**Unit-II**

**Medium Access Control and Network Layer 04 Hours**

**Medium Access Control:** Legacy Standard : 10 Mbps IEEE 802.3 Standard(Ethernet), High Speed Ethernet Standards: Fast, Gigabit and 10Gigabit.

**Wireless Standards:** IEEE 802.11a/b/g/n/ac, IEEE 802.15, IEEE 802.15.4 and IEEE 802.16 Standards, CSMA/CA

**Switching Techniques and IP Addressing**: Circuit, Message and Packet Switching.

**Logical Addressing:** IPv4 and IPv6 Network Layer Protocols: Internet Protocol(IP), Internet Control Message Protocol(ICMP)

1. **Medium Access Control (MAC) – Brief Notes**

**Medium Access Control (MAC)** is a sublayer of the Data Link Layer in the OSI model responsible for **coordinating how devices access a shared communication medium** in a network. It ensures orderly communication, efficient use of bandwidth, and avoidance of data collisions in both wired and wireless networks.

**1.1 Functions of MAC:**

* **Addressing:** Uses MAC addresses to uniquely identify devices.
* **Channel Access:** Determines when a device can transmit on the medium.
* **Frame Delimiting and Error Checking:** Helps in detecting and isolating errors in frames.
* **Collision Handling:** Manages collisions using techniques like **CSMA/CD** (in Ethernet) and **CSMA/CA** (in Wi-Fi).

**1.2 Types of Access Methods:**

* **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Used in legacy Ethernet; devices sense the medium and detect collisions.
* **CSMA/CA (Collision Avoidance):** Used in wireless networks like Wi-Fi to avoid collisions before they occur.
* **Token Passing:** Used in Token Ring networks; a token controls which device can transmit.

**1.3 Importance:**

* Enables multiple devices to share the same medium efficiently.
* Minimizes data collisions and transmission delays.
* Ensures fairness and reliability in data communication.

**2. CSMA/CD (Carrier Sense Multiple Access/ Collision Detection)**

* **CSMA/CD** is a **network protocol** used in **wired Ethernet networks (IEEE 802.3)** to control access to the shared communication medium and to handle **collisions** when two devices transmit simultaneously.
* CSMA/CD is a media access control method that was widely used in Early Ethernet technology/LANs when there used to be shared Bus Topology and each node ( Computers) was connected by Coaxial Cables. Nowadays Ethernet is Full Duplex and Topology is either Star (connected via Switch or Router) or point-to-point (Direct Connection). Hence CSMA/CD is not used but they are still supported though.
* Consider a scenario where there are 'n' stations on a link and all are waiting to transfer data through that channel. In this case, all 'n' stations would want to access the link/channel to transfer their own data. The problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.
* CSMA/CD is one such technique where different stations that follow this protocol agree on some terms and collision detection measures for effective transmission. This protocol decides which station will transmit when so that data reaches the destination without corruption.

**2.1 How Does CSMA/CD Work?**

* **Step 1:** Check if the sender is ready to transmit data packets.
* **Step 2:** Check if the transmission link is idle.

The sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. The sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

* **Step 3:** Transmit the data & check for collisions.

The sender transmits its data on the link. CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.

* **Step 4:** If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

**2.2 Advantages:**

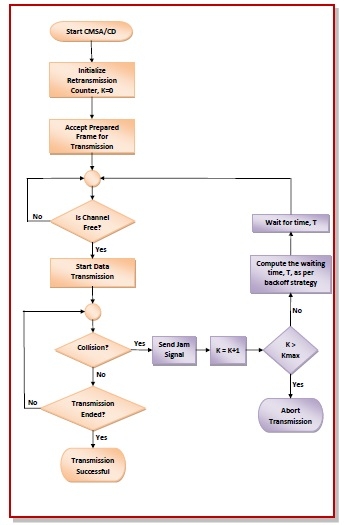
* Simple and decentralized.
* Efficient under **low traffic**.
* Reduces transmission errors through real-time collision monitoring.

**2.3 Limitations:**

* **Inefficient in high traffic**: Collision frequency increases.
* Only works in **half-duplex** Ethernet (not full-duplex).
* Not suitable for wireless (can’t detect collisions reliably).

