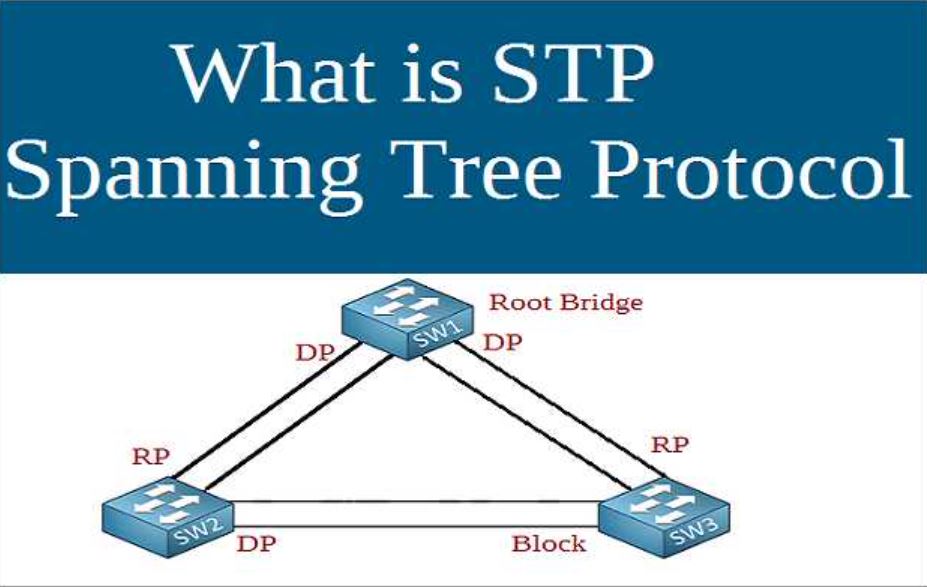
**Identifying VLAN**:

* + VLANs are identified by a numerical identifier (VLAN ID) assigned to them. Each VLAN represents a unique broadcast domain within the network.



**Basic Operation of STP (Spanning Tree Protocol)**:

* + STP prevents network loops in redundant switch topologies by identifying and blocking redundant paths. It selects the best path to the root bridge and places other paths in a blocked state until needed.



**IPv4 Subnetting**:

* + IPv4 subnetting involves dividing a large IP network into smaller subnetworks called subnets. This enables efficient use of IP address space and allows for better network organization and management.

IPv4 addresses are divided into classes, each with its own range of addresses and default subnet masks. Here's a brief overview:

* + **Class A Addresses (1.0.0.0 to 126.0.0.0)**:

Class A addresses are used for large networks, with the first octet reserved for the network portion and the remaining three octets for hosts.

The default subnet mask for Class A addresses is 255.0.0.0, which provides for up to 16,777,214 hosts per network.

* + **Class B Addresses (128.0.0.0 to 191.255.0.0)**:

Class B addresses are used for medium-sized networks, with the first two octets reserved for the network portion and the remaining two octets for hosts.

The default subnet mask for Class B addresses is 255.255.0.0, allowing for up to 65,534 hosts per network.

* + **Class C Addresses (192.0.0.0 to 223.255.255.0)**:

Class C addresses are used for small networks, with the first three octets reserved for the network portion and the last octet for hosts.

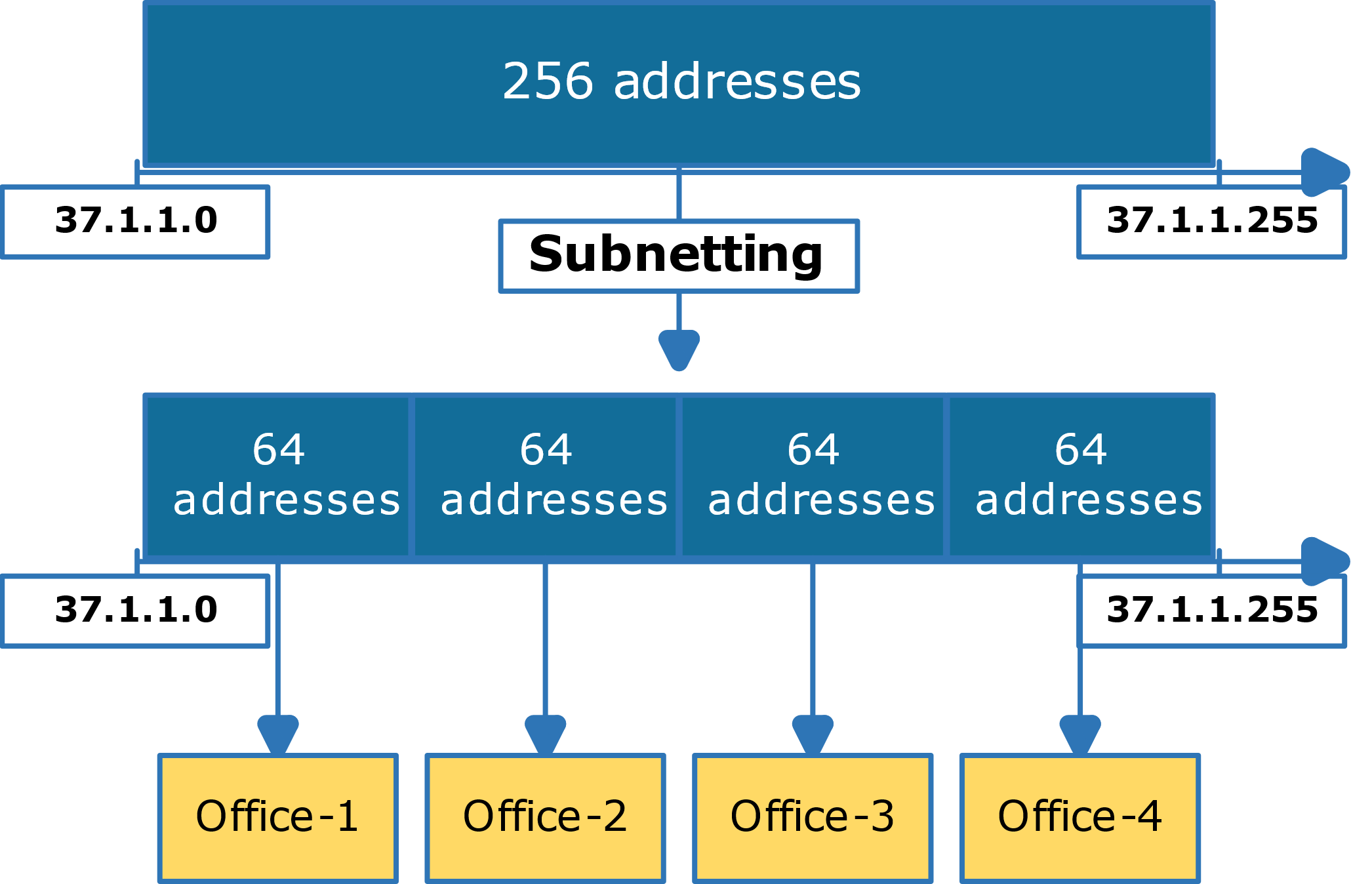
The default subnet mask for Class C addresses is 255.255.255.0, providing for up to 254 hosts per network.

