**NETWORKING**

**Team:3**Team members :-

Repaka SomaSekhara Venkata Durga S Prakash(Lead)

23B21A4655  
V.Sai swetha

236Q1A4620

P.Pavan

23B21A4631

B.Yamani

23B21A4622

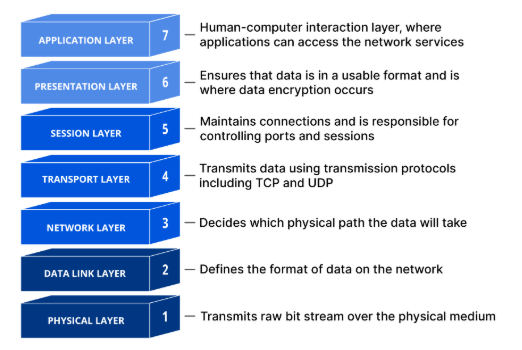
**Week -1**

**THEORETICAL LEARNING**

1. **What are OSI and TCP/IP architecture?**

**OSI Model(**Open systems interconnection**)**

* A **theoretical** model created by ISO (International Organization for Standardization) to standardize networking functions.
* The OSI model helps to understand how different networking components and protocols work together.
* It has 7 layers each layer has its own specific purpose and communicates with the layers directly above and below it.



| **Layer** | **Name** | **Key Function** | **Data Unit** | **Examples of protocols and devices** |
| --- | --- | --- | --- | --- |
| 7 | Application | Network services for user applications | Data | HTTP, FTP, SMTP, DNS |
| 6 | Presentation | Data format, encryption, compression | Data | SSL, JPEG, ASCII, MPEG |
| 5 | Session | Session control between apps | Data | NetBIOS, RPC |
| 4 | Transport | Reliable data delivery (TCP/UDP) | Segments | TCP (reliable), UDP (fast, no reliability |
| 3 | Network | Logical addressing, routing | Packets | IP, ICMP, IGMP, routers |
| 2 | Data Link | MAC addressing, error detection | Frames | Ethernet, ARP, switches |
| 1 | Physical | Physical transmission of bits | Bits | Cables, Hubs, NICs |

## **OSI Model: 7 Layers Explained**

### **1. Physical Layer**

* **Function**: Transmits raw **bits (0s and 1s)** over a physical medium.
* Deals with: Hardware, cables, connectors, voltages, signals.
* **Examples**: Ethernet cables, fiber optics, hubs, radio signals.
* **Data unit**: **Bits**

**2. Data Link Layer**

* **Function**: Ensures **error-free** transmission between two directly connected devices.
* Adds **MAC addresses**, handles **frames**, detects/corrects errors.
* **Examples**: Ethernet, Wi-Fi (IEEE 802.11), ARP, switches.
* **Data unit**: **Frames**

**3. Network Layer**

* **Function**: Handles **routing** and **logical addressing** (IP).
* Finds the best path to send data across networks.
* **Examples**: IP, ICMP, routers.
* **Data unit**: **Packets**

**4. Transport Layer**

* **Function**: Provides **reliable (TCP)** or **unreliable (UDP)** delivery of data.
* Manages flow control, error checking, segmentation, and reassembly.
* **Examples**: TCP, UDP, port numbers.
* **Data unit**: **Segments** (TCP) / **Datagrams** (UDP)

**5. Session Layer**

* **Function**: Manages and controls **connections (sessions)** between applications.
* Opens, uses, and closes sessions; maintains dialogs.
* **Examples**: NetBIOS, RPC, PPTP.
* **Data unit**: **Data**

**6. Presentation Layer**

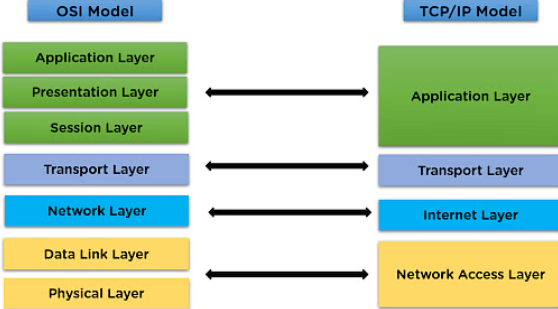
* **Function**: Translates data between application and network.
* Handles **data format conversion**, **encryption/decryption**, and **compression**.
* **Examples**: SSL/TLS, JPEG, ASCII, MPEG.
* **Data unit**: **Data**

**7. Application Layer**

* **Function**: Closest to the user. Provides **network services** to applications.
* Where users interact with networked apps (e.g., browser, email).
* **Examples**: HTTP, FTP, SMTP, DNS, Telnet.
* **Data unit**: **Data**

**TCP/IP architecture(**Transmission Control Protocol/Internet Protocol**)**

* A **practical** and widely used model that forms the basis of the internet.
* TCP/IP is the model actually used in real networks like the Internet. It's simpler and based on protocols developed for real implementation.
* It has 4 layers which combines some OSI layers into broader groups.



| **TCP/IP Layer** | **Main Functions** | **Examples** | **OSI Equivalent** |
| --- | --- | --- | --- |
| Application | User-level services and communication | HTTP, FTP, SMTP, DNS | OSI Layers 7, 6, 5 |
| Transport | Reliable or fast data transmission | TCP, UDP | OSI Layer 4 |
| Internet | Logical addressing, routing | IP, ICMP | OSI Layer 3 |
| Network Access (Link) | Physical transmission, MAC addressing | Ethernet, ARP, Wi-Fi | OSI Layers 2 and 1 |

### **Network Access Layer** (also called Link Layer or Data Link + Physical)

### **Function**: Responsible for how data is physically sent through the network.

### Deals with **hardware**, **MAC addresses**, and **local delivery**.

### It includes both the OSI **Data Link Layer** and **Physical Layer**.

### **Examples**: Ethernet, Wi-Fi (IEEE 802.11), ARP, Frame Relay, switches, NICs

### **Data unit**: **Frames** and **Bits**

**2. Internet Layer**

* **Function**: Handles **logical addressing and routing** of packets.
* Ensures the data gets from source to destination across multiple networks.
* Adds **IP addresses** and routes packets using routers.
* **Examples**: IP (IPv4/IPv6), ICMP (ping), IGMP
* **Data unit**: **Packets**

**3.Transport Layer**

* **Function**: Provides **end-to-end communication** between applications.
* Ensures **reliable delivery** (TCP) or **fast, connectionless delivery** (UDP).
* Handles segmentation, flow control, and error checking.
* **Examples**: **TCP**, **UDP**, port numbers (e.g., port 80 for HTTP)
* **Data unit**: **Segments** (TCP) or **Datagrams** (UDP)

1. **Application Layer**

* **Function**: Provides **network services to users and applications**.
* This is where apps like browsers, email, and file transfer programs operate.
* Includes the OSI **Application**, **Presentation**, and **Session** layers.
* **Examples**: HTTP (web), FTP (file transfer), DNS (domain names), SMTP (email), Telnet
* **Data unit**: **Data**

1. **Working of Network Devices.**

**1. Hub**

### **Definition**:

A hub is a basic networking device that connects multiple computers or other network devices in a LAN.

### **Working**:

* A hub operates at **Layer 1 (Physical Layer)** of the OSI model.
* When it receives a signal from one of its ports, it **copies and broadcasts** the signal to **all other ports**.
* The receiving devices check if the data is meant for them by inspecting the destination MAC address.
* It **does not filter traffic** or know the destination of the data.

