**Assignment-2**

1. **Describe IPv4 address range and explain examples of subnetting ?**

### IPv4 Address Range

IPv4 addresses are 32-bit numerical labels that identify devices on a network. These addresses are typically written in dotted decimal format, consisting of four octets (8 bits each), separated by periods. For example: 192.168.1.1.

* The total possible IPv4 address space is 2322^{32} addresses, which equals 4,294,967,296 unique addresses.
* The range of valid IPv4 addresses is from 0.0.0.0 to 255.255.255.255.

### Address Classes

IPv4 addresses are divided into different classes for different purposes. Here’s a quick overview of the main classes:

1. Class A:  
   * Address range: 0.0.0.0 to 127.255.255.255
   * Default subnet mask: 255.0.0.0
   * Supports 16 million hosts (2^24 - 2 usable addresses).
   * Reserved for large networks.
2. Class B:  
   * Address range: 128.0.0.0 to 191.255.255.255
   * Default subnet mask: 255.255.0.0
   * Supports 65,000 hosts (2^16 - 2 usable addresses).
   * Reserved for medium-sized networks.
3. Class C:  
   * Address range: 192.0.0.0 to 223.255.255.255
   * Default subnet mask: 255.255.255.0
   * Supports 254 hosts (2^8 - 2 usable addresses).
   * Reserved for small networks.
4. Class D (Multicast):  
   * Address range: 224.0.0.0 to 239.255.255.255
   * Used for multicast addressing (sending data to multiple recipients).
5. Class E (Reserved for Future Use):  
   * Address range: 240.0.0.0 to 255.255.255.255
   * Reserved for experimental purposes.

### Subnetting

Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks (subnets). The primary goal of subnetting is to improve network performance and security, and to make efficient use of IP address space.

#### Subnet Masks

A subnet mask defines the boundary between the network portion and the host portion of an IP address. The subnet mask is applied to an IP address through a bitwise AND operation to separate the network and host parts.

* Default Subnet Masks:
  + Class A: 255.0.0.0
  + Class B: 255.255.0.0
  + Class C: 255.255.255.0

#### Example of Subnetting

Let's walk through a simple subnetting example.

Suppose you have a Class C IP address: 192.168.1.0/24. This means:

* Network address: 192.168.1.0
* Subnet mask: 255.255.255.0 (which corresponds to /24 or 24 bits for the network portion).
* Available addresses for hosts: 192.168.1.1 to 192.168.1.254.

Now, you want to create 4 subnets from this Class C network.

Step 1: Determine the new subnet mask.

To create 4 subnets, we need to borrow 2 bits from the host portion (since 2^2 = 4). The original subnet mask is 255.255.255.0 (which is /24), so by borrowing 2 bits, we get a new subnet mask of 255.255.255.192 (or /26).

Step 2: Create the subnets.

With a /26 subnet mask, each subnet will have 64 addresses (2^6). The network addresses for the subnets will be:

1. 192.168.1.0/26 (Network: 192.168.1.0, Range: 192.168.1.1 to 192.168.1.62, Broadcast: 192.168.1.63)
2. 192.168.1.64/26 (Network: 192.168.1.64, Range: 192.168.1.65 to 192.168.1.126, Broadcast: 192.168.1.127)
3. 192.168.1.128/26 (Network: 192.168.1.128, Range: 192.168.1.129 to 192.168.1.190, Broadcast: 192.168.1.191)
4. 192.168.1.192/26 (Network: 192.168.1.192, Range: 192.168.1.193 to 192.168.1.254, Broadcast: 192.168.1.255)

Each subnet has a total of 64 addresses, but only 62 usable IP addresses (since the network address and broadcast address are reserved).

1. **List of private addresses ?**

Private IPv4 addresses are reserved for use within private networks and are not routable over the public internet. These addresses are defined by the Internet Assigned Numbers Authority (IANA) and are specified in RFC 1918 for IPv4.

Here are the ranges of private IPv4 addresses:

### Class A Private IP Range:

* 10.0.0.0 to 10.255.255.255
* Subnet mask: 255.0.0.0 (or /8)

### Class B Private IP Range:

* 172.16.0.0 to 172.31.255.255
* Subnet mask: 255.240.0.0 (or /12)

### Class C Private IP Range:

* 192.168.0.0 to 192.168.255.255
* Subnet mask: 255.255.255.0 (or /16)

### Summary of Private Address Ranges:

* Class A: 10.0.0.0 – 10.255.255.255
* Class B: 172.16.0.0 – 172.31.255.255
* Class C: 192.168.0.0 – 192.168.255.255

These private IP address ranges can be used within internal networks, such as home or office networks, but are not directly accessible from the internet. To allow communication between a private network and the public internet, devices typically use Network Address Translation (NAT).

1. **What is routing? Explain work of Router and protocol ?**

### Routing:

Routing is the process of determining the best path for data to travel across a network from its source to its destination. It is essentially the mechanism that allows data packets to move between different networks or subnets. Routing is carried out by routers, which examine the destination IP address of each packet and forward it to the appropriate next hop toward its final destination.

### Router:

A router is a network device that forwards data packets between different networks. It connects different networks (such as a local area network (LAN) to the internet) and uses routing tables and protocols to determine the optimal path for forwarding packets.

#### Work of a Router:

* Forwarding Packets: A router checks the destination IP address of incoming data packets and forwards them to the next device or router in the path based on the routing table.
* Routing Table: The router maintains a routing table that lists the possible destinations and the best path to each one. The table is dynamically updated using routing protocols.
* Network Address Translation (NAT): Routers often perform NAT to allow devices on a private network to access the public internet by translating private IP addresses to a single public IP address.