* + Subnet masks are used to divide IP addresses into network and host portions. They consist of 32 bits, with the network portion represented by consecutive 1s followed by the host portion represented by consecutive 0s.

For example:

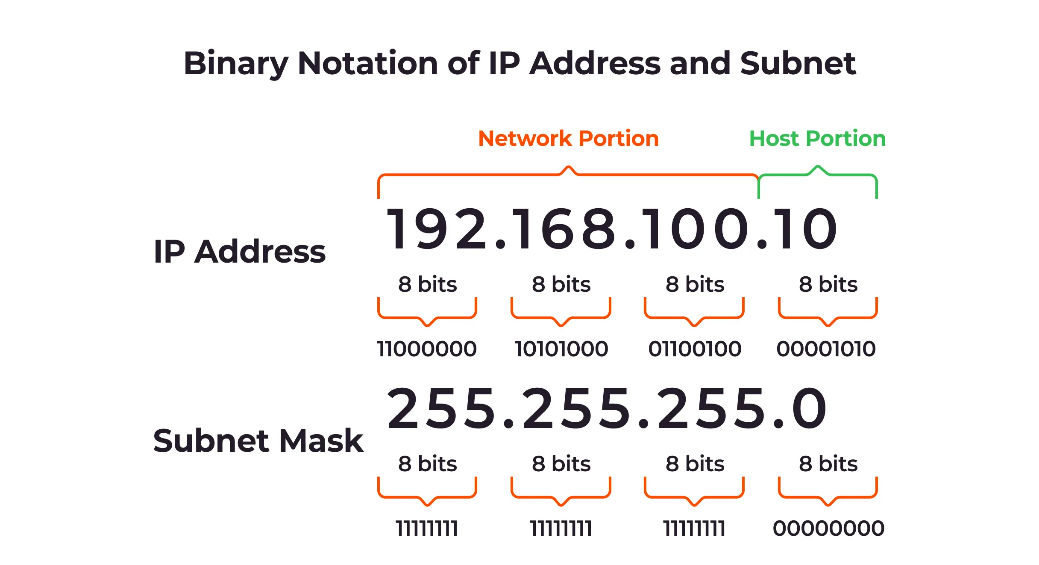
In a Class C network with the default subnet mask of 255.255.255.0, the first 24 bits are allocated for the network portion, leaving 8 bits for hosts.

* + Subnetting involves borrowing bits from the host portion to create smaller subnetworks. For instance, subnetting a Class C network into smaller networks might involve using a subnet mask like 255.255.255.192, which creates subnets with 62 usable hosts each.



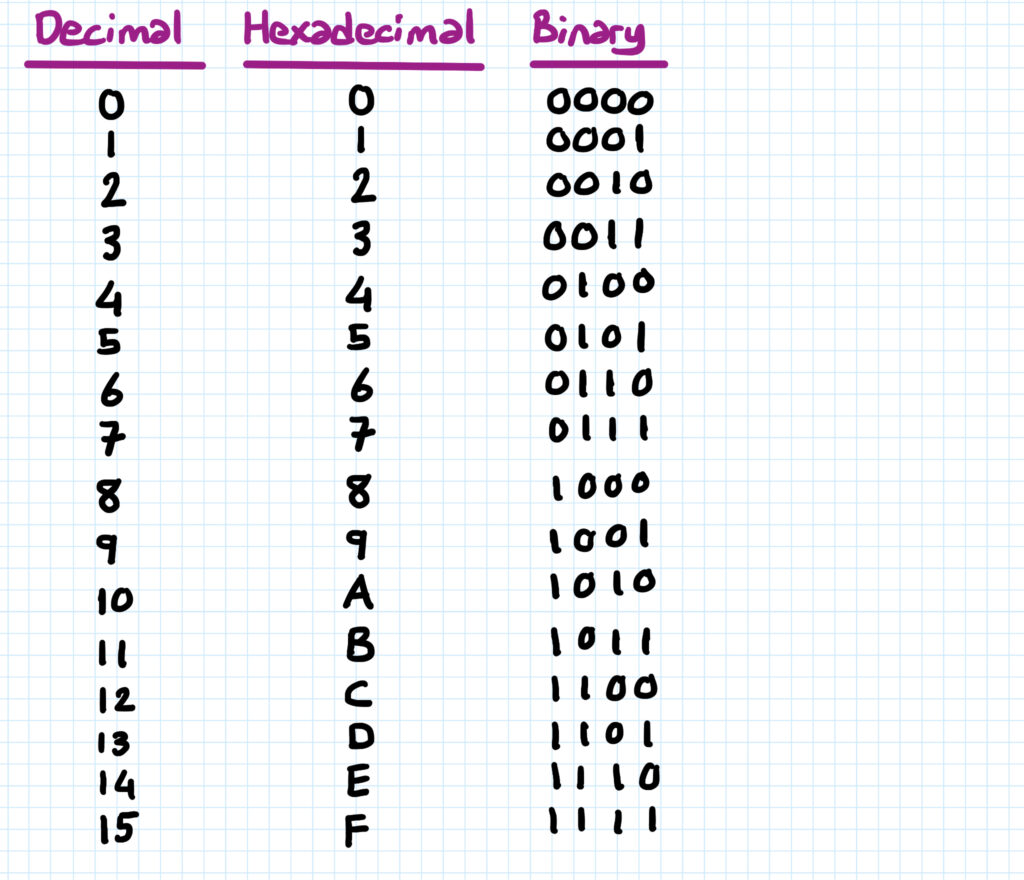
**Subnet Mask**:

* + A subnet mask is a 32-bit number used in IPv4 addressing to separate the network and host portions of an IP address. It determines which portion of the IP address identifies the network and which portion identifies the host.



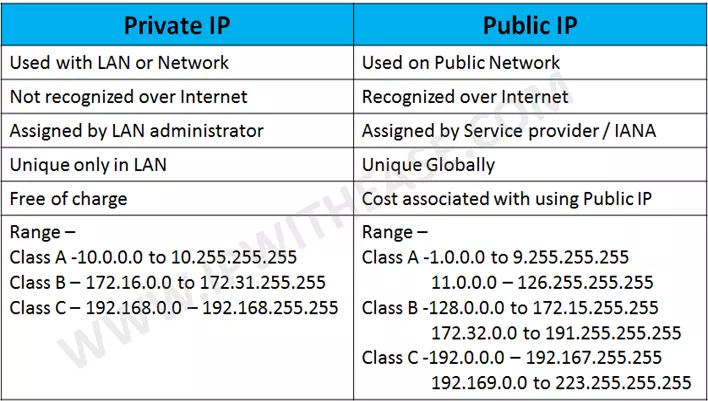
**Binary, Decimal, Hexadecimal**:

* + Binary is a base-2 numbering system using 0s and 1s. Decimal is a base-10 numbering system using digits from 0 to 9. Hexadecimal is a base-16 numbering system using digits from 0 to 9 and letters from A to F.