### **Types**:

* Active Hub (amplifies signal)
* Passive Hub (just distributes signal)

### **Disadvantage**:

* Causes **network congestion** due to broadcasting.
* No intelligence; cannot reduce collisions.

**2. Switch**

### **Definition**:

A switch is a smart device used in LANs to connect devices and forward data based on MAC addresses.

### **Working**:

* Operates at **Layer 2 (Data Link Layer)**.
* Maintains a **MAC address table** (switching table).
* When it receives a frame:
* It **reads the MAC address** of the sender and adds it to the table.
* It **checks the destination MAC address**.
* It forwards the frame **only to the intended port**, reducing traffic.

### **Advanced Feature**:

Some switches operate at Layer 3 (Layer 3 Switches) and perform routing functions.

### **Advantage**:

* Reduces unnecessary traffic.
* **Supports full duplex communication**.

**3. Router**

### **Definition**:

A router is a device that connects **multiple networks** together and routes data between them using IP addresses.

### **Working**:

* Operates at **Layer 3 (Network Layer)**.
* Maintains a **routing table**.
* When it receives a packet:
* It reads the **destination IP address**.
* It checks the routing table for the **best path**.
* Forwards the packet to the next hop or destination.
* Can perform **NAT (Network Address Translation)** to allow private IPs to access the internet.

### **Advantage**:

* **Connects different networks** (e.g., LAN to WAN).
* Provides **security features** (firewall, packet filtering).

**4. Modem (Modulator-Demodulator)**

### **Definition**:

A modem connects your **local network** to the **Internet** using an ISP’s infrastructure.

### **Working**:

* Converts **digital signals** from a computer to **analog signals** (modulation) for transmission over telephone or coaxial cables.
* On the receiving end, it **converts analog signals back** to digital (demodulation).
* Typically used in **DSL, cable, or fiber** internet connections.

### **Types**:

* DSL Modem
* Cable Modem
* Fiber Modem

**5. Access Point (AP)**

### **Definition**:

An access point allows **wireless devices** to connect to a **wired network**.

### **Working**:

* Operates at **Layer 2**.
* Acts like a **hub or switch** for Wi-Fi devices.
* Converts **wired Ethernet signals** to **wireless radio signals** and vice versa.
* Uses **Wi-Fi protocols** (like 802.11) for communication.

### **Advantage**:

* Provides wireless connectivity in large areas.
* Can extend the wireless range.

**6. Repeater**

### **Definition**:

A repeater is used to **amplify or regenerate** signals to extend the range of a network.

### **Working**:

* Operates at **Layer 1**.
* Takes the **weak or distorted signal**, cleans it, **amplifies it**, and sends it onward.
* Does **not filter** or interpret data.

### **Use Case**:

Used in long-distance LANs or Wi-Fi range extensions.

**7. Bridge**

### **Definition**:

A bridge connects **two or more network segments**, making them function as a single network.

### **Working**:

* Operates at **Layer 2**.
* Maintains a MAC address table.
* **Learns** which devices are on which side of the bridge.
* Forwards data **only if needed** between segments to reduce traffic.

**Use Case**:

Useful in managing **network traffic** and **segmentation**.

**8. Gateway**

### **Definition**:

A gateway connects **networks that use different protocols**.

### **Working**:

* Operates at **all OSI layers**, depending on its function.
* Translates data formats and protocols between networks (e.g., from TCP/IP to AppleTalk).
* Often acts as a **protocol converter**.

### **Use Case**:

Used to connect **different architectures** or **communication systems**.

**9. Network Interface Card (NIC)**

### **Definition**:

A hardware component that allows a device to connect to a network.

### **Working**:

* Can be wired (Ethernet) or wireless (Wi-Fi).
* Operates at **Layer 2**.
* Has a unique **MAC address**.
* Converts data into **electrical or radio signals** for transmission.

**10. Firewall (Hardware-based)**

### **Definition**:

A device that **monitors and controls** incoming and outgoing network traffic based on security rules.

### **Working**:

* Can operate at **Layer 3 to Layer 7**.
* Inspects **packets** or **data streams**.
* Blocks or allows traffic based on **predefined rules**.

## **11. Brouter (Bridge + Router)**

### **Definition**:

A **hybrid device** that functions both as a bridge and a router.

### **Working**:

* **Bridges traffic** for non-routable protocols (e.g., NetBEUI).
* **Routes traffic** for routable protocols (e.g., IP).
* Combines the **filtering ability of a bridge** and the **routing capabilities of a router**.

**12. CSU/DSU (Channel Service Unit/Data Service Unit)**

### **Definition**:

Used to connect digital lines (like T1 or T3) to routers or LANs.

### **Working**:

* **CSU** provides **line conditioning and error correction**.
* **DSU** handles **data formatting** and controls the flow of data.
* Together, they ensure **compatibility** between a leased digital line and your internal network.

**13. Load Balancer**

### **Definition**:

Distributes **network or application traffic** across multiple servers or connections.

### **Working**:

* Operates at **Layer 4 (Transport)** or **Layer 7 (Application)**.
* Uses algorithms (Round Robin, Least Connections, etc.) to **distribute load**.
* Ensures **high availability, fault tolerance, and optimized performance**.

**14. Wireless Range Extender (Wi-Fi Extender)**

### **Definition**:

A device that repeats wireless signals to **extend the coverage area** of a Wi-Fi network.

### **Working**:

* Connects to an existing wireless network.
* **Receives the Wi-Fi signal**, amplifies it, and rebroadcasts it.
* Works similarly to a **repeater**, but specifically for Wi-Fi.

**15. Proxy Server (Hardware Appliance)**

### **Definition**:

Acts as an **intermediary** between client and server, often in hardware form for larger networks.

### **Working**:

* **Caches content**, filters traffic, and hides client IP addresses.
* Can monitor, control, or log user activity.
* Useful for **security, anonymity, and performance optimization**.

**16. VPN Concentrator**

### **Definition**:

A dedicated hardware device for handling **VPN (Virtual Private Network)** connections.

### **Working**:

* Manages **multiple encrypted tunnels** between remote users and the main network.
* Authenticates users and **encrypts/decrypts** traffic.
* Used in **enterprise networks** for secure remote access.

**17. Antenna (Used with APs and Routers)**

### **Definition**:

Not a networking device by itself but a **component** that transmits/receives wireless signals.

### **Types**:

* **Omnidirectional** – Broadcasts in all directions.
* **Directional** – Focuses signal in a specific direction for long-range communication.

**18. Media Converter**

### **Definition**:

A device that converts one **media type** to another (e.g., copper to fiber).

### **Working**:

Converts **electrical signals to light signals** and vice versa.

* Useful when integrating **fiber optics** into an Ethernet network.