### Routing Protocols:

Routing protocols are used by routers to dynamically discover and maintain the best paths in the network. Some common types of routing protocols include:

1. Interior Gateway Protocols (IGP): Used within an organization or local network.  
   * RIP (Routing Information Protocol): A distance-vector protocol that calculates the best path based on hop count.
   * OSPF (Open Shortest Path First): A link-state protocol that calculates the best path using the network topology.
   * EIGRP (Enhanced Interior Gateway Routing Protocol): A hybrid protocol combining aspects of both distance-vector and link-state protocols.
2. Exterior Gateway Protocols (EGP): Used to exchange routing information between different networks (typically between ISPs).  
   * BGP (Border Gateway Protocol): The protocol used to exchange routing information on the internet.

### In Summary:

* Routing ensures data finds the best path from source to destination.
* Routers are devices that forward packets between networks using routing tables and protocols.
* Routing Protocols (e.g., RIP, OSPF, BGP) help routers determine and maintain optimal paths in the network.

Let me know if you'd like more detail on any of these**!**

1. **Which software we use for routing and switching ?**

Here’s a quick list of software used for routing and switching:

1. Cisco IOS – Used on Cisco routers and switches, supports advanced routing and switching protocols.
2. Junos OS – Used on Juniper Networks devices, known for scalability and flexibility in routing.
3. MikroTik RouterOS – Affordable software for small to medium-sized networks, offering both routing and switching features.
4. pfSense – Open-source software for routing and firewalling, commonly used in small networks or as a virtual appliance.
5. VyOS – Open-source Linux-based routing software, suitable for custom routers and virtual setups.
6. Huawei VRP – Routing and switching software used in Huawei networking devices, suitable for enterprise and service provider networks.
7. Cumulus Linux – Linux-based software designed for data centers with full routing and switching support.
8. ExtremeXOS – Used on Extreme Networks devices for high-performance routing and switching in enterprise environments.
9. **Explain Basic command ?**

Here are some basic networking commands used in routing and switching on common network devices (routers, switches) or operating systems (like Linux or Cisco devices):

### Cisco Router/Switch Basic Commands

1. show ip interface brief:  
   * Displays a summary of the router's or switch's IP interfaces (IP address, interface status, etc.).

Example:  
 Router# show ip interface brief

1. show running-config:  
   * Displays the current configuration running on the router or switch.

Example:  
 Router# show running-config

1. show ip route:  
   * Shows the routing table of the router, which contains information about known networks and their routes.

Example:  
 Router# show ip route

1. ping:  
   * Sends an ICMP echo request to check network connectivity between devices.

Example:  
 Router# ping 192.168.1.1

1. traceroute:  
   * Traces the path packets take to a destination, showing each hop in the network.

Example:  
 Router# traceroute 8.8.8.8

1. enable:  
   * Moves from user mode to privileged EXEC mode, allowing access to more advanced commands.

Example:  
 Router> enable

1. config terminal:  
   * Enters global configuration mode, where network configurations can be modified.

Example:  
 Router# config terminal

1. interface:  
   * Configures a specific interface (e.g., Ethernet, VLAN) on the router or switch.

Example:  
 Router(config)# interface GigabitEthernet 0/1

1. ip address:  
   * Assigns an IP address to an interface.

Example:  
 Router(config-if)# ip address 192.168.1.1 255.255.255.0

1. no shutdown:  
   * Enables an interface that has been administratively shut down.

Example:  
 Router(config-if)# no shutdown

1. show version:  
   * Displays system hardware and software information, including device model and IOS version.

Example:  
 Router# show version

1. copy running-config startup-config:  
   * Saves the current running configuration to the startup configuration file, which is loaded when the router or switch restarts.

Example:  
 Router# copy running-config startup-config

1. reload:  
   * Restarts the router or switch.

Example:  
 Router# reload

### Linux-based Networking Commands

1. ifconfig:  
   * Displays or configures network interfaces (similar to show ip interface brief in Cisco).

Example:  
 sudo ifconfig

1. ip addr show:  
   * Displays IP addresses and network interfaces.

Example:  
 ip addr show

1. ping:  
   * Checks connectivity to another network device.

Example:  
 ping 192.168.1.1

1. netstat:  
   * Displays network connections, routing tables, and interface statistics.

Example:  
 netstat -r

1. route:  
   * Displays or modifies the IP routing table.

Example:  
 route -n

1. traceroute:  
   * Traces the path of packets to a destination.

Example:  
 traceroute 8.8.8.8

1. ip route:  
   * Displays the routing table on Linux systems.

Example:  
 ip route show

### Summary of Basic Commands:

* Configuration & Status: show running-config, show ip interface brief, ifconfig, ip addr show
* Testing & Troubleshooting: ping, traceroute, netstat
* Routing Table: show ip route, ip route show, route -n
* Interface Configuration: interface, ip address, no shutdown
* System Info: show version, show running-config

These commands are essential for managing, troubleshooting, and configuring network devices like routers and switches.

1. **Types of Routing – example of Static routing ?**

### Types of Routing

Routing is the process of selecting paths in a network to send data packets from one device to another. There are three main types of routing:

1. Static Routing  
   * Manually configured by network administrators.
   * Suitable for small networks with limited route changes.
   * Does not adapt automatically to network changes.
   * Example: A simple home or small office network where all routes are predefined.
2. Dynamic Routing  
   * Uses protocols like RIP, OSPF, and BGP to update routing tables automatically.
   * Adapts to network changes and failures.
   * Used in larger networks with frequently changing topologies.
3. Default Routing  
   * Used when a router does not have a specific route for a destination.
   * All unknown traffic is forwarded to a predefined gateway.
   * Often used in small networks connecting to the internet.