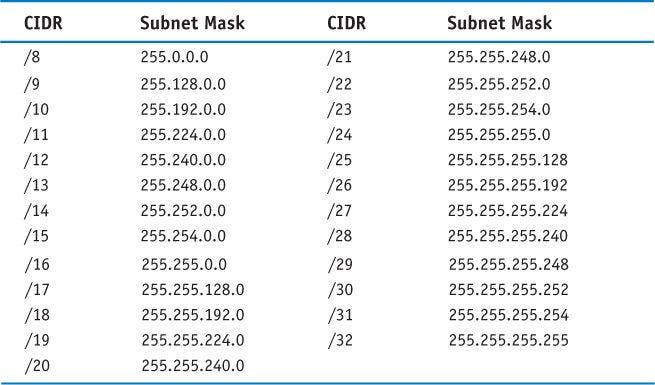
**Need for Public IPv4 and Private IP Addressing**:

* + Public IPv4 addresses are globally unique addresses assigned to devices connected to the Internet. Private IP addressing uses reserved address ranges defined by RFC 1918 for use within private networks, allowing organizations to conserve public IP addresses.



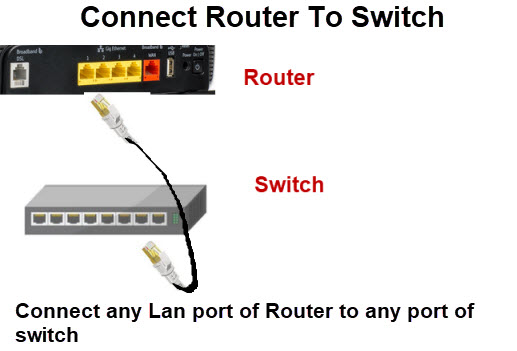
**Subnet Prefix**:

* Subnet prefix is a notation used in CIDR (Classless Inter-Domain Routing) to represent the network portion of an IP address along with the number of bits used for subnetting.



**Connecting Router with Switch**:

* To connect a router with a switch, you typically use Ethernet cables to connect router LAN interfaces to switch ports. This enables communication between devices connected to the switch and those connected to the router, allowing for inter-VLAN routing and internet access



Connecting a router to a switch is a common practice in networking to enable communication between different networks or VLANs. Here's how you can connect a router to a switch:

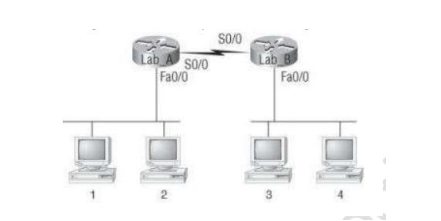
1. **Physical Connection**:
   * Ensure that the router and the switch are powered off before making any connections.
   * Use Ethernet cables to connect one of the LAN (Ethernet) ports on the router to one of the switch's available ports. Usually, any numbered Ethernet port (e.g., Ethernet 1, Ethernet 2) on the router can be used for this purpose.
   * Insert one end of the Ethernet cable into an available LAN port on the router and the other end into an available port on the switch.
2. **Configuration**:
   * Power on both the router and the switch.
   * Access the router's configuration interface. This is typically done by entering the router's IP address into a web browser and logging in with the router's administrative credentials. Consult the router's documentation for specific instructions on how to access its configuration interface.
   * In the router's configuration interface, configure the interface connected to the switch. This may involve assigning an IP address to the interface and enabling routing functionality.
   * Configure the switch if necessary. This may involve configuring VLANs, trunk ports, or other settings depending on your network requirements.
3. **Testing and Verification**:
   * After configuring the router and switch, test the connection to ensure that devices connected to the switch can communicate with devices connected to the router.
   * Ping devices on both sides of the connection to verify connectivity.
   * Check the router's routing table to ensure that it has learned routes from the switch's network, and vice versa if necessary.
4. **Additional Considerations**:
   * Consider configuring routing protocols (e.g., RIP, OSPF) if you have multiple routers or need dynamic routing between the router and the switch.
   * You may need to configure access control lists (ACLs) or firewall rules on the router to control traffic between the router and the switch.

Explain Routing Basics with command

1. **Viewing Routing Table**:
   * **show ip route**: This command displays the routing table of the router, showing the routes the router knows about and how it will forward packets to reach different networks.
2. **Adding Static Routes**:
   * **ip route [destination-network] [subnet-mask] [next-hop]**: This command is used to add a static route to the routing table of the router. It specifies the destination network, subnet mask, and the next hop IP address or exit interface.
3. **Configuring Dynamic Routing Protocols**:
   * **router ospf [process-id]**: This command enters OSPF (Open Shortest Path First) routing configuration mode.
   * **network [network-address] [wildcard-mask] area [area-id]**: This command specifies which networks are participating in OSPF and in which OSPF area they belong.
   * **router rip**: This command enters RIP (Routing Information Protocol) routing configuration mode.
   * **network [network-address]**: This command specifies which networks are participating in RIP.
4. **Verifying Dynamic Routing Protocols**:
   * **show ip protocols**: This command displays the current settings and status of the routing protocols configured on the router.
   * **show ip ospf neighbor**: This command displays OSPF neighbor information.
   * **show ip rip database**: This command displays the RIP routing table.
5. **Default Route**:
   * **ip route 0.0.0.0 0.0.0.0 [next-hop]**: This command adds a default route to the routing table, allowing the router to forward packets with unknown destinations to the specified next hop.
6. **Routing Metrics**:
   * Routers use various metrics to determine the best path to a destination, such as hop count, bandwidth, delay, reliability, and cost.
7. **Administrative Distance**:
   * Administrative distance is a measure of the trustworthiness of routing information received from different sources. Lower administrative distances are preferred.

Understanding these routing basics and the associated commands helps network administrators configure and manage routing in their network environments effectively. It enables routers to make informed decisions about how to forward data packets based on the current network topology and routing information.

Configuration basic IP address in fig.



Let’s start with command and also we can configure IPv4s in the cisco packet tracer with graphically by tapping router or computer icons .

* On router lab 1 go to CLI by tapping lab 1 router and give following commands.

ENABLE

CONF T (CONFIGURE TERMINAL)

INTERFACE FASETHERNET0/0 (ACCESING TO IN WHICH PORT CONNECTED)

IP ADDRESS 10.0.0.1 255.0.0.0 (USED CLASS A AND IPv4)

NO SHUT

EXIT

INTERFACE SERIAL0/0

IP ADDRESS 20.0.0.1 255.0.0.0

NO SHUT

EXIT

DO WR (SAVING CONFIGURATION)

* On router lab 2 same commands will be applied but the ip address and the subnet mask (not in this case) will be different.

ENABLE

CONF T (CONFIGURE TERMINAL)

INTERFACE FASETHERNET0/0 (ACCESING TO IN WHICH PORT CONNECTED)

IP ADDRESS 20.0.0.2 255.0.0.0 (USED CLASS A AND IPv4)

NO SHUT

EXIT

INTERFACE SERIAL0/0

IP ADDRESS 20.0.0.1 255.0.0.0

NO SHUT

EXIT

DO WR (SAVING CONFIGURATION)

* Now for the computer tap on computer and go to the ip configuration and give IPv4 address and subnet mask and Default gateway (most important for routing) and same as another computer but different for lab 2 routers the IPv4 addresses will be different and also the default gateway.
* Now for the routing we can use different routing like static,Default,RIP,EIGRP,OSPF,BGP . depends upon what we choose here in this case we use RIP v3 it is easy as on commands and GUI.
* For that we have to configure on both router lab 1 lab 1 and lab 2.