1. **study about the protocols (like DHCP, ARP, FTP, SSH,HTTP, DNS etc…)**

### **1. Application Layer Protocols (OSI Layer 7)**

| **Protocol** | **Port Number(s)** | **Purpose** |
| --- | --- | --- |
| **HTTP** | 80 (TCP) | Web page requests/responses |
| **HTTPS** | 443 (TCP) | Secure web communication using SSL/TLS |
| **FTP** | 21 (TCP) | File transfer |
| **SFTP** | 22 (TCP) | Secure file transfer over SSH |
| **FTPS** | 990 (TCP) | FTP over SSL/TLS |
| **SMTP** | 25, 587 (TCP) | Sending email |
| **POP3** | 110 (TCP) | Downloads emails to client |
| **IMAP** | 143, 993 (TCP) | Manages emails on server |
| **DNS** | 53 (UDP/TCP) | Resolves domain names to IP addresses |
| **DHCP** | 67 (UDP server), 68 (UDP client) | Dynamically assigns IP addresses |
| **SNMP** | 161 (UDP), 162 (UDP) | Network monitoring and management |
| **Telnet** | 23 (TCP) | Remote terminal access (insecure) |
| **SSH** | 22 (TCP) | Secure remote login and file transfer |
| **NTP** | 123 (UDP) | Network time synchronization |
| **LDAP** | 389 (TCP), 636 (TCP) | Directory services / Authentication |
| **RDP** | 3389 (TCP/UDP) | Remote desktop GUI access |
| **SIP** | 5060, 5061 (TCP/UDP) | VoIP call setup and signaling |
| **TFTP** | 69 (UDP) | Lightweight file transfer |
| **Syslog** | 514 (UDP) | Logs system messages from network devices |
| **SMB** | 445 (TCP) | File/printer sharing in Windows |
| **NetBIOS** | 137-139 (UDP/TCP) | Legacy Windows networking |
| **RTP** | 5004, 5005 (UDP) | Real-time media transmission (VoIP) |
| **H.323** | 1720 (TCP) | Voice/video calls in VoIP |

### **2. Transport Layer Protocols (OSI Layer 4)**

| **Protocol** | **Port Number** | **Purpose** |
| --- | --- | --- |
| **TCP** | N/A | Reliable, connection-oriented communication |
| **UDP** | N/A | Unreliable, connectionless communication |
| **SCTP** | 9899 | Stream control, multi-homing and multi-streaming |

### **3. Network Layer Protocols (OSI Layer 3)**

| **Protocol** | **Port Number** | **Purpose** |
| --- | --- | --- |
| **IPv4/IPv6** | N/A | Core protocols for addressing and routing |
| **ICMP** | N/A | Diagnostic and control (e.g., ping, traceroute) |
| **IGMP** | N/A | Multicast group membership management |
| **IPSec** | Various | Secures IP packets with encryption/authentication |
| **NAT** | N/A | Translates private IPs to public IPs |

### **4. Data Link Layer Protocols (OSI Layer 2)**

| **Protocol** | **Port Number** | **Purpose** |
| --- | --- | --- |
| **ARP** | N/A | Resolves IP address to MAC address |
| **PPP** | N/A | Encapsulation for direct connections |
| **L2TP** | 1701 (UDP) | Tunneling protocol at Layer 2 |
| **STP/RSTP** | N/A | Prevents loops in Ethernet networks |
| **MAC** | N/A | Media access control in Ethernet |
| **802.1Q** | N/A | VLAN tagging for Ethernet frames |

### 🟥 **5. Routing & Other Key Protocols**

| **Protocol** | **Port Number** | **Purpose** |
| --- | --- | --- |
| **BGP** | 179 (TCP) | Inter-domain routing (between ISPs) |
| **OSPF** | 89 (IP) | Interior routing based on link-state algorithm |
| **RIP** | 520 (UDP) | Interior routing using distance vector algorithm |
| **EIGRP** | 88 (IP) | Cisco proprietary routing protocol |
| **MPLS** | N/A | High-speed forwarding using labels |
| **GRE** | 47 (IP Proto) | Tunnels packets over other protocols |
| **TLS/SSL** | 443 (TCP) | Encryption for HTTPS and other secure protocols |

## Key Categories of Protocols

| **Category** | **Example Protocols** |
| --- | --- |
| **Web** | HTTP, HTTPS |
| **Email** | SMTP, IMAP, POP3 |
| **File Transfer** | FTP, SFTP, TFTP, SMB |
| **Network Management** | SNMP, Syslog |
| **Remote Access** | SSH, Telnet, RDP |
| **Routing** | RIP, OSPF, BGP, EIGRP |
| **Name Resolution** | DNS, NetBIOS |
| **Time Sync** | NTP |
| **Security** | IPSec, SSL/TLS |
| **VoIP** | SIP, RTP, H.323 |

1. **What is Internet Protocol(IPV4) and (IPV6)**

### **Internet Protocol (IP)**

The **Internet Protocol (IP)** is a fundamental protocol in the **network layer (Layer 3)** of the **OSI** and **TCP/IP** models. It is responsible for **addressing and routing** packets of data so they can travel across networks and arrive at the correct destination. IP is connectionless and provides **best-effort delivery**, meaning it does not guarantee delivery, order, or error-free communication.

There are **two versions** of IP currently in use:

**1. IPv4 (Internet Protocol Version 4)**

### **Definition**:

IPv4 is the **4th version of the Internet Protocol**, developed in the early 1980s. It is the most widely used version and forms the foundation of most of the internet today.

**Key Features**:

| **Feature** | **Description** |
| --- | --- |
| **Address Size** | 32-bit address |
| **Address Format** | Decimal (e.g., 192.168.0.1) |
| **Address Space** | ~4.3 billion (2³²) addresses |
| **Header Size** | 20 bytes (minimum), up to 60 bytes |
| **Packet Fragmentation** | Supported |
| **Configuration** | Manual or via DHCP |
| **Security** | Optional (can use IPsec) |
| **Broadcast** | Supported |

**IPv4 Address Example**:

CopyEdit

192.168.1.1

Divided into **4 octets**, each ranging from **0–255**, separated by dots.

### **Advantages**:

Simpler and easier to configure.

Widely supported by all systems and devices.

Efficient for small networks.

### **Disadvantages**:

**Limited address space** (exhaustion of addresses).

**No built-in encryption or authentication**.

**Manual configuration** can be cumbersome for large networks.

## **2. IPv6 (Internet Protocol Version 6)**

### **Definition**:

IPv6 is the **successor to IPv4**, designed to solve its limitations, especially the **limited address space**.

It was developed by the IETF and officially published in **1998**.

### **Key Features**:

| **Feature** | **Description** |
| --- | --- |
| **Address Size** | 128-bit address |
| **Address Format** | Hexadecimal (e.g., 2001:0db8:85a3::8a2e:0370:7334) |
| **Address Space** | ~3.4×10³⁸ addresses |
| **Header Size** | 40 bytes (fixed) |
| **Packet Fragmentation** | Handled by the sender, not routers |
| **Configuration** | Auto-config via SLAAC or DHCPv6 |
| **Security** | Mandatory support for IPsec |
| **Broadcast** | Not supported (uses multicast/anycast instead) |

### **IPv6 Address Example**:

Makefile

CopyEdit

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Can be compressed as:

Ruby

CopyEdit

2001:db8:85a3::8a2e:370:7334

### **Advantages**:

**Vast address space** – enough for every device on Earth and more.

**Better security** – IPsec is required.

**Simplified header** – more efficient processing.

**No need for NAT** – each device can have a unique global IP.

**Auto-configuration** – easier management.

### **Disadvantages**:

Not all systems or applications fully support IPv6.

Requires updates to existing infrastructure.

Complexity in transition from IPv4 (dual stack, tunneling).

## **IPv4 vs IPv6 Summary Table**

| **Feature** | **IPv4** | **IPv6** |
| --- | --- | --- |
| Address Length | 32 bits | 128 bits |
| Address Format | Decimal (e.g., 192.168.1.1) | Hexadecimal (e.g., 2001:db8::1) |
| Address Space | ~4.3 billion | ~340 undecillion |
| Header Size | 20–60 bytes | 40 bytes (fixed) |
| Configuration | Manual/DHCP | SLAAC/DHCPv6 |
| Security | Optional | Mandatory IPsec support |
| NAT Required | Yes (due to shortage) | No |
| Broadcast | Yes | No (uses multicast/anycast) |

1. **Study in details about the subnetting.**

## 1. **What is Subnetting?**

**Subnetting** is the process of splitting a single IP network (or IP address block) into multiple smaller networks (subnets). This allows better utilization of IP addresses and improves network performance and security.