### Example of Static Routing (Cisco Router Configuration)

Assume we have two routers (R1 and R2) connected through the network:

R1 (192.168.1.1) -------- (192.168.1.2) R2

To configure a static route in R1 to reach a network behind R2 (e.g., 192.168.2.0/24), the command would be:

R1(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.2

This command tells R1 that any packet destined for the 192.168.2.0/24 network should be sent to R2's IP address (192.168.1.2).

1. **Explain Dynamic routing ?**

### Dynamic Routing

Definition:  
 Dynamic routing is a networking technique in which routers automatically learn and update routes using routing protocols. This allows the network to adapt to topology changes, such as link failures or new network additions, without manual intervention.

### How Dynamic Routing Works

1. Routers exchange routing information using dynamic routing protocols.
2. Routing tables are updated automatically based on network changes.
3. Best paths are selected dynamically using algorithms that consider factors like hop count, bandwidth, and latency.

### Advantages of Dynamic Routing

Scalability – Works well for large and complex networks.  
 Automatic Updates – Adjusts routes when network topology changes.  
 Load Balancing – Can distribute traffic efficiently across multiple paths.  
 Less Administrative Effort – No need for manual route configurations.

### Disadvantages of Dynamic Routing

Higher Resource Usage – Requires more CPU and memory than static routing  
 Slower Convergence – Takes time to update and propagate route chnges.  
 Complexity – More difficult to configure and troubleshoot compared to static routing.

### Types of Dynamic Routing Protocols

Dynamic routing uses protocols to share routing information between routers. These protocols fall into two main categories:

1. Distance Vector Protocols – Determine the best route based on the number of hops (routers) between the source and destination.  
   * Example:
     + RIP (Routing Information Protocol) – Uses hop count as a metric, with a maximum of 15 hops.
     + IGRP (Interior Gateway Routing Protocol) – Cisco’s proprietary protocol, an improvement over RIP.
2. Link-State Protocols – Consider factors like speed, bandwidth, and congestion rather than just hop count.  
   * Example:
     + OSPF (Open Shortest Path First) – Uses Dijkstra’s algorithm to compute the shortest path.
     + IS-IS (Intermediate System to Intermediate System) – Similar to OSPF, used in large ISPs and backbone networks.
3. Hybrid Protocols – Combine features of both distance vector and link-state protocols.  
   * Example:
     + EIGRP (Enhanced Interior Gateway Routing Protocol) – Cisco’s advanced protocol that provides fast convergence and efficient routing.
     + BGP (Border Gateway Protocol) – Used for routing between different networks (e.g., between ISPs on the internet).

### Example of Dynamic Routing (OSPF Configuration in Cisco Router)

R1(config)# router ospf 1

R1(config-router)# network 192.168.1.0 0.0.0.255 area 0

R1(config-router)# exit

This configures OSPF on a Cisco router to advertise the 192.168.1.0/24 network in area 0.

### When to Use Dynamic Routing?

Large networks with frequently changing topology  
 Environments where manual route management is impractical  
 Networks requiring high availability and redundancy

1. **Difference between RIP EIGRP and OSPF ?**

### 1. RIP (Routing Information Protocol)

* Type: Distance Vector Protocol
* Metric Used: Hop count (Maximum 15 hops)
* Algorithm: Bellman-Ford
* Convergence Speed: Slow
* Routing Updates: Sent every 30 seconds (causes extra network traffic)
* Classless Support: RIP v1 (No), RIP v2 (Yes, supports VLSM)
* Best for: Small networks (due to hop count limitation)
* Resource Usage: Low
* Protocol Number: Uses UDP Port 520

#### 2. EIGRP (Enhanced Interior Gateway Routing Protocol)

* Type: Hybrid Protocol (Distance Vector + Link-State)
* Metric Used: Composite metric (Bandwidth, Delay, Load, Reliability)
* Algorithm: DUAL (Diffusing Update Algorithm)
* Convergence Speed: Fast
* Routing Updates: Sent only when topology changes occur (reduces overhead)
* Classless Support: Yes (Supports VLSM and CIDR)
* Best for: Medium to Large Cisco-based networks
* Resource Usage: Moderate
* Proprietary or Open Standard: Cisco Proprietary
* Protocol Number: Uses Protocol Number 88

#### 3. OSPF (Open Shortest Path First)

* Type: Link-State Protocol
* Metric Used: Cost (Based on Bandwidth)
* Algorithm: Dijkstra’s Shortest Path First (SPF)
* Convergence Speed: Faster than RIP but slightly slower than EIGRP
* Routing Updates: Sent only when topology changes occur
* Classless Support: Yes (Supports VLSM and CIDR)
* Best for: Large multi-vendor enterprise networks
* Resource Usage: High
* Proprietary or Open Standard: Open Standard (Works on all devices)
* Protocol Number: Uses Protocol Number 89

1. **Perform Examples of RIP EIGRP and OSPF with different area concepts?**

## 1. RIP Configuration (Version 2)

### Scenario:

Two routers (R1 and R2) are connected, and we need to enable RIP v2 for communication.

### Network Topology:

R1 (192.168.1.1) ---- (192.168.1.2) R2

R1's LAN: 10.0.0.0/24

R2's LAN: 20.0.0.0/24

### RIP Configuration on R1:

R1(config)# router rip

R1(config-router)# version 2 # Enables RIP v2

R1(config-router)# no auto-summary # Disables automatic summarization

R1(config-router)# network 192.168.1.0

R1(config-router)# network 10.0.0.0

R1(config-router)# exit

### RIP Configuration on R2:

R2(config)# router rip

R2(config-router)# version 2

R2(config-router)# no auto-summary

R2(config-router)# network 192.168.1.0

R2(config-router)# network 20.0.0.0

R2(config-router)# exit

Explanation:

* RIP v2 is used because it supports VLSM and CIDR.
* no auto-summary ensures subnets are advertised properly instead of classful boundaries.
* network commands define which networks should participate in RIP.