Now for router Lab 1

ENABLE

CONF T (CONFIGURE TERMINAL)

Router rip

Network 10.0.0.0 255.0.0.0

Network 20.0.0.0 255.0.0.0

Do wr

* Here after router rip commands we entered router configuration mode and in router rip protocol and we gave network to be routed by router.
* On router lab 2 the commands will be same. We have to configure both router for routing.

For router Lab 2

ENABLE

CONF T (CONFIGURE TERMINAL)

Router rip

Network 10.0.0.0 255.0.0.0

Network 20.0.0.0 255.0.0.0

Do wr

* Don’t forget to fire command do wr it will save the configuration that we made.
* Lastly we have to ping between wo computer go to lab 1 computer by tapping on computer and go to the commands and ping 20.0.0.1 if it

Create static routes

“**Static routes** allow precise control over network traffic. You can add them using the route add command in Windows. For example:

route add destination\_network MASK subnet\_mask gateway\_ip metric\_cost

Replace the placeholders with actual values. To make it persistent, add -p at the end. If you need to remove a static route, use route delete.”

Explain EIGRP:

EIGRP stands for Enhanced Interior Gateway Routing Protocol. It's a dynamic routing protocol used in computer networks for automatically routing data across networks within a router.

EIGRP is an advanced distance-vector routing protocol developed by Cisco Systems.

It uses a composite metric that takes into account various factors such as bandwidth, delay, reliability, and load to calculate the best path to a destination network.

EIGRP sends partial routing updates only when there is a change in the network topology, reducing bandwidth usage.

It supports classless routing and VLSM (Variable Length Subnet Masking).

EIGRP uses the Diffusing Update Algorithm (DUAL) to prevent routing loops and ensure fast convergence in case of network changes.

Explain OSPF Basics:

OSPF stands for Open Shortest Path First. It's a dynamic routing protocol commonly used in large enterprise networks and ISPs (Internet Service Providers).

OSPF is a link-state routing protocol, which means routers exchange information about the state of their links with neighboring routers.

It calculates the shortest path to a destination based on a cost metric associated with each link.

OSPF routers form adjacencies with neighboring routers to exchange routing information.

It supports CIDR (Classless Inter-Domain Routing) and VLSM (Variable Length Subnet Masking).

OSPF uses a hierarchical network design with areas to scale large networks efficiently.

Explain OSPF Area:

In OSPF, an area is a logical grouping of networks and routers.

OSPF routers in the same area share a common link-state database, which reduces the amount of routing information exchanged and improves network efficiency.

OSPF uses a hierarchical structure of areas, with the backbone area (Area 0) being the central routing backbone.

Each OSPF router must belong to at least one area, and all areas must connect to the backbone area.

Areas help to scale OSPF networks by reducing the amount of routing information flooding and improving convergence time.

Explain DR/BR Selection:

In OSPF, the DR (Designated Router) and BDR (Backup Designated Router) are roles assigned to routers in broadcast and non-broadcast multi-access networks (such as Ethernet).

The DR and BDR are responsible for maintaining neighbor relationships with other routers in the network and exchanging routing information.

The DR is elected based on priority, with the router having the highest priority becoming the DR. If priorities are tied, the router with the highest Router ID is selected.

The BDR is the router with the second-highest priority or Router ID.

The DR and BDR help reduce OSPF overhead by reducing the number of adjacencies formed in multi-access networks.

Describe IPv6 addresses:

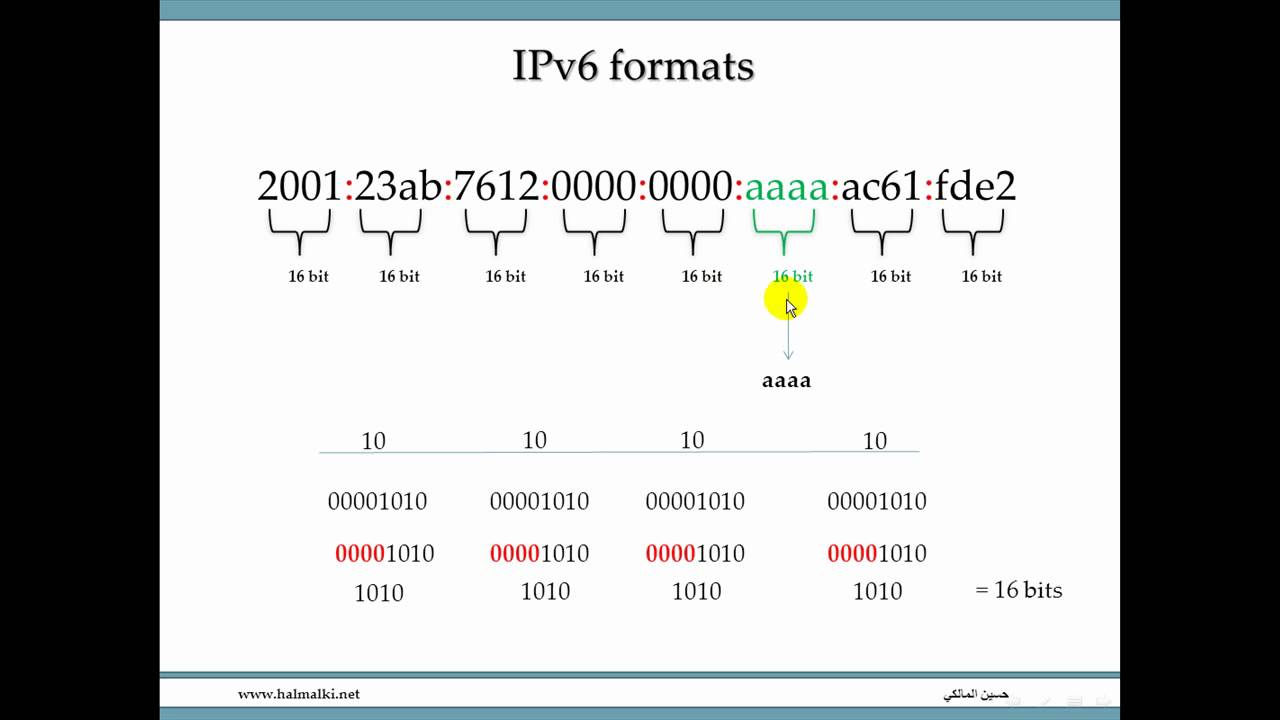
IPv6 addresses are 128-bit hexadecimal addresses used to identify devices on a network in the IPv6 protocol.

IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons, for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Leading zeros in each group can be omitted, and consecutive groups of zeros can be replaced by a double colon (::) to shorten the representation, for example, 2001:db8::8a2e:370:7334.

IPv6 addresses are divided into different types such as unicast, multicast, and anycast addresses.

Unicast addresses are used for one-to-one communication, multicast addresses for one-to-many communication, and anycast addresses for one-to-nearest communication to a group of devices.



What is 6to4 tunnel?:

6to4 tunneling is a technique used to transmit IPv6 packets over an IPv4 network.

It allows IPv6 traffic to be encapsulated within IPv4 packets, enabling communication between IPv6-enabled devices across an IPv4 network infrastructure.