**2.4 Applications:**

* Used in **legacy Ethernet** (10Base-5, 10Base-2, 10Base-T).
* **Replaced** in modern networks by **full-duplex switched Ethernet**, where CSMA/CD is no longer needed.



**3 CSMA/CA**

CSMA/CA is a network multiple access method used in wireless networks to avoid collisions before they happen, unlike CSMA/CD which detects collisions after they occur. CSMA/CA is used primarily in IEEE 802.11 (Wi-Fi) networks.

**3.1 Working Principle:**

1. **Carrier Sensing:**

A node listens to the medium (channel) to check if it is idle or busy.

1. **If Channel is Idle:**

* The node waits for a short time interval (Interframe Space, IFS).
* Then sends a **Request to Send (RTS)** packet to the receiver.

1. **If Receiver is Ready:**

* It responds with a **Clear to Send (CTS)** packet.
* The sender then sends the data.

1. **Collision Avoidance:**

* Nearby nodes that hear RTS or CTS defer their transmissions.
* This prevents hidden terminal problems.

**3.2 Key Components:**

* **RTS (Request to Send) :** Used by sender to reserve the channel.
* **CTS (Clear to Send) :**Sent by receiver to confirm readiness and instruct others to back off.
* **NAV (Network Allocation Vector):** A timer set by nodes overhearing RTS/CTS indicating how long the medium will be busy.

**3.3 Timing Intervals:**

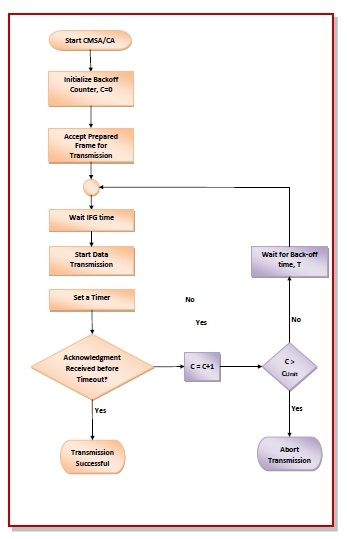
* **IFS (Inter Frame Space):**Time gap between data transmissions to prioritize access.
* **Backoff Time:** Randomized waiting time before retrying to send, reducing collision chances.

**3.4 Advantages:**

* Reduces chances of collision in wireless media.
* Prevents hidden and exposed terminal problems.
* Efficient in networks where nodes can't detect collisions.

**3.5 Limitations:**

* Increases latency due to RTS/CTS handshake.
* Overhead for small data packets.
* Not foolproof against all collisions (e.g., simultaneous RTS).



**4. IEEE 802.3**

The **IEEE 802.3** standard defines the specifications for **Ethernet**, a widely adopted technology for **Local Area Networks (LANs)**. The legacy version of this standard supports a **data rate of 10 Mbps** and uses a **shared medium** for communication based on **CSMA/CD** protocol.

**4.1 Key Features:**

* **Speed**: 10 Mbps (Megabits per second).
* **Access Method**: CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
* **Topology**: Bus or Star (with hubs).
* **Transmission Mediums**:
  + **10BASE5**: Thick coaxial cable.
  + **10BASE2**: Thin coaxial cable.
  + **10BASE-T**: Twisted-pair copper (Category 3 or 5).
  + **10BASE-F**: Optical fiber.

**4.2 Advantages:**

* **Simplicity**: Easy to implement and understand.
* **Cost-effective**: Uses inexpensive cabling.
* **Interoperability**: Standardized frame formats and MAC layer.
* **Widely Adopted**: Foundation for later Ethernet developments.

**4.3 Limitations:**

* **Low Speed**: Only 10 Mbps; insufficient for modern data needs.
* **High Collision Rate**: Shared medium causes performance degradation.
* **Half-Duplex**: Inefficient compared to full-duplex systems.
* **Distance Constraints**: Limited range without repeaters.

**4.4 Use Case (Historical):**

* Popular in **early LANs** during the 1980s and 1990s.
* Used in **office networks**, **university labs**, and **small businesses**.