## 2. EIGRP Configuration (Autonomous System 100)

### Scenario:

Three routers (R1, R2, R3) with EIGRP enabled in Autonomous System 100.

### Network Topology:

R1 (10.1.1.1) ---- (10.1.1.2) R2 ---- (10.1.1.3) R3

R1's LAN: 192.168.1.0/24

R2's LAN: 192.168.2.0/24

R3's LAN: 192.168.3.0/24

### EIGRP Configuration on R1:

R1(config)# router eigrp 100 # Define AS number

R1(config-router)# network 10.1.1.0 0.0.0.255

R1(config-router)# network 192.168.1.0 0.0.0.255

R1(config-router)# no auto-summary

R1(config-router)# exit

### EIGRP Configuration on R2:

R2(config)# router eigrp 100

R2(config-router)# network 10.1.1.0 0.0.0.255

R2(config-router)# network 192.168.2.0 0.0.0.255

R2(config-router)# no auto-summary

R2(config-router)# exit

### EIGRP Configuration on R3:

R3(config)# router eigrp 100

R3(config-router)# network 10.1.1.0 0.0.0.255

R3(config-router)# network 192.168.3.0 0.0.0.255

R3(config-router)# no auto-summary

R3(config-router)# exit

Explanation:

* EIGRP 100 defines the Autonomous System (AS).
* network commands specify which networks will participate in EIGRP routing updates.
* no auto-summary prevents classful summarization to ensure proper subnet advertisement.

## 3. OSPF Configuration (with Multi-Area)

### Scenario:

Three routers (R1, R2, R3) configured with OSPF multi-area design.

### Network Topology (Multi-Area OSPF):

AREA 0 (BACKBONE)

----------------

| |

(10.0.0.1) (10.0.0.2)

R1 -------------- R2

| |

AREA 1 | AREA 2 |

(192.168.1.0) (192.168.2.0)

| |

R3 R4

### OSPF Configuration on R1 (Backbone - Area 0):

R1(config)# router ospf 1

R1(config-router)# network 10.0.0.0 0.0.0.255 area 0

R1(config-router)# exit

### OSPF Configuration on R2 (Backbone - Area 0):

R2(config)# router ospf 1

R2(config-router)# network 10.0.0.0 0.0.0.255 area 0

R2(config-router)# exit

### OSPF Configuration on R3 (Area 1):

R3(config)# router ospf 1

R3(config-router)# network 192.168.1.0 0.0.0.255 area 1

R3(config-router)# exit

### OSPF Configuration on R4 (Area 2):

R4(config)# router ospf 1

R4(config-router)# network 192.168.2.0 0.0.0.255 area 2

R4(config-router)# exit

Explanation:

* OSPF is structured into multiple areas for better scalability.
* Area 0 (Backbone) is the central hub connecting other areas.
* R1 and R2 operate in Area 0 (Backbone), while R3 and R4 belong to Area 1 and Area 2, respectively.
* This design improves network performance and reduces routing overhead.

## Comparison of RIP, EIGRP, and OSPF Configurations

| Feature | RIP | EIGRP | OSPF |
| --- | --- | --- | --- |
| Routing Type | Distance Vector | Hybrid | Link-State |
| Metric Used | Hop Count | Bandwidth, Delay, Load, Reliability | Cost (Based on Bandwidth) |
| Convergence Speed | Slow | Fast | Medium |
| Network Size | Small | Medium to Large | Large Enterprise |
| Multi-Area Support | No | No | Yes |
| Vendor Compatibility | Open Standard | Cisco Proprietary | Open Standard |
| Hop Limit | 15 | No Limit | No Limit |
| Algorithm Used | Bellman-Ford | DUAL | Dijkstra's SPF |

1. **Example of Default routing ?**

### Example of Default Routing

Definition:  
 Default routing is used when a router does not have a specific route for a destination network and forwards all unknown traffic to a predefined default gateway. It is commonly used in small networks or when a router connects to an ISP for internet access.

### Scenario:

A network has Router R1, which connects an internal LAN (192.168.1.0/24) to the ISP (Internet Service Provider) via Router R2. R1 does not know all internet routes, so it needs a default route to send all unknown traffic to R2 (Gateway: 10.0.0.2).

### Network Topology:

LAN (192.168.1.0/24) ---- (192.168.1.1) R1 ---- (10.0.0.2) R2 (ISP)

### Default Route Configuration on R1

R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2

Explanation:

* 0.0.0.0 0.0.0.0 represents any destination (unknown networks).
* 10.0.0.2 is the next-hop IP (Router R2) to forward all unknown traffic.
* This ensures that R1 sends all non-local traffic (such as internet requests) to R2.

### Verification Commands:

After configuring, verify the default route with:

R1# show ip route

You should see an entry like:

S\* 0.0.0.0/0 [1/0] via 10.0.0.2

* S\* means a static default route.
* [1/0] is the administrative distance and metric.
* via 10.0.0.2 shows the next-hop router.

### Use Cases for Default Routing:

Small office/home networks connecting to the internet  
 Edge routers forwarding traffic to ISPs  
 Networks with only one exit point

1. **Explain Autonomous system number ?**

An Autonomous System (AS) is a group of IP networks and routers under a single administrative control, such as an ISP, enterprise, or data center. These systems operate using a common routing policy and are identified by a unique Autonomous System Number (ASN).