## 2. **Why Subnetting is Needed**

| **Reason** | **Description** |
| --- | --- |
| **Efficient IP Address Utilization** | Prevents IP wastage by allocating addresses only as needed |
| **Improved Security** | Restricts broadcast domains, limiting exposure to attacks |
| **Better Performance** | Reduces network congestion by decreasing broadcast traffic |
| **Simplified Management** | Easier to isolate and troubleshoot network segments |
| **Routing Efficiency** | Enables hierarchical addressing and route summarization |

## 3. **Basic Terminologies**

| **Term** | **Description** |
| --- | --- |
| **IP Address** | A 32-bit (IPv4) or 128-bit (IPv6) address used to identify a device on a network |
| **Subnet Mask** | A 32-bit number that divides an IP address into network and host portions |
| **Network Address** | First address in a subnet; identifies the subnet itself |
| **Broadcast Address** | Last address in a subnet; used to send data to all hosts in that subnet |
| **Host Address** | Usable addresses between the network and broadcast address |
| **CIDR Notation** | Compact form to represent subnet mask using a slash (e.g., /24) |

## 4. **Subnet Mask and CIDR Notation**

A **Subnet Mask** separates the **network** part from the **host** part of the IP address.

| **CIDR** | **Subnet Mask** | **Number of Hosts** |
| --- | --- | --- |
| /8 | 255.0.0.0 | 16,777,214 |
| /16 | 255.255.0.0 | 65,534 |
| /24 | 255.255.255.0 | 254 |
| /30 | 255.255.255.252 | 2 |

Formula to calculate number of hosts per subnet:

\text{Number of Hosts} = 2^{(32 - \text{CIDR})} - 2  
]

## 5. **How Subnetting Works**

### Step-by-step Subnetting Process:

**Example**: Subnet 192.168.1.0/24 into 4 subnets.

**Determine Subnet Bits**:  
We need 4 subnets → 22=42^2 = 422=4 → use 2 bits from host part.

**New Subnet Mask**:  
/24 + 2 = /26 → 255.255.255.192

**Subnet Ranges**:

| **Subnet** | **Range** | **Broadcast** | **Usable Hosts** |
| --- | --- | --- | --- |
| 0 | 192.168.1.0 – 192.168.1.63 | 192.168.1.63 | 192.168.1.1 – 192.168.1.62 |
| 1 | 192.168.1.64 – 192.168.1.127 | 192.168.1.127 | 192.168.1.65 – 192.168.1.126 |
| 2 | 192.168.1.128 – 192.168.1.191 | 192.168.1.191 | 192.168.1.129 – 192.168.1.190 |
| 3 | 192.168.1.192 – 192.168.1.255 | 192.168.1.255 | 192.168.1.193 – 192.168.1.254 |

## 6. **Subnetting Formulas**

| **Purpose** | **Formula** |
| --- | --- |
| Number of Subnets | 2n2^n2n, where n = number of borrowed bits |
| Number of Hosts | 2h−22^h - 22h−2, where h = number of host bits left |
| New Subnet Mask | Add borrowed bits to the default mask |
| Block Size | 256−Subnet Mask Value of Block Octet256 - \text{Subnet Mask Value of Block Octet}256−Subnet Mask Value of Block Octet |

## 7. **Types of Subnetting**

### 1. **Fixed-Length Subnet Masking (FLSM)**

All subnets are of equal size.

Easier to implement.

Wastes IPs if subnets require different sizes.

### 2. **Variable-Length Subnet Masking (VLSM)**

Subnets can be of different sizes.

More efficient IP utilization.

Slightly complex to plan and manage.

## 8. **Subnetting Example**

### Example: Subnet a Class B network 172.16.0.0/16 to have 1000 subnets.

Need 1000 subnets → 210=10242^{10} = 1024210=1024 → 10 bits

New Subnet Mask = /16 + 10 = /26 → 255.255.255.192

Each subnet will have:

26−2=622^6 - 2 = 6226−2=62 usable hosts

## 9. **Subnetting in IPv6 (Brief)**

IPv6 uses **128-bit** addresses.

Subnetting is done using **CIDR** (e.g., /64 is standard).

Uses **hextet boundaries**, not dotted-decimal.

No need to subtract 2 for network/broadcast (they don’t exist in IPv6).

## 10. **Advantages and Disadvantages of Subnetting**

### ✅ Advantages:

Efficient IP address management

Reduced network congestion

Improved security and isolation

Simplified network administration

❌ Disadvantages:

Adds complexity to network design

Requires careful planning and documentation

Can lead to routing table growth

11. **Applications of Subnetting**

Large corporate networks

ISPs and data centers

Universities and campuses

Cloud infrastructure (AWS, Azure, GCP)

Network security zones (DMZ, internal, external

## 12. **Tools for Subnetting**

**Subnet calculators** (online or CLI tools)

**Cisco Packet Tracer** (for practice)

**Binary math** for manual subnetting

**IP planning software** (e.g., SolarWinds IPAM)

### 📝 Example Problem:

**"Subnet the network 192.168.10.0/24 to create 6 subnets. Provide the subnet mask, subnet ranges, and number of usable hosts per subnet."**

### ✅ **Step 1: Determine How Many Bits to Borrow**

You need **6 subnets**.

Find the smallest power of 2 ≥ 6:

23=8(3 bits needed)2^3 = 8 \quad (\text{3 bits needed})23=8(3 bits needed)

### ✅ **Step 2: Calculate the New Subnet Mask**

Original subnet mask: /24 → 255.255.255.0

Borrowed 3 bits → new mask: /24 + 3 = /27

**New subnet mask**:

Binary: 11111111.11111111.11111111.11100000

Decimal: 255.255.255.224

### ✅ **Step 3: Calculate Block Size**

Block size =

256−Last octet of subnet mask=256−224=32256 - \text{Last octet of subnet mask} = 256 - 224 = 32256−Last octet of subnet mask=256−224=32

### ✅ **Step 4: List All Subnets**

| **Subnet** | **Network Address** | **First Host** | **Last Host** | **Broadcast Address** |
| --- | --- | --- | --- | --- |
| 0 | 192.168.10.0 | 192.168.10.1 | 192.168.10.30 | 192.168.10.31 |
| 1 | 192.168.10.32 | 192.168.10.33 | 192.168.10.62 | 192.168.10.63 |
| 2 | 192.168.10.64 | 192.168.10.65 | 192.168.10.94 | 192.168.10.95 |
| 3 | 192.168.10.96 | 192.168.10.97 | 192.168.10.126 | 192.168.10.127 |
| 4 | 192.168.10.128 | 192.168.10.129 | 192.168.10.158 | 192.168.10.159 |
| 5 | 192.168.10.160 | 192.168.10.161 | 192.168.10.190 | 192.168.10.191 |
| (Optional) 6 | 192.168.10.192 | 192.168.10.193 | 192.168.10.222 | 192.168.10.223 |
| (Optional) 7 | 192.168.10.224 | 192.168.10.225 | 192.168.10.254 | 192.168.10.255 |

Each subnet has 25−2=302^5 - 2 = 3025−2=30 usable hosts.