**4.5** **10BASE-T Mean?**

* **10BASE-T** is an Ethernet standard defined under **IEEE 802.3**. It refers to:
* **10** → Maximum data rate of **10 Megabits per second (Mbps)**
* **BASE** → **Baseband** signaling (uses the entire bandwidth for a single signal)
* **T** → **Twisted Pair** cabling (usually unshielded twisted pair – UTP)
* **"Legacy"** refers to an **older standard, system, or technology** that is **still in use**, even though **newer and more advanced alternatives** are available.

**5. High Speed Ethernet Standards**

**5.1. Fast Ethernet (100 Mbps)**

* **Standard:** IEEE 802.3u
* **Speed:** 100 Megabits per second (Mbps)
* **Key Features:**
* 10x faster than traditional 10BASE-T
* Backward compatible with 10 Mbps Ethernet
* Uses **100BASE-TX**, **100BASE-FX**, etc.
* **Transmission Media:**
* **100BASE-TX**: Two pairs of Category 5 UTP cables (max 100 meters)
* **100BASE-FX**: Fiber optics for longer distances
* **Advantages:**
* Low-cost upgrade from 10BASE-T
* Simple implementation for LANs
* **Limitations:**
* Speed insufficient for modern applications like HD video, large datasets, etc.

**5.2. Gigabit Ethernet (1 Gbps)**

* **Standard:** IEEE 802.3ab (Copper), 802.3z (Fiber)
* **Speed:** 1 Gigabit per second (Gbps)
* **Key Features:**
* 10x faster than Fast Ethernet
* Can use **fiber** or **twisted-pair copper**
* Supports **1000BASE-T**, **1000BASE-SX**, **1000BASE-LX**, etc.
* **Transmission Media:**
* **1000BASE-T**: Uses all 4 pairs of Cat5e or higher cables (max 100 meters)
* **1000BASE-SX/LX**: Fiber optic for longer distances
* **Advantages:**
* Ideal for high-speed file transfer, video streaming, VoIP
* Compatible with existing copper networks using upgraded cables
* **Limitations:**
* Higher hardware costs than Fast Ethernet
* Susceptible to electromagnetic interference on long copper runs

**5.3. 10-Gigabit Ethernet (10 Gbps)**

* **Standard:** IEEE 802.3ae
* **Speed:** 10 Gigabits per second (Gbps)
* **Key Features:**
* 10x faster than Gigabit Ethernet
* Typically used in **data centers**, **enterprise backbones**, and **high-performance networks**
* Common types: **10GBASE-SR**, **10GBASE-LR**, **10GBASE-ER**, **10GBASE-T**
* **Transmission Media:**
* **10GBASE-T**: Cat6a/Cat7 copper cables (up to 100m)
* **10GBASE-SR/LR**: Fiber optic cables for medium to long distances
* **Advantages:**
* Extremely high bandwidth for virtualization, cloud computing, and big data
* Supports high-performance computing and storage networking
* **Limitations:**
* Expensive hardware (NICs, switches, cabling)
* Higher power consumption
* Not needed in typical home or small business networks

**5.4 Summary Comparison Table:**

| **Feature** | **Fast Ethernet** | **Gigabit Ethernet** | **10-Gigabit Ethernet** |
| --- | --- | --- | --- |
| Speed | 100 Mbps | 1 Gbps | 10 Gbps |
| Standard | IEEE 802.3u | IEEE 802.3ab/z | IEEE 802.3ae |
| Medium | Cat5, Cat5e | Cat5e, Cat6, Fiber | Cat6a, Cat7, Fiber |
| Max Cable Length | 100 m | 100 m (Cat5e) | 100 m (Cat6a/Cat7) |
| Use Case | LANs | High-speed LANs | Data centers, servers |

**6.IEEE 802.11 Wireless Standards Overview**

These standards define how wireless data is transmitted over radio waves in **Wi-Fi** networks. Each new version improves speed, range, and bandwidth efficiency.