In a 6to4 tunnel, IPv6 packets are encapsulated with an IPv4 header, using a special IPv6 prefix (2002::/16) to indicate that the packet should be routed through a 6to4 gateway.

6to4 tunnels automatically create virtual point-to-point links between 6to4 gateway routers, allowing IPv6 traffic to traverse IPv4 networks without the need for explicit configuration of each intermediate router.

Explain Wireless Technology:

Wireless technology refers to communication systems that transmit and receive data over the airwaves without the need for physical connections.

It enables mobility and flexibility in various applications such as mobile phones, Wi-Fi internet access, Bluetooth devices, and wireless sensor networks.

Wireless technologies use electromagnetic waves to carry signals, utilizing different frequencies and modulation techniques depending on the application.

Common wireless technologies include Wi-Fi (IEEE 802.11), Bluetooth, Zigbee, NFC (Near Field Communication), and cellular networks (e.g., 4G LTE, 5G).

Explain Basic Wireless Devices:

Basic wireless devices include devices that enable wireless communication either by transmitting or receiving data over the air.

Examples of basic wireless devices include:

Wireless routers: Devices that enable Wi-Fi connectivity by broadcasting wireless signals for devices to connect to.

Wireless access points: Devices that provide wireless access to a wired network, typically used to extend Wi-Fi coverage.

Wireless network interface cards (NICs): Hardware components installed in devices such as laptops, smartphones, and tablets to enable wireless connectivity.

Wireless adapters: External devices that connect to a computer via USB or other interfaces to provide wireless connectivity.

Bluetooth adapters: Devices that enable Bluetooth connectivity for devices that don't have built-in Bluetooth capability.

Explain Wireless Security:

Wireless security refers to measures taken to protect wireless networks and devices from unauthorized access, interception, and malicious attacks.

Common wireless security mechanisms include:

Encryption: Securely encoding data transmitted over the wireless network to prevent unauthorized interception. Common encryption protocols include WPA/WPA2-PSK (Wi-Fi Protected Access), WEP (Wired Equivalent Privacy), and AES (Advanced Encryption Standard).

Authentication: Verifying the identity of devices and users before allowing access to the wireless network. This can be achieved through passwords, digital certificates, or biometric authentication.

MAC filtering: Restricting access to the wireless network based on the MAC addresses of devices. Only devices with approved MAC addresses are allowed to connect.

Firewalls: Filtering and monitoring network traffic to prevent unauthorized access and protect against network-based attacks.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Monitoring and analyzing network traffic for signs of suspicious activity or attacks, and taking action to prevent them.



Explain WPA or WPA2 Pre-Shared Key with ad values:

WPA (Wi-Fi Protected Access) and WPA2 are security protocols designed to secure wireless networks.

WPA/WPA2 Pre-Shared Key (PSK) is a method of authentication where all devices on the network share a common passphrase.

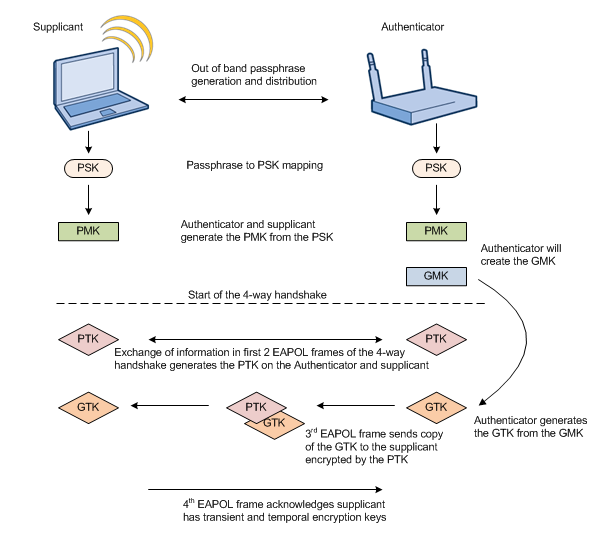
The Pre-Shared Key is used to generate encryption keys for securing data transmitted over the wireless network.

Advantages of using WPA/WPA2-PSK include:

Ease of implementation: Setting up WPA/WPA2-PSK only requires configuring the same passphrase on all devices.

Strong encryption: WPA/WPA2-PSK uses strong encryption algorithms such as AES (Advanced Encryption Standard) to protect data.

Convenience: Once configured, devices can connect to the wireless network automatically without the need for additional authentication.

Compatibility: WPA/WPA2-PSK is widely supported by most modern wireless devices and access points.

**Logging into a Switch**:

* + To log in to a network switch, you typically use either Telnet or SSH (Secure Shell) protocols.
  + **Telnet**: Telnet allows you to remotely access the switch’s command-line interface (CLI) over the network. You connect to the switch’s IP address using the Telnet client and provide valid credentials (username and password).
  + **SSH**: SSH is a more secure alternative to Telnet. It encrypts the communication between your local machine and the switch. To log in via SSH:
    1. Open a terminal or command prompt.
    2. Type: ssh username@switch-ip-address
    3. Enter your password when prompted.
  + Once logged in, you’ll be in the **User EXEC mode** (also known as user mode).

**Switch User Modes**:

* + **User EXEC Mode**:
    1. Limited access mode.
    2. Allows basic monitoring commands (e.g., checking status, interface statistics).
    3. Prompt: switch>
  + **Privileged EXEC Mode (Enable Mode)**:
    1. Provides full access to the switch’s configuration.
    2. Use the enable command to enter this mode.
    3. Useful for troubleshooting and viewing configurations.
    4. Prompt: switch#
  + **Global Configuration Mode**:
    1. Configure global settings affecting the entire switch.
    2. Use the configure terminal command to enter this mode.
    3. Set parameters like passwords, interfaces, and routing.
    4. Prompt: switch(config)#

Switch> // User Mode

Switch> enable // Entering Enable Mode

Switch# // Enable Mode

Switch# configure terminal // Entering Global Configuration Mode

Switch(config)# // Global Configuration Mode

**Gathering Basic Switch Information**:

* + Use commands like show version, show interfaces, and show running-config.
  + These commands provide details about the switch model, software version, interfaces, and current configuration.
  + Switch# show version // Display switch information
  + Switch# show running-config // Display current configuration
  + Switch# show interfaces // Display interface status
  + Switch# show vlan // Display VLAN information

**SSH (Secure Shell)**:

* + SSH is a secure protocol for remote access to network devices.
  + It encrypts data during communication.
  + Use it instead of Telnet for enhanced security.

Switch(config)# hostname SW1 // Set hostname

SW1(config)# ip domain-name example.com // Set domain name

SW1(config)# crypto key generate rsa // Generate RSA keys

SW1(config)# ip ssh version 2 // Use SSH version 2

SW1(config)# line vty 0 15 // Configure line vty for SSH

SW1(config-line)# transport input ssh // Allow SSH access

**Configuring SSH on a Switch**:

* + Enable SSH globally: crypto key generate rsa
  + Configure SSH version and authentication methods.
  + Create user accounts with SSH access: username <username> secret <password>
  + Enable SSH on specific interfaces: ip ssh version 2

SW1(config-line)# exit // Exit Line Configuration Mode

SW1(config)# exit // Exit Global Configuration Mode

**Telnet Setting**:

* + Telnet is less secure than SSH.
  + Enable Telnet globally: line vty 0 15, transport input telnet.