An Autonomous System Number (ASN) is a unique 16-bit or 32-bit number assigned to an AS by the Internet Assigned Numbers Authority (IANA) and regional Internet registries (RIRs). Routers use ASNs to exchange routing information between different networks using Border Gateway Protocol (BGP).

### Types of ASNs

1. Public ASN
   * Assigned by IANA and RIRs.
   * Used for BGP routing between different organizations.
   * Example: ISPs, large enterprises, or cloud providers.
2. Private ASN
   * Used for internal networks that do not need to connect to external ASNs.
   * Range: 64512 - 65534 (16-bit) or 4200000000 - 4294967294 (32-bit).
   * Example: Enterprises using BGP internally between data centers.

### Types of Autonomous Systems

1. Stub AS
   * Connected to only one other AS (e.g., a small organization using a single ISP).
2. Multihomed AS
   * Connected to multiple ASNs for redundancy but does not route traffic between them.
3. Transit AS
   * Routes traffic between multiple ASNs (e.g., ISPs providing backbone connectivity).

### ASN Format (16-bit vs. 32-bit)

| Type | Range | Example |
| --- | --- | --- |
| 16-bit ASN | 1 - 65534 | 64500 (Private), 12345 (Public) |
| 32-bit ASN | 65536 - 4294967295 | 4200000001 (Private), 200000 (Public) |

### Example: ASN in BGP Configuration

#### Scenario:

An ISP (AS 65001) connects to another ISP (AS 65002) using BGP.

#### BGP Configuration on Router R1 (AS 65001):

R1(config)# router bgp 65001

R1(config-router)# neighbor 192.168.1.2 remote-as 65002

R1(config-router)# exit

* This command configures BGP on R1 with ASN 65001 and establishes a BGP peer with R2 (65002).

### Why is ASN Important?

Helps routers identify different networks on the internet.  
 Allows ISPs and enterprises to exchange routing information via BGP.  
 Prevents routing loops and enhances network security.  
 Supports load balancing and redundancy in large-scale networks.

1. **What is switching to explain VLAN ?**

Switching is the process of forwarding data packets within a network based on MAC addresses. A network switch is a Layer 2 device that operates in a LAN (Local Area Network) to connect multiple devices and efficiently forward data between them.

#### Types of Switching:

1. Circuit Switching – Establishes a dedicated communication path (e.g., telephone networks).
2. Packet Switching – Data is broken into packets and sent independently (e.g., internet).
3. Message Switching – Entire messages are sent and stored before forwarding.

### What is a VLAN (Virtual Local Area Network)?

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a switch that segments the network into multiple broadcast domains. VLANs allow devices in different physical locations to communicate as if they were on the same network, improving security and reducing congestion.

#### Key Features of VLANs:

✔ Segmentation: Divides a physical switch into multiple logical networks.  
 ✔ Security: Prevents unauthorized access by isolating devices into different VLANs.  
 ✔ Broadcast Control: Reduces unnecessary traffic by limiting broadcast domains.  
 ✔ Flexibility: Devices can be grouped logically instead of physically.

### Example VLAN Configuration on a Cisco Switch

#### Scenario:

A company has two departments: Sales (VLAN 10) and IT (VLAN 20). We configure a switch to separate these departments using VLANs.

#### Step 1: Create VLANs

Switch(config)# vlan 10

Switch(config-vlan)# name Sales

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name IT

Switch(config-vlan)# exit

#### Step 2: Assign Ports to VLANs

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

* Port Fa0/1 is assigned to VLAN 10 (Sales).
* Port Fa0/2 is assigned to VLAN 20 (IT).

### VLAN Types:

1. Default VLAN (VLAN 1) – The built-in VLAN on all switches.
2. Data VLAN – Used for user data (e.g., VLAN 10 for Sales).
3. Voice VLAN – Dedicated for VoIP traffic to ensure quality.
4. Management VLAN – Used for switch management (e.g., VLAN 99).
5. Native VLAN – The VLAN that carries untagged traffic on trunk links.

### How VLANs Improve Networks

Reduces Broadcast Traffic – Limits the spread of broadcast packets.  
 Enhances Security – Prevents unauthorized access to sensitive data.  
 Increases Performance – Segments traffic, reducing network congestion.  
 Simplifies Management – Logical separation allows easier network changes.

1. **What is Access port and trunk port ?**

In VLAN-based networks, switch ports are configured as either Access Ports or Trunk Ports to control how traffic is transmitted between devices.

## 1. What is an Access Port?

An Access Port is a switch port that carries traffic for only one VLAN. It is typically used to connect end devices such as computers, printers, or VoIP phones.

### Key Features of Access Ports:

Assigned to a single VLAN (e.g., VLAN 10 for Sales).  
 Strips VLAN tags from incoming frames before forwarding to the connected device.  
 Used for end-user devices that don’t understand VLAN tagging.  
 Cannot carry multiple VLANs.

### Example Configuration of Access Port (Cisco Switch)

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

* FastEthernet 0/1 is now an Access Port assigned to VLAN 10.
* Any device connected to this port will only communicate within VLAN 10.

## 2. What is a Trunk Port?

A Trunk Port is a switch port that carries traffic for multiple VLANs. It is used to connect switches together or link to routers, servers, or VLAN-aware devices.

### Key Features of Trunk Ports:

Carries multiple VLANs over a single link.  
 Uses VLAN tagging (IEEE 802.1Q) to identify which VLAN a frame belongs to.  
 Typically used for switch-to-switch or switch-to-router connections.  
 Can have a Native VLAN that carries untagged traffic.