1. **Distinguish between the routing protocols.**

**BASED ON ROUTING TYPE**

| **Type** | **Description** | **Example Protocols** |
| --- | --- | --- |
| **Static Routing** | Routes are manually configured by network admins. Not dynamic or automatic. | N/A (Manually configured) |
| **Dynamic Routing** | Routes are automatically adjusted based on network topology changes. | RIP, OSPF, EIGRP, BGP |

**BASED ON SCOPE**

| **Type** | **Description** | **Example Protocols** |
| --- | --- | --- |
| **Interior Gateway Protocol (IGP)** | Used for routing **within a single autonomous system (AS)**. | RIP, OSPF, EIGRP, IS-IS |
| **Exterior Gateway Protocol (EGP)** | Used for routing **between different autonomous systems**. | BGP |

**BY ROUTING ALGORITHM**

| **Type** | **Description** | **How it works** | **Examples** |
| --- | --- | --- | --- |
| **Distance Vector** | Shares entire routing tables periodically with direct neighbors | Uses Bellman-Ford algorithm | RIP, IGRP |
| **Link State** | Each router builds a full map of the network using LSAs | Uses Dijkstra’s SPF algorithm | OSPF, IS-IS |
| **Path Vector** | Routers maintain AS-level path information | Uses Path vector mechanism | BGP |
| **Hybrid** | Combines both Distance Vector and Link State | Efficient, loop-free convergence | EIGRP |

**MAJOR ROUTING PROTOCOLS**

### **RIP (Routing Information Protocol)**

| **Feature** | **Details** |
| --- | --- |
| **Type** | Distance Vector |
| **Metric** | Hop count (Max 15 hops) |
| **Algorithm** | Bellman-Ford |
| **Convergence** | Slow |
| **Updates** | Every 30 seconds |
| **Loop Prevention** | Split horizon, poison reverse |
| **Use Case** | Small networks |
| **Advantages** | Simple to configure, supported widely |
| **Disadvantages** | Limited scalability, slow convergence, max 15-hop limit |

### **OSPF (Open Shortest Path First)**

| **Feature** | **Details** |
| --- | --- |
| **Type** | Link State (IGP) |
| **Metric** | Cost (based on bandwidth) |
| **Algorithm** | Dijkstra’s SPF |
| **Updates** | Event-triggered (not periodic) |
| **Hierarchical Design** | Areas (Backbone Area 0, and others) |
| **Loop Prevention** | SPF ensures no loops |
| **Use Case** | Large enterprise networks |
| **Advantages** | Fast convergence, scalable, classless |
| **Disadvantages** | More complex to configure than RIP |

### **EIGRP (Enhanced Interior Gateway Routing Protocol)**

| **Feature** | **Details** |
| --- | --- |
| **Type** | Hybrid (Cisco proprietary, now open standard) |
| **Metric** | Bandwidth, delay, load, reliability |
| **Algorithm** | DUAL (Diffusing Update Algorithm) |
| **Updates** | Event-driven |
| **Loop Prevention** | Feasible successor concept |
| **Use Case** | Medium to large Cisco networks |
| **Advantages** | Fast convergence, flexible metrics |
| **Disadvantages** | Initially Cisco-only (vendor lock-in) |

### **IS-IS (Intermediate System to Intermediate System)**

| **Feature** | **Details** |
| --- | --- |
| **Type** | Link State |
| **Metric** | Cost |
| **Algorithm** | Dijkstra (SPF) |
| **Encapsulation** | Runs over Layer 2 (no IP needed) |
| **Use Case** | Service providers and academic networks |
| **Advantages** | Very scalable, fast, stable |
| **Disadvantages** | Complex configuration, less familiar than OSPF |

### **BGP (Border Gateway Protocol)**

| **Feature** | **Details** |
| --- | --- |
| **Type** | Path Vector (EGP) |
| **Metric** | AS-path, policy-based |
| **Algorithm** | Path Vector |
| **Update Trigger** | Event-based |
| **Loop Prevention** | AS-path attribute |
| **Use Case** | Internet routing between ASes |
| **Advantages** | Extremely scalable, policy-based routing |
| **Disadvantages** | Complex, slow convergence, requires deep expertise |

1. **Make a Brief notes on VLAN, Voice VLAN, Data VLAN**

### **1. VLAN (Virtual Local Area Network)**

**Definition**: VLAN is a logical subdivision of a physical network that groups devices into separate broadcast domains, regardless of physical location.

**Purpose**: To improve network efficiency, security, and manageability by isolating traffic.

**Key Features**:

Reduces broadcast traffic.

Enhances security by isolating sensitive data.

Simplifies network management.

**Types**:

**Static VLAN**: Ports are manually assigned to VLANs.

**Dynamic VLAN**: VLAN membership is assigned automatically using MAC addresses.

### **2. Data VLAN**

**Definition**: A VLAN dedicated to carrying **user-generated data** traffic such as emails, web browsing, and file transfers.

**Purpose**: To separate user data from other types of traffic (e.g., voice, management).

**Key Point**:

It is the most common type of VLAN.

Each department (HR, Finance, etc.) may have its own data VLAN.

### **3. Voice VLAN**

**Definition**: A specialized VLAN configured to carry **VoIP (Voice over IP)** traffic from IP phones.

**Purpose**: To ensure high-quality voice communication by prioritizing voice packets.

**Key Features**:

Supports QoS (Quality of Service) for low latency, jitter, and packet loss.

IP phones connect to a switch port that carries both voice and data using trunking.

**Configuration**:

A single switch port can be configured with both a **Voice VLAN** and a **Data VLAN**.

Voice VLAN typically has higher priority in QoS settings.  
  
  
  
 **Practical Learning  
  
Networking**

**Practical learning :**

1. Assigning IP addresses to the interfaces.
2. Making subnets in any type of IP classes
3. Configuration of routing protocols