**6.1 IEEE 802.11a**

* **Released:** 1999
* **Frequency Band:** 5 GHz
* **Max Data Rate:** 54 Mbps
* **Modulation:** OFDM (Orthogonal Frequency Division Multiplexing)

**Advantages:**

* Less interference (compared to 2.4 GHz)
* Higher data rate than 802.11b

**Limitations:**

* Shorter range due to 5 GHz propagation limits
* Less compatible with older devices

**Usage:**

* Early enterprise networks
* Environments needing high speed and less interference
* Industrial applications with controlled access

**6.2 IEEE 802.11b**

* **Released:** 1999
* **Frequency Band:** 2.4 GHz
* **Max Data Rate:** 11 Mbps
* **Modulation:** DSSS (Direct Sequence Spread Spectrum)

**Advantages:**

* Wider range
* Compatible with many devices

**Limitations:**

* Susceptible to interference (microwaves, Bluetooth)
* Low data rate

**Usage:**

* Early home and small office Wi-Fi setups
* Devices where long-range communication is more important than speed
* Legacy IoT devices (still found in some places)

**6.3 IEEE 802.11g**

* **Released:** 2003
* **Frequency Band:** 2.4 GHz
* **Max Data Rate:** 54 Mbps
* **Modulation:** OFDM + DSSS (backward compatibility with 802.11b)

**Advantages:**

* Combines speed of 802.11a with range of 802.11b
* Compatible with 802.11b devices

**Limitations:**

* Same interference issues as 802.11b (2.4 GHz)

**Usage:**

* Home networks (especially in the 2000s)
* Wi-Fi routers supporting both 802.11b and g devices
* Public Wi-Fi in cafes, schools, and small offices

**6.4 IEEE 802.11n**

* **Released:** 2009
* **Frequency Bands:** 2.4 GHz **and** 5 GHz (dual-band)
* **Max Data Rate:** Up to 600 Mbps
* **Technology Used:**
  + **MIMO** (Multiple Input, Multiple Output)
  + **Channel bonding** (40 MHz wide channels)

**Advantages:**

* High speed and long range
* Better signal reliability
* Backward compatible with 802.11a/b/g

**Limitations:**

* Performance depends on environment and interference

**Usage:**

* Widely used in modern homes and businesses
* Streaming HD videos, video conferencing, online gaming
* Routers with dual-band (2.4 + 5 GHz) support
* Smart TVs, laptops, tablets, smartphones

**6.5 IEEE 802.11ac**

* **Released:** 2013
* **Frequency Band:** 5 GHz
* **Max Data Rate:** Up to 1.3 Gbps (Wave 1), 6.9 Gbps (Wave 2)
* **Technology Used:**
  + **MU-MIMO** (Multi-User MIMO)
  + **Wider channels (80/160 MHz)**
  + **Beamforming**

**Advantages:**

* Very high speed and capacity
* Supports multiple users simultaneously (MU-MIMO)
* Best for HD/4K streaming and gaming

**Limitations:**

* Operates only on 5 GHz (shorter range than 2.4 GHz)
* Requires compatible devices

**Usage:**

* High-speed home and office networks
* 4K/8K video streaming, cloud computing, real-time gaming
* Multi-device environments with high bandwidth needs
* Wi-Fi mesh systems, enterprise-grade access points

**6.6** **Summary Table**

| **Standard** | **Frequency** | **Max Speed** | **Modulation** | **Key Features** |
| --- | --- | --- | --- | --- |
| 802.11a | 5 GHz | 54 Mbps | OFDM | Less interference, short range |
| 802.11b | 2.4 GHz | 11 Mbps | DSSS | Long range, more interference |
| 802.11g | 2.4 GHz | 54 Mbps | OFDM | Good speed & compatibility |
| 802.11n | 2.4/5 GHz | 600 Mbps | MIMO | Dual band, long range |
| 802.11ac | 5 GHz | 1.3–6.9 Gbps | MU-MIMO | High speed, beamforming |

**7. IEEE 802.15 – Wireless Personal Area Networks (WPANs)**

IEEE 802.15 is a set of standards developed for **Wireless Personal Area Networks (WPANs)**. These networks support **short-range wireless communication** between devices within a personal operating space, typically within **10 meters**.