### Example Configuration of Trunk Port (Cisco Switch)

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,30

Switch(config-if)# switchport trunk native vlan 99

Switch(config-if)# exit

* FastEthernet 0/2 is now a Trunk Port.
* It allows VLAN 10, 20, and 30 to pass through.
* VLAN 99 is set as the Native VLAN, meaning untagged frames are assigned to VLAN 99.

## Differences Between Access Port & Trunk Port

| Feature | Access Port | Trunk Port |
| --- | --- | --- |
| VLAN Support | Supports only one VLAN | Supports multiple VLANs |
| VLAN Tagging | No tagging, frames are untagged | Uses 802.1Q tagging |
| Device Connection | Used for end devices (PCs, printers, phones) | Used for switch-to-switch or switch-to-router connections |
| Native VLAN | Not applicable | Supports Native VLAN for untagged traffic |
| Example Usage | Connecting a computer to VLAN 10 | Connecting two switches carrying VLAN 10, 20, 30 |

### Final Thoughts

* Use Access Ports for connecting end devices that don’t need to understand VLANs.
* Use Trunk Ports for connecting switches or routers that need to pass traffic for multiple VLANs.

1. **List of basic SHOW commands. • Explain Layer 2 and Layer 3 switch ?**

### Basic SHOW Commands in Cisco Devices

show version – Displays device hardware, software version, and uptime.  
 show running-config – Shows the current configuration in RAM.  
 show startup-config – Displays the configuration stored in NVRAM.  
 show interfaces – Shows status and details of all interfaces.  
 show ip interface brief – Displays a summary of interfaces with IPs and status.  
 show mac address-table – Shows the MAC address table on a switch.  
 show vlan brief – Displays VLANs configured on the switch.  
 show interfaces trunk – Shows active trunk ports and VLANs allowed.  
 show ip route – Displays the routing table.  
 show arp – Shows the ARP table (MAC-to-IP mapping).  
 show spanning-tree – Displays Spanning Tree Protocol (STP) status.  
 show cdp neighbors – Shows directly connected Cisco devices.

### Layer 2 vs. Layer 3 Switch

#### 1. Layer 2 Switch (L2)

Operates at Data Link Layer (Layer 2).  
 Uses MAC addresses for forwarding traffic.  
 Cannot perform IP routing between VLANs.  
 Supports VLAN segmentation and trunking.  
 Uses Spanning Tree Protocol (STP) to prevent loops.  
 Requires an external router for inter-VLAN communication.  
 Used for small networks and Access Layer connections.

#### 2. Layer 3 Switch (L3)

Operates at Network Layer (Layer 3).  
 Can perform both switching (MAC-based) and routing (IP-based).  
 Supports inter-VLAN routing (without an external router).  
 Uses IP routing protocols (e.g., OSPF, EIGRP, RIP).  
 Provides higher performance in large networks.  
 Used for enterprise networks, Core Layer, and Data Centers.

### **Key Differences Between L2 and L3 Switch:-**

| Feature | Layer 2 Switch | Layer 3 Switch |
| --- | --- | --- |
| Works on | Data Link Layer (L2) | Network Layer (L3) |
| Traffic Forwarding | Based on MAC addresses | Based on IP addresses |
| Routing Capability | No | Yes |
| Inter-VLAN Routing | Needs an external router | Built-in routing |
| Routing Protocols | Not supported | Supports OSPF, EIGRP, BGP |
| Use Case | Small networks, Access Layer | Large networks, Core Layer |

1. **Example – VLAN Access port and trunk port?**

A company has two departments:

* Sales (VLAN 10)
* IT (VLAN 20)

We will configure:

1. Access Ports to assign computers in each department to their VLANs.
2. Trunk Ports to allow VLAN traffic between switches.

## 1. Access Port Configuration

Access ports are used to connect end devices (PCs, printers, etc.) to a specific VLAN.

### Example: Assigning VLANs to Access Ports

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10 # Assign to VLAN 10 (Sales)

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20 # Assign to VLAN 20 (IT)

Switch(config-if)# exit

Port Fa0/1 is assigned to VLAN 10 (Sales).  
 Port Fa0/2 is assigned to VLAN 20 (IT).  
 Devices connected to these ports will only communicate within their VLAN.

## 2. Trunk Port Configuration

Trunk ports allow multiple VLANs to pass between switches or to a router for inter-VLAN communication.

### Example: Configuring a Trunk Port

Switch(config)# interface fastEthernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20

Switch(config-if)# switchport trunk native vlan 99 # Assign native VLAN

Switch(config-if)# exit

Port Fa0/24 is now a Trunk Port.  
 Allows VLAN 10 (Sales) and VLAN 20 (IT) traffic between switches.  
 Native VLAN 99 is used for untagged traffic.

Diagram Representation

PC1 (Sales) ---- Fa0/1 [Switch] Fa0/24 ---- [Switch] Fa0/24 ---- Fa0/2 (PC2 IT)

VLAN 10 Access Port Trunk Port Trunk Port VLAN 20

1. **Example of inter VLAN routing ?**

A company has two departments:

* Sales (VLAN 10) – 192.168.10.0/24
* IT (VLAN 20) – 192.168.20.0/24

Employees in VLAN 10 (Sales) need to communicate with employees in VLAN 20 (IT). Since VLANs are separate broadcast domains, a Layer 3 device (Router or Layer 3 Switch) is required to route packets between them.

## 1. Method 1: Inter-VLAN Routing Using a Router (Router-on-a-Stick)

In this method, a router with a single trunk link is used to route traffic between VLANs.