     RIP

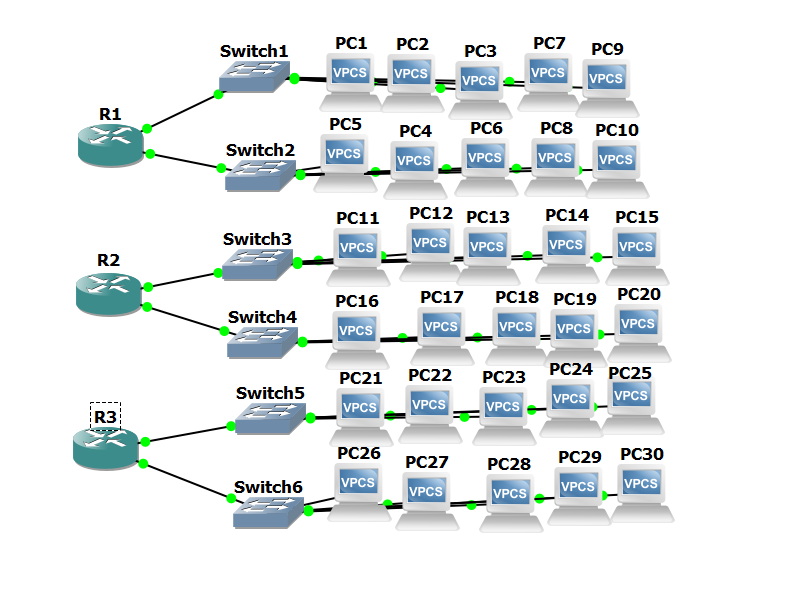
      OSPF

      EIGRP

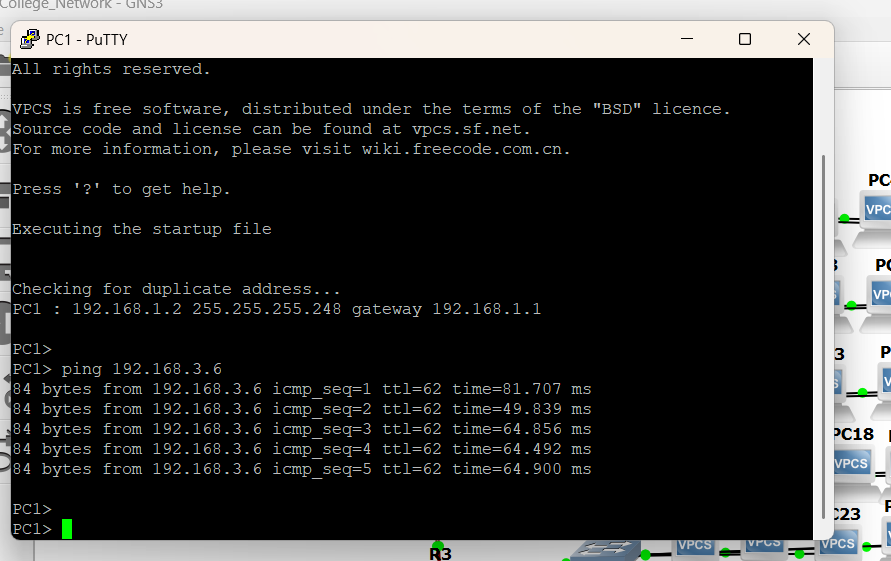
      BGP

1. Configuration of VLANS and its types

**Network Design:-**

****

**\* Assigning IP addresses to the interfaces :**



**➤ What it means:**

Assigning an IP address allows a device to communicate in a network. Each interface (like Ethernet0, FastEthernet1, etc.) in a router or switch needs a unique IP address.

➤ Steps:

**192.168.1.2** → IP address of the PC

**255.255.255.248**→ Subnet mask

**192.168.1.1** → Default gateway

=> **Verify the configuration:** show ( This is a command is used to verify the configuration and its gives the result either its configured or not **Similarly assigning of ip address was done to all the PCs**

**Configuration of Routers:**

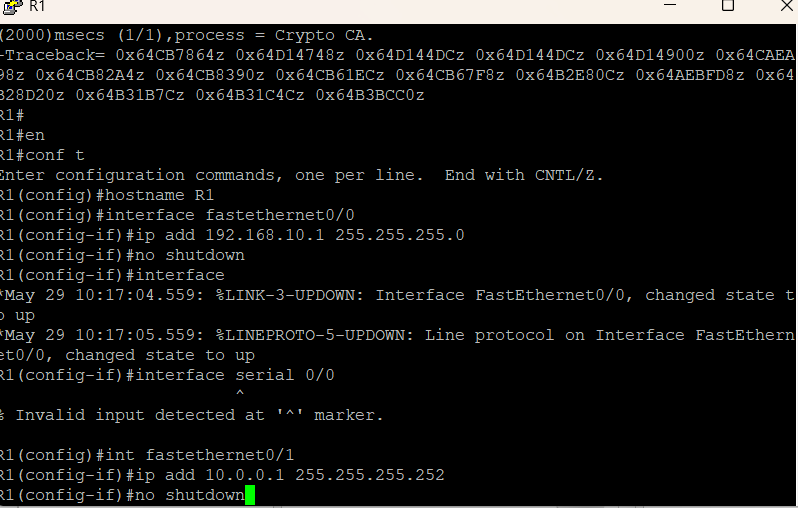
enable

configure terminal

interface fastEthernet0/0

ip address 192.168.1.1 255.255.255.0

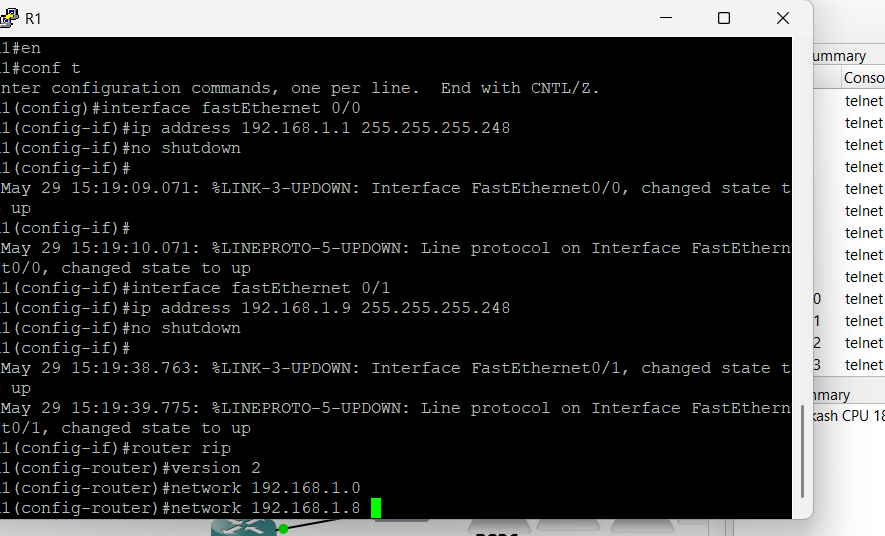
no shutdown



Similarly for R2 and R3

**RIP : (Routing Information Protocol )** :-

A distance-vector protocol that uses hop count as a metric.  
Slow convergence and supports up to 15 hops.  
Simple but outdated, mostly used for learning purposes.



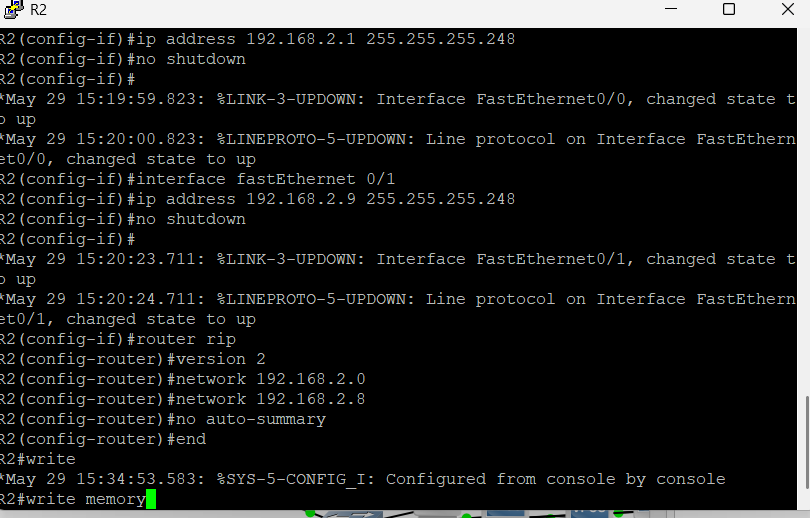
Steps:

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# network 192.168.1.0

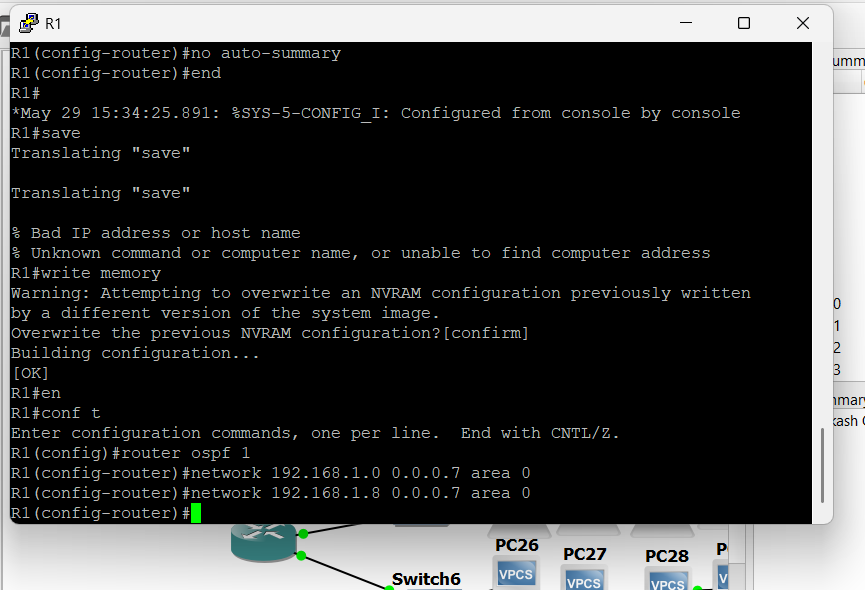
Router(config-router)# exit



Similarly for the router 3

➤OSPF (Open Shortest Path First) :-

A link-state protocol that uses cost based on bandwidth.  
It converges quickly and supports large, hierarchical networks.  
Open standard, widely used in enterprise networks.



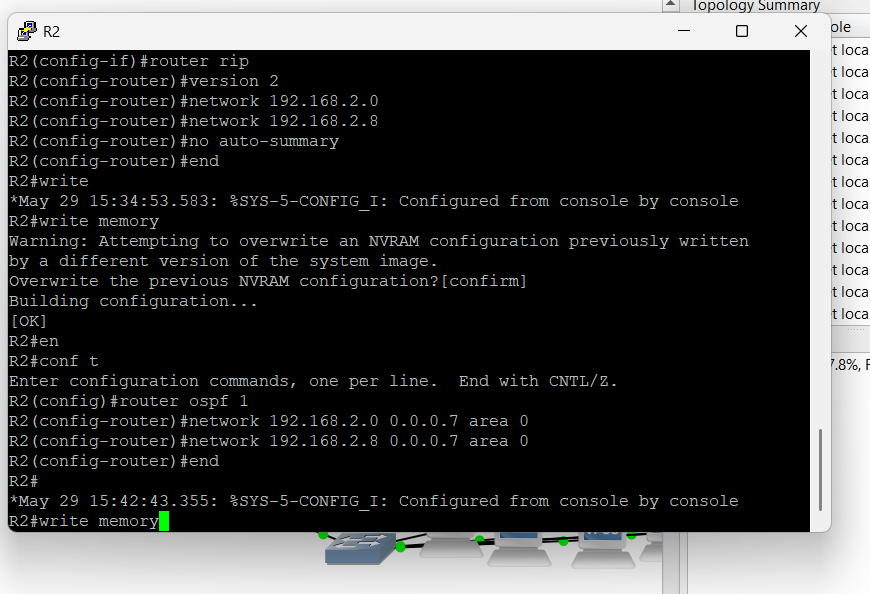
➤Steps :

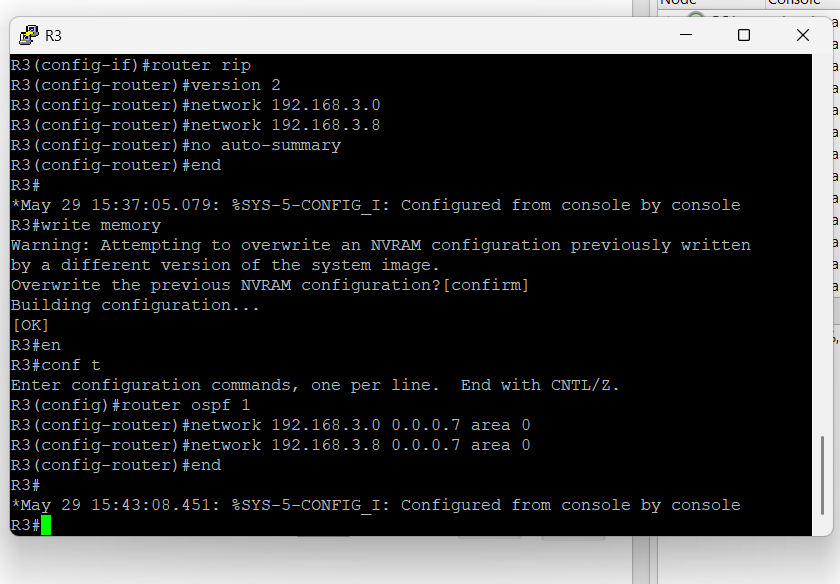
Router(config)# router eigrp 10

Router(config-router)# network 192.168.1.0

Router(config-router)# no auto-summary

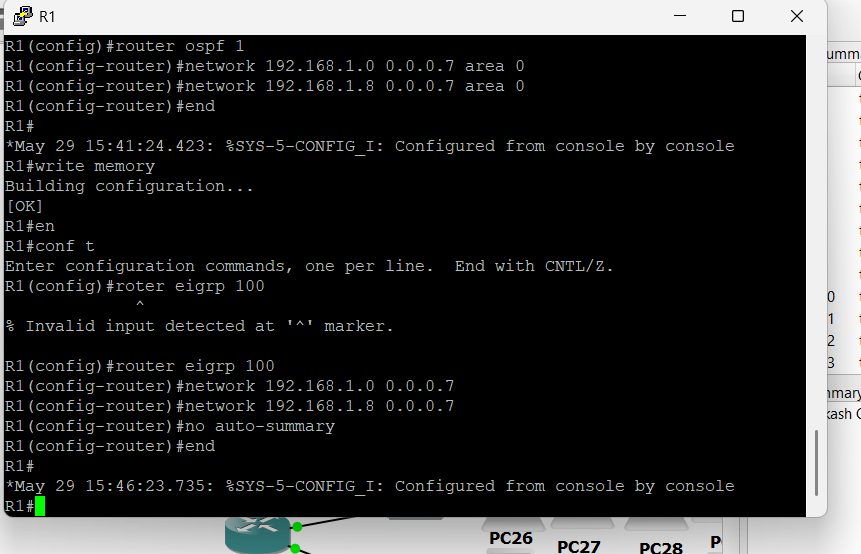
Router(config-router)# exit





**➤ EIGRP (Enhanced Interior Gateway Routing Protocol) :**

A Cisco proprietary hybrid protocol (distance vector + link state features).  
Fast convergence and efficient use of bandwidth.  
Supports VLSM, unequal-cost load balancing, and is scalable.