**Key Objectives:**

* Enable **low-power**, **low-cost**, and **short-range** wireless communication.
* Support both **low-data-rate** and **high-data-rate** applications.
* Facilitate communication between **mobile and stationary devices** like smartphones, smartwatches, wearables, headphones, sensors, etc.

**Types / Variants of IEEE 802.15:**

| **Standard** | **Description** | **Application** |
| --- | --- | --- |
| **802.15.1** | Based on Bluetooth | Short-range wireless communication in phones, headsets |
| **802.15.3** | High data rate WPANs (~11–55 Mbps) | Wireless multimedia systems (video, gaming) |
| **802.15.4** | Low data rate, low power, low complexity | Zigbee, 6LoWPAN, IoT networks, smart meters |
| **802.15.6** | Body Area Networks (BANs) | Wearable health monitoring, implants |
| **802.15.7** | Visible Light Communication (VLC) | Communication using LED lights (Li-Fi) |

**Features:**

* Operates typically in **2.4 GHz ISM band** (unlicensed).
* Supports **point-to-point, point-to-multipoint**, and **peer-to-peer** communication.
* Designed to minimize **interference** with other standards like IEEE 802.11 (Wi-Fi).

**Advantages:**

* Energy-efficient (especially 802.15.4)
* Ideal for **IoT**, **smart homes**, and **healthcare**
* Cost-effective and easy to deploy
* Can work without infrastructure (peer-to-peer)

**Limitations:**

* Limited communication range (~10 meters)
* Lower bandwidth compared to Wi-Fi
* Vulnerable to interference from other 2.4 GHz devices
* Security concerns if not properly configured

**8. IEEE 802.15.4?**

IEEE 802.15.4 is a standard specifically designed for **low-rate, low-power, and low-cost** wireless communication over **short distances**. It forms the foundation for higher-level protocols like:

* **Zigbee**
* **6LoWPAN**
* **Thread**
* **MiWi**

**Key Features:**

| **Feature** | **Details** |
| --- | --- |
| **Frequency Bands** | 2.4 GHz (global), 868 MHz (Europe), 915 MHz (North America) |
| **Data Rate** | 250 kbps (2.4 GHz), 20–40 kbps (sub-GHz bands) |
| **Range** | ~10 to 100 meters (depending on power and environment) |
| **Topology Support** | Star and Peer-to-Peer (Mesh via Zigbee) |
| **Power Efficiency** | Extremely low; suitable for battery-powered devices |
| **Modulation** | O-QPSK (2.4 GHz), BPSK (868/915 MHz) |

**Architecture Overview:**

IEEE 802.15.4 supports two device roles:

* **Full-Function Device (FFD):** Can communicate with any other device and act as a network coordinator.
* **Reduced-Function Device (RFD):** Simplified device, communicates only with FFD; ideal for sensors/actuators.

These form:

* **Star topology**: One coordinator, multiple devices.
* **Peer-to-peer (mesh)**: Multiple FFDs, enabling robust network paths.

**Advantages:**

* **Energy Efficient**: Ideal for battery-powered sensors.
* **Scalable**: Supports large-scale mesh networks with upper-layer protocols (e.g., Zigbee).
* **Low Complexity and Cost**: Hardware and implementation are lightweight.
* **Reliable for IoT**: Designed for interference resilience in sensor environments.

**Limitations:**

* **Low Data Rate**: Not suitable for video/audio streaming.
* **Limited Range**: Needs repeaters or mesh routing for extended areas.
* **Requires Upper Layers**: Alone, 802.15.4 provides only physical and MAC layers.

**Use Cases:**

* Smart homes and cities (Zigbee-based devices)
* Wireless sensor networks
* Industrial automation
* Environmental monitoring
* Medical and health monitoring (BANs)

**9. IEEE 802.16?**

IEEE 802.16 is a set of standards developed for **broadband wireless access (BWA)** systems, particularly over **metropolitan areas**. It is most famously associated with **WiMAX (Worldwide Interoperability for Microwave Access)**.