### Step 1: Configure VLANs on the Switch

Switch(config)# vlan 10

Switch(config-vlan)# name Sales

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name IT

Switch(config-vlan)# exit

### Step 2: Assign VLANs to Access Ports

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

### Step 3: Configure a Trunk Port to the Router

Switch(config)# interface fastEthernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20

Switch(config-if)# exit

### Step 4: Configure Sub-Interfaces on the Router

Router(config)# interface gigabitEthernet 0/0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface gigabitEthernet 0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitEthernet 0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Router(config-subif)# exit

✔ Router now routes traffic between VLAN 10 and VLAN 20.  
 ✔ PCs in VLAN 10 use 192.168.10.1 as the gateway.  
 ✔ PCs in VLAN 20 use 192.168.20.1 as the gateway.

## 2. Method 2: Inter-VLAN Routing Using a Layer 3 Switch

Instead of using a router, we can configure SVIs (Switch Virtual Interfaces) on a Layer 3 switch to handle inter-VLAN routing.

### Step 1: Enable Routing on the Switch

Switch(config)# ip routing

### Step 2: Create VLANs

Switch(config)# vlan 10

Switch(config-vlan)# name Sales

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name IT

Switch(config-vlan)# exit

### Step 3: Configure SVIs (Virtual Interfaces for Each VLAN)

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 20

Switch(config-if)# ip address 192.168.20.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

### Step 4: Assign VLANs to Access Ports

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

✔ No need for a router! The switch itself routes traffic between VLANs.  
 ✔ PCs in VLAN 10 use 192.168.10.1 as the gateway.  
 ✔ PCs in VLAN 20 use 192.168.20.1 as the gateway.

### Which Method to Choose?

| Feature | Router-on-a-Stick | Layer 3 Switch |
| --- | --- | --- |
| Hardware Used | Router & Switch | Layer 3 Switch |
| Performance | Slower (Router processes traffic) | Faster (Switch processes traffic) |
| Scalability | Good for small networks | Better for large networks |
| Configuration Complexity | Moderate | Easier |

1. **Explain switching method and VTP ?**

## Switching Methods in Networking

Switching is a process where network devices forward frames based on MAC addresses. There are three primary switching methods:

### 1. Store-and-Forward Switching

The switch receives the entire frame, checks for errors (CRC Check), and then forwards it.  
 Provides high reliability since corrupted frames are discarded.  
 Slower than other methods because it processes the entire frame before forwarding.  
 Used in enterprise networks where accuracy is crucial.

### 2. Cut-Through Switching

The switch forwards the packet immediately after reading the destination MAC address.  
 Faster than store-and-forward but does not check for errors.  
 Suitable for low-latency environments like VoIP and real-time applications.

### 3. Fragment-Free Switching (Hybrid)

The switch reads the first 64 bytes before forwarding the frame.  
 Reduces forwarding delays while checking for small errors.  
 Used in performance-sensitive environments.

## VLAN Trunking Protocol (VTP)

VTP (VLAN Trunking Protocol) is a Cisco-proprietary protocol used to manage VLANs across multiple switches.

### How VTP Works?

Sends VLAN information between switches to maintain consistency.  
 Reduces manual VLAN configuration on multiple switches.  
 Works over trunk links (802.1Q or ISL).

### VTP Modes:

| Mode | Function |
| --- | --- |
| Server | Creates, modifies, and propagates VLANs. Default mode. |
| Client | Cannot create VLANs, only receives updates from a server. |
| Transparent | Maintains its own VLANs and does not sync with VTP. |

### VTP Configuration Example:

Switch(config)# vtp domain MY\_COMPANY

Switch(config)# vtp mode server

Switch(config)# vtp password secure123

VTP Domain: Ensures all switches share VLAN info.  
 VTP Mode: Set as server to manage VLANs.  
 VTP Password: Ensures security for updates.

1. **What is spanning Tree – Mention spanning tree protocol and algorithm ?**

Layer 2 protocol that prevents switching loops in redundant networks.  
 Ensures only one active path exists between switches.  
 Automatically reactivates blocked links if an active link fails.

Types of Spanning Tree Protocols (STP Variants)

STP (802.1D) – Original, slow convergence (~50 sec).  
 RSTP (802.1w) – Faster convergence (~6 sec).  
 MSTP (802.1s) – Supports multiple STP instances.  
 PVST+ (Cisco) – Separate STP instance per VLAN.  
 Rapid PVST+ – Faster Cisco version of PVST+.

### Spanning Tree Algorithm (STA) – Key Steps

Elect Root Bridge – Switch with the lowest Bridge ID is selected.  
 Select Root Ports – Best path to the Root Bridge on each switch.  
 Select Designated Ports – One per network segment to forward traffic.  
 Block Redundant Ports – Prevents loops but reactivates if needed.

### Spanning Tree Timers

Hello Time – BPDU messages interval (2 sec).  
 Forward Delay – Listening/Learning state duration (15 sec).  
 Max Age – Time before BPDU expires (20 sec).

1. **Example of Per VLAN spanning tree ?**

Cisco proprietary STP version that runs a separate STP instance per VLAN.  
 Allows load balancing by using different Root Bridges for different VLANs.  
 Works only on Cisco switches and uses ISL or 802.1Q trunking.

## Scenario:

We have two VLANs (VLAN 10 & VLAN 20) and two switches (SW1 & SW2).