Switch(config)# line vty 0 15 // Configure line vty for Telnet

Switch(config-line)# transport input telnet // Allow Telnet access

Switch(config-line)# exit // Exit Line Configuration Mode

Switch(config)# exit // Exit Global Configuration Mode

**Verifying Switch Interface Status**:

* + Use show interfaces status to view interface status (up/down, speed, duplex).

Switch# show interfaces // View interface status

**Configuring VLANs**:

* + Create VLANs:  vlan <vlan-id>
  + Assign VLANs to interfaces: interface <interface> -> switchport mode access -> switchport access vlan <vlan-id>

Switch(config)# vlan 10 // Create VLAN 10

Switch(config-vlan)# name Sales // Assign name to VLAN 10

Switch(config-vlan)# exit // Exit VLAN Configuration Mode

**Verifying VLANs**:

* + Use show vlan to see configured VLANs and their associated interfaces.

Switch# show vlan // Verify VLAN configuration

**Configuring VLAN Trunking**:

* + Use switchport mode trunk on trunk interfaces.
  + Trunks carry multiple VLANs over a single link.

Switch(config)# interface GigabitEthernet0/1 // Enter interface configuration mode

Switch(config-if)# switchport mode trunk // Set interface to trunk mode

**Reasons for Using VLANs**:

* + Segmentation for security, broadcast control, and efficient resource utilization.

**Static VLANs**:

* + Manually assign VLANs to switch ports.

**Dynamic VLANs**:

* + Assign VLANs dynamically based on user authentication (e.g., 802.1X).

**STP Timer**:

* + Spanning Tree Protocol (STP) timers control convergence.
  + Key timers: Hello time, Max Age, Forward Delay.

**Switch Root Cost Calculation**:

* + Root cost is based on the cumulative path cost to the root bridge.
  + Lower cost paths are preferred.

**Configuring STP on a Switch**:

* + Enable STP: spanning-tree vlan <vlan-id> root primary
  + Adjust timers if needed.

Switch(config)# spanning-tree vlan 10 // Enable STP for VLAN 10

**Verifying STP on a Switch**:

* + Use show spanning-tree to see STP status.

Switch# show spanning-tree // View STP information

**Port Security**:

* + Prevent unauthorized devices from connecting.
  + Commands: switchport port-security, switchport port-security violation restrict.

Switch# show port-security interface gigabitethernet0/1 // Display port security configuration on specific port

Classified Default Subnet Masks:

In IP addressing, there are five classes: A, B, C, D, and E.

Each class has a specific range of IP addresses and dictates the number of devices allowed on a network.

Here are the default subnet masks for each class:

Class A: Subnet mask is 255.0.0.0 (8 bits for the network portion).

Class B: Subnet mask is 255.255.0.0 (16 bits for the network portion).

Class C: Subnet mask is 255.255.255.0 (24 bits for the network portion).

Classless Inter-Domain Routing (CIDR):

CIDR is a method that allows more efficient use of IP addresses.

It allocates and routes IP addresses based on their network prefix rather than their class.

CIDR addresses are represented using slash notation (e.g., 192.168.1.0/24).

It provides flexibility in allocating arbitrary-sized blocks of IP addresses.

Defining Subnetting Addresses:

Subnetting is the technique of dividing a large network into smaller subnetworks.

Let’s consider an example:

Suppose an administrator has the IP range 192.168.1.0/24.

Departments and their requirements:

Sales and Purchase: 120 hosts

Development: 50 hosts

Accounts: 26 hosts

Management: 5 hosts

Using VLSM, we allocate subnets with different subnet masks to meet these requirements efficiently.

Classless vs. Classful Addressing:

* Classful Addressing:

Divides IP addresses into fixed-length classes (A, B, C, D, E).

Each class has a specific range.

Less practical and can lead to IP address wastage.

* Classless Addressing (CIDR):

Introduced to replace classful addressing.

Allows more flexible allocation of IP addresses.

Uses variable-length subnet masks (VLSM) to optimize IP address usage.

Details of VLSM (Variable Length Subnet Mask):

VLSM allows subnets of different sizes within the same network.

It divides IP address ranges into smaller subnets based on specific requirements.

For example, using different subnet masks for subnets with varying numbers of hosts.

Static Routing:

Static routing involves manually configuring routes in routers.

Routes remain fixed unless manually changed.

Suitable for small networks or specific scenarios.

Default Routing:

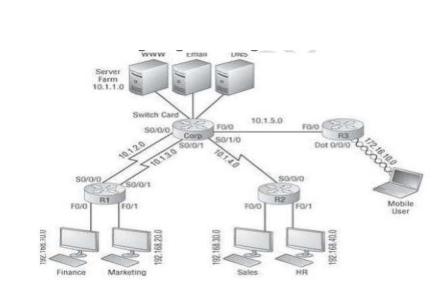
Default routes (also called gateway of last resort) are used when no specific route exists for a destination.

They point to a default gateway for forwarding packets to external networks.

Configuring IP Routing:

Configure routing protocols (e.g., RIP, OSPF) to dynamically exchange routing information.

Set up static routes for specific destinations.



Interface Configuration:

To configure an interface (e.g., S0/0/0):

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.0

no shutdown

Hostname Configuration:

Set the hostname of the device (e.g., Server):

hostname Server

Static Route Configuration:

To add a static route (e.g., to reach 192.168.20.0/24 via 10.1.30.1):

ip route 192.168.20.0 255.255.255.0 10.1.30.1

VLAN Configuration:

Create VLANs (e.g., Finance, Marketing):

vlan 10

name Finance

vlan 20

name Marketing

Switchport Configuration:

Assign VLANs to switch ports (e.g., FastEthernet0/1):

interface FastEthernet0/1

switchport mode access

switchport access vlan 10

Router Configuration:

Configure a router (e.g., R3):

hostname R3

Subnet Configuration:

Define subnets (e.g., 192.168.40.0/24):

ip subnet-zero

Default Gateway Configuration:

Set the default gateway (e.g., 10.1.5.1):

ip default-gateway 10.1.5.1

Configure VLAN Routing:

There are several ways to implement inter-VLAN routing:

Traditional Inter-VLAN Routing:

Uses a router with multiple physical interfaces, one for each VLAN.

Each router interface becomes the default gateway for hosts in its associated VLAN.

Router-on-a-Stick Inter-VLAN Routing:

Uses a single router interface connected to a trunk port on a switch.

Subinterfaces are created on the router for each VLAN.

Multilayer Switch Inter-VLAN Routing:

A multilayer switch (Layer 3 switch) performs inter-VLAN routing.

Each VLAN is assigned an SVI (Switched Virtual Interface) with an IP address.

To configure traditional inter-VLAN routing on a Cisco device, follow these steps:

Create VLANs (e.g., VLANs 10 and 20) on the switch.

Assign the VLANs to switch ports.

Configure router interfaces with IP addresses for each VLAN.

Ensure the router’s interface IP addresses become the default gateways for hosts in each VLAN.

Routing Protocol Metric:

Routing protocols use metrics to determine the best route.

Metrics are numerical values associated with specific routes.

Lower metric values indicate better paths.

Examples:

RIP: Uses hop count as the metric (maximum hop count is 15).