**Key Features:**

| **Feature** | **Details** |
| --- | --- |
| **Technology Name** | WiMAX (802.16d – fixed, 802.16e – mobile) |
| **Frequency Bands** | 2–11 GHz (Non-Line-of-Sight), 10–66 GHz (Line-of-Sight) |
| **Data Rate** | Up to 70 Mbps (in early versions); >100 Mbps in newer releases |
| **Coverage Range** | 2 to 50 km (urban to rural environments) |
| **Access Method** | OFDMA (Orthogonal Frequency-Division Multiple Access) |
| **Duplexing Methods** | TDD (Time Division Duplex) and FDD (Frequency Division Duplex) |

**Architecture Overview:**

1. **Base Station (BS)** – Central unit providing broadband service to multiple users.
2. **Subscriber Station (SS)** or Customer Premise Equipment (CPE) – Devices that receive WiMAX signal at user end.

Supports:

* **Point-to-Multipoint (PMP)** connectivity
* **Mesh or Relay mode** for extended coverage

**Advantages:**

* **High-Speed Internet**: Competes with DSL/cable in underserved areas.
* **Long Range**: Much wider coverage compared to Wi-Fi.
* **Quality of Service (QoS)**: Built-in support for voice, video, and data prioritization.
* **Mobility Support**: In 802.16e (Mobile WiMAX).

**Limitations:**

* **Line-of-Sight Requirements**: For certain high-frequency deployments.
* **High Setup Cost**: Especially in areas with existing 4G/5G infrastructure.
* **Decline in Use**: Overshadowed by LTE and 5G in many regions.
* **Battery Consumption**: Higher compared to Wi-Fi in mobile use.

**Use Cases:**

* Last-mile broadband for rural areas
* Internet backhaul for cellular networks
* Temporary or emergency internet deployments
* Connectivity in areas without wired infrastructure

**8. Switching Techniques**

In large networks, there may be more than one paths for transmitting data from **sender** to receiver. Selecting a path that data must take out of the available options is called **switching**. There are two popular switching techniques – circuit switching and packet switching.

**8.1 Circuit Switching**

When a dedicated path is established for data transmission between sender and receiver, it is called circuit switching. When any network node wants to send data, be it audio, video, text or any other type of information, a **call request signal** is sent to the receiver and acknowledged back to ensure availability of dedicated path. This dedicated path is then used to send data. ARPANET used circuit switching for communication over the network.

**Advantages of Circuit Switching**

Circuit switching provides these advantages over other switching techniques −

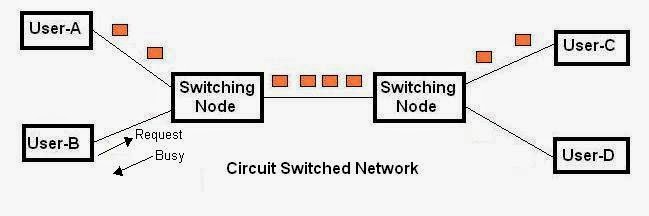
* Once path is set up, the only delay is in data transmission speed
* No problem of congestion or garbled message

**Disadvantages of Circuit Switching**

Circuit switching has its disadvantages too −

* Long set up time is required
* A request token must travel to the receiver and then acknowledged before any transmission can happen
* Line may be held up for a long time

**Example:** Telephone Network



**8.2 Message switching**

Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. In message switching, end users communicate by sending and receiving *messages* that included the entire data to be shared. Messages are the smallest individual unit.

Also, the sender and receiver are not directly connected. There are a number of intermediate nodes transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems.

They provide 2 distinct and important characteristics:

1. **Store and forward –** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it’ll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery –** This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination

**Advantages of Message Switching –**

**Message switching has the following advantages:**

1. As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in network.
2. In message switching, the data channels are shared by the network devices.
3. It makes the traffic management efficient by assigning priorities to the messages.