* SW1 should be Root Bridge for VLAN 10
* SW2 should be Root Bridge for VLAN 20

### Step 1: Configure VLANs on Both Switches

Switch1(config)# vlan 10

Switch1(config-vlan)# name Sales

Switch1(config-vlan)# exit

Switch1(config)# vlan 20

Switch1(config-vlan)# name IT

Switch1(config-vlan)# exit

### Step 2: Set Root Bridge for VLANs

#### On Switch 1 (Root for VLAN 10)

Switch1(config)# spanning-tree vlan 10 root primary

Switch1(config)# spanning-tree vlan 20 root secondary

Switch1 becomes Root Bridge for VLAN 10.  
 Switch1 is secondary for VLAN 20 in case Switch2 fails.

#### On Switch 2 (Root for VLAN 20)

Switch2(config)# spanning-tree vlan 20 root primary

Switch2(config)# spanning-tree vlan 10 root secondary

Switch2 becomes Root Bridge for VLAN 20.  
 Switch2 is secondary for VLAN 10 in case Switch1 fails.

### Step 3: Verify PVST+ Configuration

Switch1# show spanning-tree vlan 10

Switch1# show spanning-tree vlan 20

1. **What is IPv6? Explain types and ip address range ?**

IPv6 (Internet Protocol version 6) is the latest version of the Internet Protocol, designed to replace IPv4 due to address exhaustion. It provides a 128-bit address space, improved security, and better network efficiency.

### Key Features of IPv6:

Larger Address Space – 128-bit addresses (≈340 undecillion addresses).  
 No NAT Required – Direct end-to-end communication.  
 Auto-configuration – Supports Stateless Address Autoconfiguration (SLAAC).  
 Built-in Security – IPSec is mandatory.  
 Better Multicasting & QoS – Supports flow labeling for traffic prioritization.

## Types of IPv6 Addresses

IPv6 addresses are categorized into three main types:

### 1. Unicast Addresses *(One-to-One Communication)*

Identifies a single device.  
 Used for point-to-point communication.  
 Types:

* Global Unicast (2000::/3) – Public, routable on the internet.
* Link-Local (FE80::/10) – Used within a local link, auto-assigned.
* Unique Local (FC00::/7) – Private, like IPv4’s 192.168.x.x.

### 2. Multicast Addresses *(One-to-Many Communication)*

Data is sent to multiple devices in a group.  
 Prefix: FF00::/8 (Examples: FF02::1 for all nodes, FF02::2 for all routers).

### 3. Anycast Addresses *(One-to-Nearest Communication)*

Assigned to multiple devices, but traffic is sent to the nearest one.  
 Used in CDNs (Content Delivery Networks) and Load Balancing.

## IPv6 Address Ranges & Examples

| IPv6 Address Type | Range (Prefix) | Example |
| --- | --- | --- |
| Global Unicast | 2000::/3 | 2001:db8::1 |
| Link-Local | FE80::/10 | FE80::1 |
| Unique Local | FC00::/7 | FD00::1 |
| Multicast | FF00::/8 | FF02::1 |
| Loopback | ::1 | ::1 |
| Unspecified | :: | :: |

Loopback (::1) – Similar to 127.0.0.1 in IPv4.  
 Unspecified (::) – Used when no valid address is assigned.

1. **Example of Ipv6 – RIP ?**

## Example: Configuring RIPng (RIP for IPv6) on Cisco Routers

RIPng (Routing Information Protocol Next Generation) is the IPv6 version of RIP. It is a distance-vector protocol that uses hop count (max 15 hops) as a metric.

Uses UDP port 521.  
 Supports IPv6 only (not compatible with IPv4 RIP).  
 Uses FF02::9 multicast address for updates.

## Scenario: IPv6 RIPng Configuration

We have two routers (R1 and R2) connected with an IPv6 network. We will configure RIPng to enable routing between networks.

### Network Details

| Router | Interface | IPv6 Address | Network |
| --- | --- | --- | --- |
| R1 | Gig0/0 | 2001:DB8:1::1/64 | 2001:DB8:1::/64 |
| R1 | Gig0/1 | 2001:DB8:2::1/64 | 2001:DB8:2::/64 |
| R2 | Gig0/0 | 2001:DB8:2::2/64 | 2001:DB8:2::/64 |
| R2 | Gig0/1 | 2001:DB8:3::1/64 | 2001:DB8:3::/64 |

### Step 1: Enable IPv6 Routing on Both Routers

R1(config)# ipv6 unicast-routing

R2(config)# ipv6 unicast-routing

### Step 2: Enable RIPng and Assign Interfaces

#### On Router R1:

R1(config)# ipv6 router rip MY-RIP

R1(config-rtr)# exit

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ipv6 address 2001:DB8:1::1/64

R1(config-if)# ipv6 rip MY-RIP enable

R1(config-if)# exit

R1(config)# interface gigabitEthernet 0/1

R1(config-if)# ipv6 address 2001:DB8:2::1/64

R1(config-if)# ipv6 rip MY-RIP enable

R1(config-if)# exit

#### On Router R2:

R2(config)# ipv6 router rip MY-RIP

R2(config-rtr)# exit

R2(config)# interface gigabitEthernet 0/0

R2(config-if)# ipv6 address 2001:DB8:2::2/64

R2(config-if)# ipv6 rip MY-RIP enable

R2(config-if)# exit

R2(config)# interface gigabitEthernet 0/1

R2(config-if)# ipv6 address 2001:DB8:3::1/64

R2(config-if)# ipv6 rip MY-RIP enable

R2(config-if)# exit

### Step 3: Verify RIPng Configuration

Check if RIPng is enabled and networks are being advertised:

R1# show ipv6 rip

R2# show ipv6 rip

Check the RIPng Routing Table:

R1# show ipv6 route rip

R2# show ipv6 route rip

Check RIPng Updates:

R1# debug ipv6 rip