EIGRP: Considers bandwidth and delay.

OSPF: Uses cost (calculated based on bandwidth).

How OSPF Calculates Route Cost:

OSPF uses cost (metric) to determine the best path.

Cost is inversely proportional to link bandwidth.

Formula: Cost = Reference bandwidth / Interface bandwidth.

Default reference bandwidth is 100 Mbps.

Example: Ethernet (10 Mbps) has a cost of 10.

Benefits and Uses of IPv6:

Larger Address Space:

IPv6 provides 128-bit addresses (340 undecillion unique addresses).

Solves the address exhaustion problem faced by IPv4.

Improved Security:

Built-in IPsec for data integrity, authentication, and encryption.

Simplified Header Format:

More efficient header structure.

Easier for routers to process.

Better Support for Mobile Devices:

Vital for the proliferation of smartphones and tablets.

IPv6 Address Example:

An IPv6 address: 3001:0da8:75a3:0000:0000:8a2e:0370:7334.

128-bit address space ensures we won’t run out of addresses.

IPv6 Routing Protocols:

IPv6 supports various routing protocols like OSPFv3, RIPng, and BGP.

These protocols enable efficient routing in IPv6 networks.

Wireless Access Points (WAP):

WAPs provide wireless connectivity to wired networks.

Used for Wi-Fi access in homes, offices, and public places.

IEEE 802.11 Transmissions:

IEEE 802.11 defines Wi-Fi standards.

Different transmission modes (e.g., 802.11a, 802.11b, 802.11g).

Independent Basic Service Set (Ad Hoc):

Ad hoc mode: Devices communicate directly without an access point.

Useful for peer-to-peer connections.

Securing Wireless Networks:

Use strong encryption (WPA3).

Change default passwords.

Disable unnecessary services.

Implement MAC filtering and firewalls.

Setting Administrative Functions:

Administrative functions involve configuring various aspects of a network device. These include setting up interfaces, routing protocols, security features, and more.

Examples of administrative functions:

Configuring IP addresses on interfaces.

Enabling routing protocols (e.g., OSPF, EIGRP).

Setting up access control lists (ACLs) for security.

Managing VLANs and trunking.

Configuring NAT (Network Address Translation).

Setting Hostnames:

The hostname identifies a network device. It’s essential for management and troubleshooting.

To set the hostname on a Cisco device:

hostname MySwitch

Setting Banners:

Banners are messages displayed when someone logs in to a device.

Types of banners:

Login Banner: Displayed before login.

MOTD (Message of the Day) Banner: Displayed after login.

To set a banner:

banner login ^ Unauthorized access prohibited! ^

banner motd ^ Welcome to MySwitch! ^

Setting Passwords:

Passwords secure access to the device.

Types of passwords:

Console Password: For console access.

Enable (Privileged) Password: For entering privileged mode.

VTY (Telnet/SSH) Password: For remote access.

To set passwords:

enable secret MySecretPassword

line console 0

password MyConsolePassword

line vty 0 15

password MyVTYPassword

Viewing, Saving, and Erasing Configurations:

To view the current configuration:

show running-config

To save the configuration to non-volatile memory (startup-config):

copy running-config startup-config

To erase the startup configuration (use with caution):

erase startup-config

Configure an IP Address on a Switch:

By default, Cisco switches forward Ethernet frames without any configuration.

To perform switch management over the network or use protocols like SNMP, the switch needs an IP address.

Configure an IP address under VLAN 1 (management domain):

interface vlan 1

ip address 10.0.0.2 255.0.0.0

no shutdown

Configuring SSH:

SSH (Secure Shell) provides secure remote access to network devices.

To configure SSH on a Cisco device:

hostname MySwitch

ip domain-name example.com

crypto key generate rsa

username admin secret mypassword

line vty 0 4

transport input ssh

login local

Configuring Telnet:

Telnet provides remote access but is less secure than SSH.

To configure Telnet:

line vty 0 4

transport input telnet

password mytelnetpassword

login

Layer 3 Switch:

Combines switch and router functionality.

Operates at both Layer 2 (switching) and Layer 3 (routing).

Efficiently routes traffic within the same LAN.

Dynamic IP Configuration with DHCP:

DHCP automatically leases IP addresses to clients.

Clients contact the DHCP server to borrow an IP address.

DHCP simplifies network management.

802.1q Protocol:

IEEE 802.1q is a VLAN tagging protocol.

Adds a VLAN ID to Ethernet frames for trunking.

Switch Port Mode Command:

Configures switch ports for specific purposes (access, trunk, etc.).

Example:

interface GigabitEthernet0/1

switchport mode access

Removing a VLAN:

To remove a VLAN:

no vlan 10

Inter-VLAN Routing:

Allows communication between VLANs.

Can be done using a router or a Layer 3 switch.

Dynamic Routing:

Routers and Layer 3 switches use dynamic routing protocols.

Examples: OSPF, EIGRP, RIP.

Routing Loop:

Occurs when routers incorrectly forward packets in a loop.

Prevented by using proper routing protocols.

Inter-Switch Connectivity:

Configure trunk links between switches for VLAN traffic.

Example:

interface GigabitEthernet0/24

switchport mode trunk

VLAN Trunking:

Allows multiple VLANs over a single link.

Uses 802.1q tagging.

PAGP (Port Aggregation Protocol):

Cisco proprietary protocol for EtherChannel (link aggregation).

Bundles multiple physical links into a single logical link.

Explain and Configure PAGP:

PAGP (Port Aggregation Protocol) is a Cisco proprietary protocol used for link aggregation (EtherChannel).

It allows multiple physical links (Ethernet ports) to be bundled into a single logical channel.

PAGP dynamically negotiates and forms an EtherChannel between compatible Cisco devices.

To configure PAGP, follow these steps:

Desirable Mode (Active):

On one side, configure the interface in desirable mode (actively initiates negotiation).

Example:

interface GigabitEthernet0/1

channel-group 1 mode desirable

Auto Mode (Passive):

On the other side, configure the interface in auto mode (responds to negotiation but doesn’t initiate).

Example:

interface GigabitEthernet0/2

channel-group 1 mode auto

Verify the EtherChannel using show etherchannel summary.

Configuring Ether Channel:

EtherChannel bundles multiple physical links into a single logical link.

Example configuration:

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 10,20

Verifying Ether Channel:

Use commands like show etherchannel summary or show interfaces port-channel.

Explain PAGP and LACP:

PAGP (Port Aggregation Protocol):

Cisco proprietary protocol.

Dynamically creates EtherChannels by exchanging PAGP packets between ports.

Supported only between Cisco devices.

LACP (Link Aggregation Control Protocol):

IEEE standard (IEEE 802.3ad).

Also creates EtherChannels dynamically.

Supported by most vendors.

Configure and Verify IPv4 Addressing and Subnetting:

To configure IPv4 addressing:

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

To verify:

show ip interface brief

Explain Network Address and Broadcast Address:

Network Address: The first address in a subnet (e.g., 192.168.1.0).

Broadcast Address: The last address in a subnet (e.g., 192.168.1.255).

Explain Classful Network:

Classful networks follow the original IP address classes (A, B, C, D, E).

Each class has fixed subnet masks.