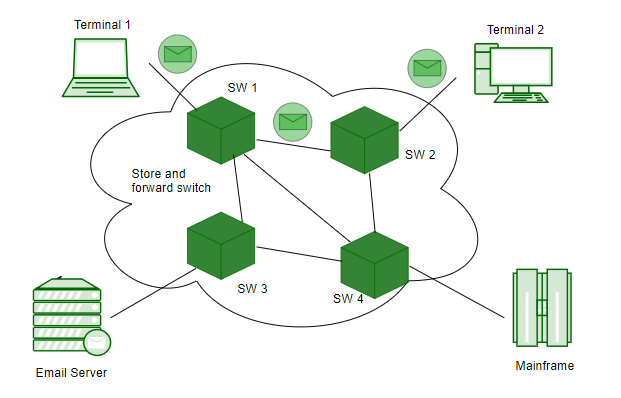
**Disadvantages of Message Switching –**

**Message switching has the following disadvantages:**

1. Message switching cannot be used for real time applications as storing of messages causes delay.
2. In message switching, message has to be stored for which every intermediate devices in the network requires a large storing capacity.

**Applications –**

The store-and-forward method was implemented in telegraph message switching centers. Today, although many major networks and systems are packet-switched or circuit switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched



**8.3 Packet switching**

**Packet switching** is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.

Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first store that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of source and destination. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different path possible over existing network.

Packet-Switched networks were designed to overcome the *weaknesses* of Circuit-Switched networks since circuit-switched networks were not very effective for small messages.

**Advantage of Packet Switching over Circuit Switching :**

* More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
* Minimal transmission latency.
* More reliable as destination can detect the missing packet.
* More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
* Cost effective and comparatively cheaper to implement.

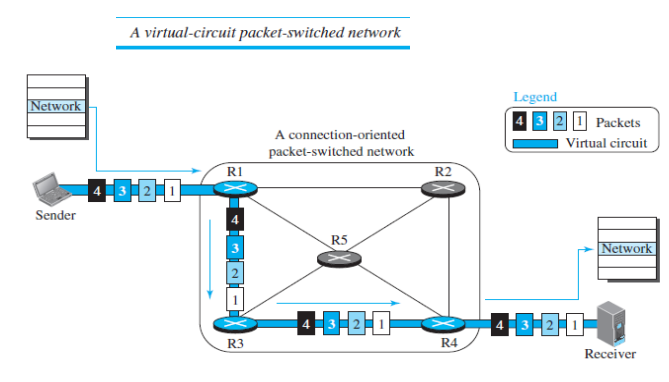
**Disadvantage of Packet Switching over Circuit Switching :**

* Packet Switching don’t give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
* Since the packets are unordered, we need to provide sequence numbers to each packet.
* Complexity is more at each node because of the facility to follow multiple path.
* Transmission delay is more because of rerouting.
* Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

**Modes of Packet Switching :**

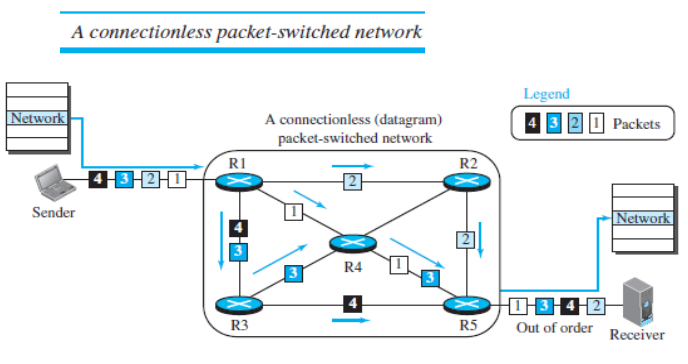
* **Connection-oriented Packet Switching (Virtual Circuit) :**

Before starting the transmission, it establishes a logical path or virtual connection using signalling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases takes place here- Setup, data transfer and tear down phase. All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc.  Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).



* **Connectionless Packet Switching (Datagram) :**

Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.  Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.