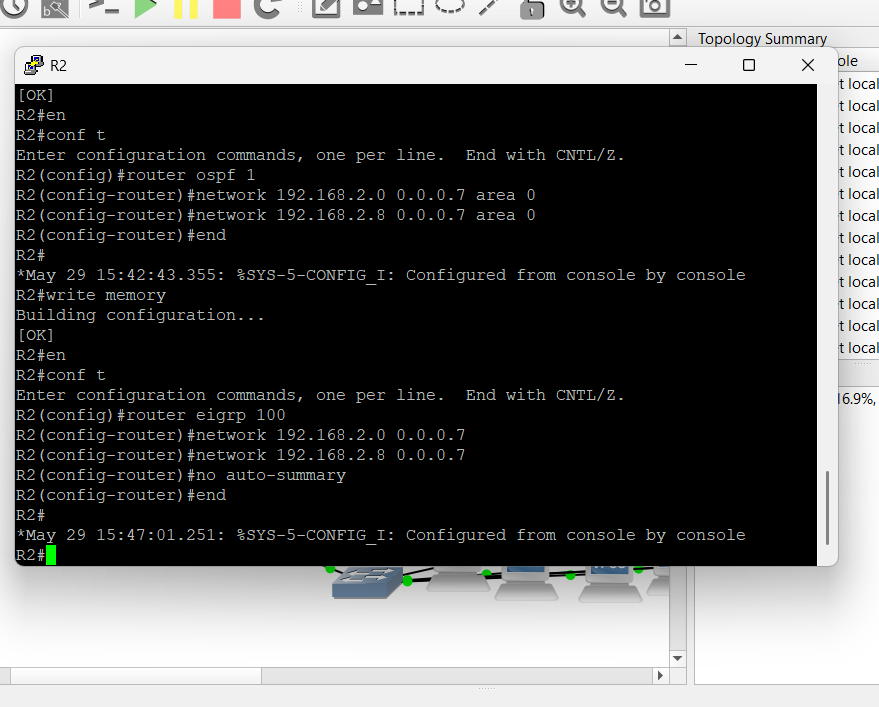
**➤Steps :**

Router(config)# router eigrp 10

Router(config-router)# network 192.168.1.0

Router(config-router)# no auto-summary

Router(config-router)# exit



**➤ BGP (Border Gateway Protocol) :**

A path-vector protocol used to route between autonomous systems (on the internet).  
Used by ISPs and large networks for global routing decisions.  
Scalable and policy-based, but complex to configure.

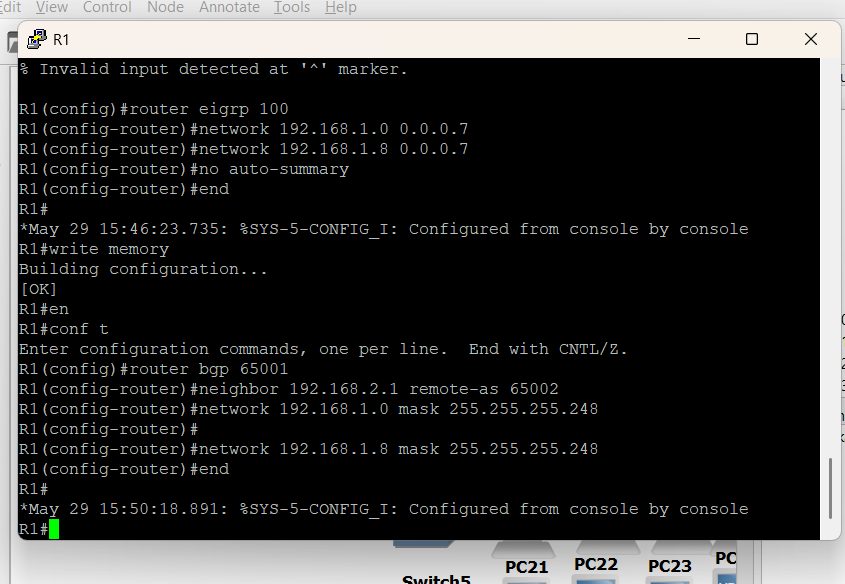
➤Steps:

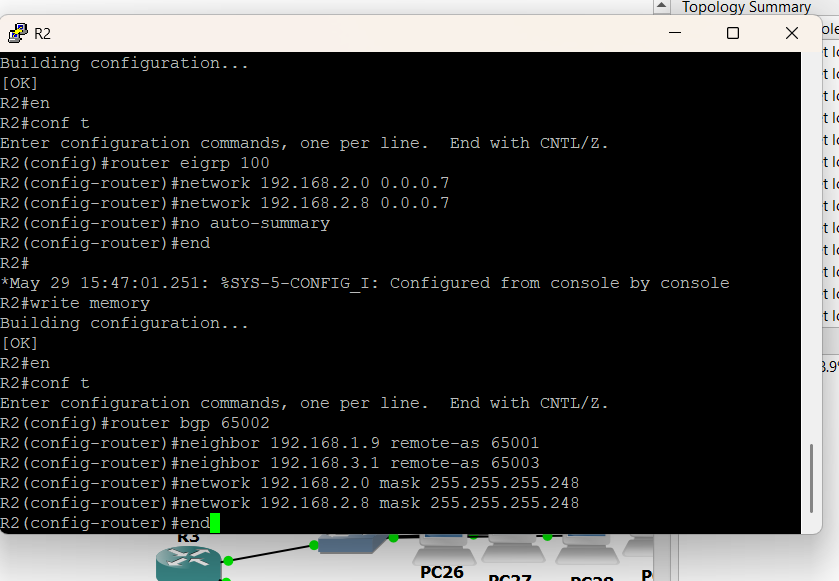
Router(config)# router bgp 65001

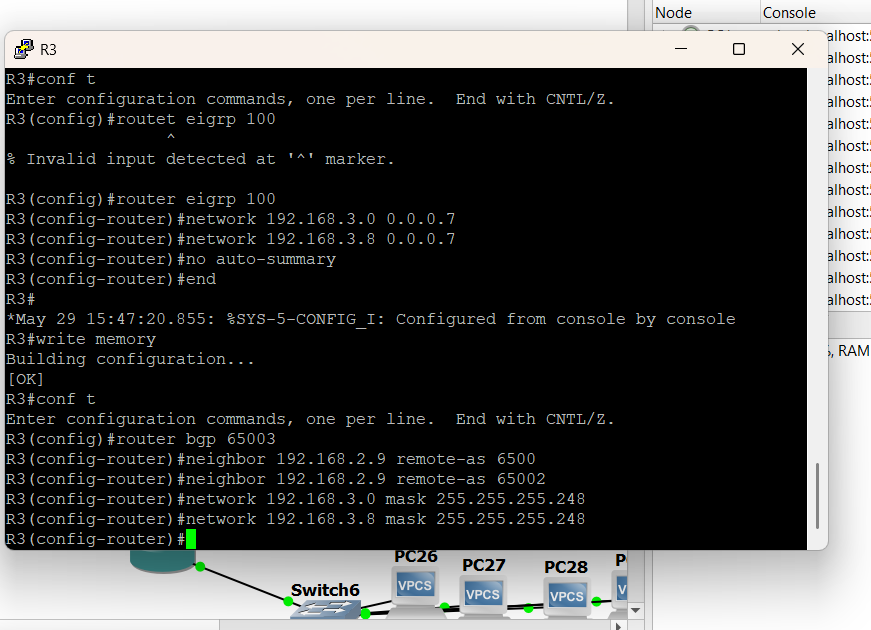
Router(config-router)# neighbor 10.0.0.2 remote-as 65002

Router(config-router)# network 192.168.1.0 mask 255.255.255.0

Router(config-router)# exit







**4. Configuration of VLANs and Its Types**

**➤ What is a VLAN?**

* **Virtual LAN** allows segmentation of a physical network into multiple logical networks.
* Devices in different VLANs can't communicate without a router or Layer 3 switch.

**➤ Types of VLANs:**

1. **Default VLAN (VLAN 1)** – All switch ports are in this by default.
2. **Data VLAN** – Carries user-generated traffic.
3. **Voice VLAN** – Used for VoIP traffic.
4. **Management VLAN** – Used to manage network devices.
5. **Native VLAN** – Used for untagged traffic on trunk ports.

**➤ Steps to Create and Assign VLAN:**

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# name Sales

Switch(config-vlan)# exit

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

**➤ To Configure Trunk Port (for multiple VLANs):**

=Switch(config)# interface fastEthernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk native vlan 1  
  
  
Note:- The above all the practical learnings are implemented in the GNS3 platform