Practice Example #5B: 255.255.255.0 (/24):

This represents a /24 subnet with 256 addresses.

Network address: 192.168.1.0

Broadcast address: 192.168.1.255

Practice Example #2A: 255.255.240.0 (/20):

This represents a /20 subnet with 4096 addresses.

Network address: 192.168.0.0

Broadcast address: 192.168.15.255

Given the Number of Hosts:

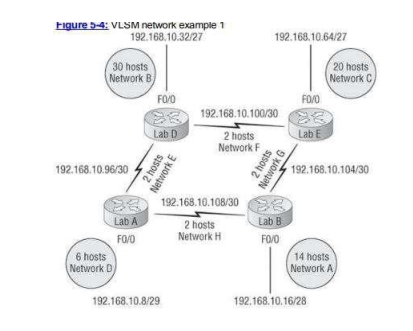
For 126 hosts: Use a /25 subnet (255.255.255.128).

For 50 hosts: Use a /26 subnet (255.255.255.192).

For 20 hosts: Use a /27 subnet (255.255.255.224).

For 5 hosts: Use a /29 subnet (255.255.255.248).

Explain this network:



Network A:

Subnet: 192.168.10.16/28

Available IP addresses: 14

Network address: 192.168.10.16

Broadcast address: 192.168.10.31

Host range: 192.168.10.17 to 192.168.10.30

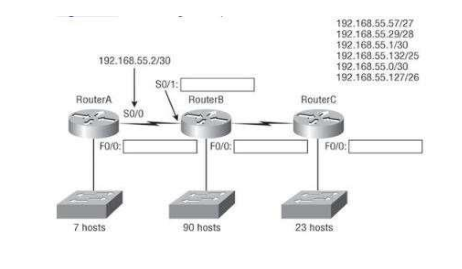
Explanation:

This is a /28 subnet, which means it has 16 available IP addresses.

The first usable IP address is 192.168.10.17, and the last usable IP address is 192.168.10.30.

The network address is 192.168.10.16, and the broadcast address is 192.168.10.31.

Put the right address in the figure:



RouterA:

S0/1: 192.168.55.2/30

S0/0: 192.168.55.1/30

F0/0: 192.168.55.57/27

RouterB:

F0/0: 192.168.55.29/28

RouterC:

F0/0: 192.168.55.132/25

Routed and Routable Protocol:

Routed Protocol:

A routed protocol is used by end devices (such as computers, servers, or printers) to send and receive data packets.

It provides addressing to end devices and encapsulates and de-encapsulates data packets.

Examples: IPv4, IPv6.

Routing Protocol:

A routing protocol is used by intermediate devices (such as routers) to discover routes and calculate the best path for data packets within a network.

It dynamically adapts to changes in network topology or traffic conditions.

Examples: OSPF, EIGRP, RIP.

IGP (Interior Gateway Protocol):

IGP is a type of routing protocol used within an autonomous system (AS) of a larger network.

It focuses on internal network routing efficiency.

Examples: RIP, OSPF, EIGRP.

Distance Vector, Link State, and Hybrid Routing:

Distance Vector:

Uses hop count (number of routers) to calculate the best path.

Examples: RIP, RIPv2.

Convergence is slow.

Broadcasts routing updates periodically.

Link State:

Uses parameters controlling traffic flows to calculate the shortest path.

Examples: OSPF.

Convergence is moderate.

Updates only when necessary or if something changes.

Hybrid:

Combines features of link state and distance vector.

Example: EIGRP.

Convergence is fast.

Updates only when necessary.

OSPFv2 (Open Shortest Path First):

OSPFv2 is a link-state routing protocol.

It calculates the shortest path using Dijkstra’s algorithm.

Suitable for larger networks.

Supports Classless Inter-Domain Routing (CIDR).

Wildcard Mask:

A wildcard mask is used to specify ranges of IP addresses.

Inverts the subnet mask.

Used in access control lists (ACLs) and routing protocols.

Address Types and Special Addresses:

Address types include unicast, multicast, and broadcast.

Special addresses include loopback (127.0.0.1), broadcast (255.255.255.255), and network (e.g., 192.168.1.0).

Configuring Cisco Routers with IPv6:

IPv6 configuration involves enabling IPv6 on interfaces, assigning IPv6 addresses, and configuringEnable IPv6 Routing Globally:

ipv6 unicast-routing

Configure an IPv6 Address on an Interface:

interface GigabitEthernet0/0

ipv6 address 2001:db8:1::1/64

no shutdown

Configure a Loopback Interface:

interface Loopback0

ipv6 address 2001:db8:2::1/64

Enable OSPFv3 for IPv6:

router ospfv3 1

router-id 1.1.1.1

area 0 range 2001:db8:1::/64

Verify the Configuration:

show ipv6 interface brief

show ipv6 ospf neighbor routing protocols.

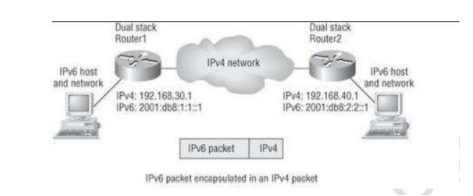
RIPng, EIGRPv6, OSPFv3:

RIPng: IPv6 version of RIP.

EIGRPv6: Enhanced Interior Gateway Routing Protocol for IPv6.

OSPFv3: OSPF for IPv6.

Create a 6to4 tunnel:



Router1 Configuration:

interface Tunnel0

ipv6 address 2001:db8:1:1::1/64

tunnel source FastEthernet0/0

tunnel mode ipv6ip 6to4

tunnel destination 192.168.40.1

Router2 Configuration:

interface Tunnel0

ipv6 address 2001:db8:2:2::1/64

tunnel source FastEthernet0/0

tunnel mode ipv6ip 6to4

tunnel destination 192.168.30.1

Verify the Tunnel:

show ipv6 interface tunnel0

802.11 Committees and Subcommittees:

The IEEE 802.11 standard, commonly known as Wi-Fi, is developed by various committees and subcommittees within the IEEE 802 working group. Here are the key ones:

Working Group (WG):

The main body responsible for developing and maintaining the 802.11 standard.

Comprised of various subgroups.

Task Group (TG):

A committee within the WG tasked with authoring specific standards or amendments.

Examples: TGme (maintenance actions), TGaz (Next Generation Positioning), TGbf (WLAN Sensing), etc.

Study Group (SG):

Researches possible future amendments.

Typically has a short lifespan (around 6 months).

Creates project authorization requests (PARs).

Topic Interest Group (TIG):

Gathers interested members to work on specific topics.

Used before forming study groups.

Standing Committee (SC):

Long-lived committee with specific roles/tasks.

Does not modify the 802.11 standard.

Ad-hoc Committee (AHC):

Short-lived committee with specific roles/tasks.

Also does not modify the standard.

These committees collaborate to develop and enhance Wi-Fi standards.

Wireless Topologies:

Wireless topologies describe how network components are arranged in a wireless network.

Common wireless topologies include:

Star Topology:

All devices connect to a central access point (AP).

AP acts as a hub for communication.

Mesh Topology:

Devices connect to each other directly.

Provides redundancy and self-healing capabilities.

Hybrid Topology:

Combines elements of other topologies.

Example: A mesh network with a central controller (star-mesh hybrid).