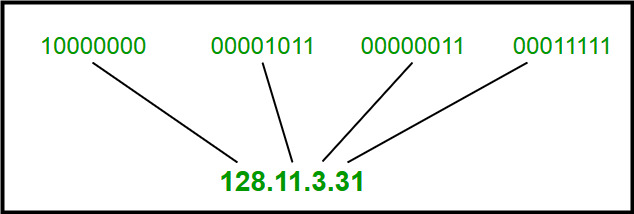
**8.4 Difference between Circuit Switching, Message Switching, Packet Switching**

| **Feature** | **Circuit Switching** | **Message Switching** | **Packet Switching** |
| --- | --- | --- | --- |
| Path Setup | Required | Not required | Optional (Virtual Circuit) |
| Resource Reservation | Dedicated | Shared | Shared |
| Delay | Low (after setup) | High (store & forward) | Variable (jitter possible) |
| Efficiency | Low | Moderate | High |
| Suitable for | Voice calls | Emails, non-real-time | Internet, real-time data |
| Data Units | Continuous stream | Entire message | Small packets |

**9. Network Addressing**

* Network Addressing is one of the major responsibilities of the network layer.
* Network addresses are always logical, i.e., software-based addresses.
* A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
* A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
* Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 232.  
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.



**9.1 Classful Addressing**

The 32 bit IP address is divided into five sub-classes. These are:

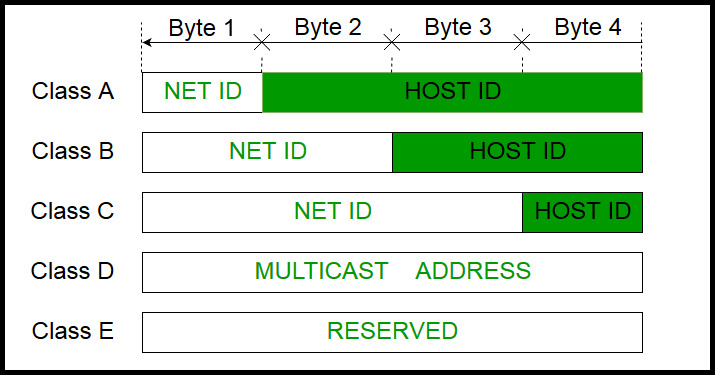
* Class A
* Class B
* Class C
* Class D
* Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 address is divided into two parts:

* **Network ID**
* **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



**Class A:**

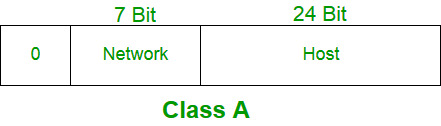
IP address belonging to class A are assigned to the networks that contain a large number of hosts.

* The network ID is 8 bits long.
* The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

* 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address. )
* 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x



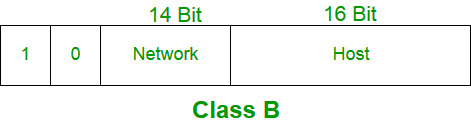
**Class B:**

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

* The network ID is 16 bits long.
* The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

* 2^14 = 16384 network address
* 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_5.jpg)

**Class C:**

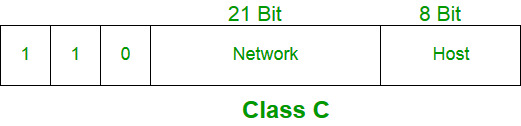
IP address belonging to class C are assigned to small-sized networks.

* + The network ID is 24 bits long.
  + The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

* + 2^21 = 2097152 network address
  + 2^8 – 2 = 254 host address

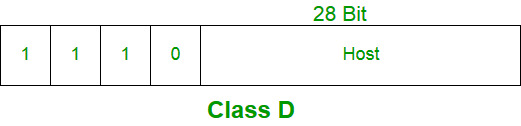
IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_6.jpg)

**Class D:**

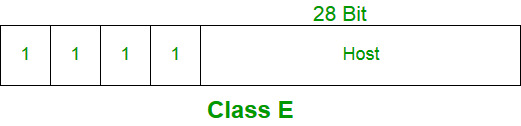
IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



**Class E:**

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn’t have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



**Range of special IP addresses:**

**169.254.0.0 – 169.254.0.16** : Link local addresses

**127.0.0.0 – 127.0.0.8** : Loop-back addresses

**0.0.0.0 – 0.0.0.8** : used to communicate within the current network.

**Rules for assigning Host ID:**

Host ID’s are used to identify a host within a network. The host ID are assigned based on the following rules:

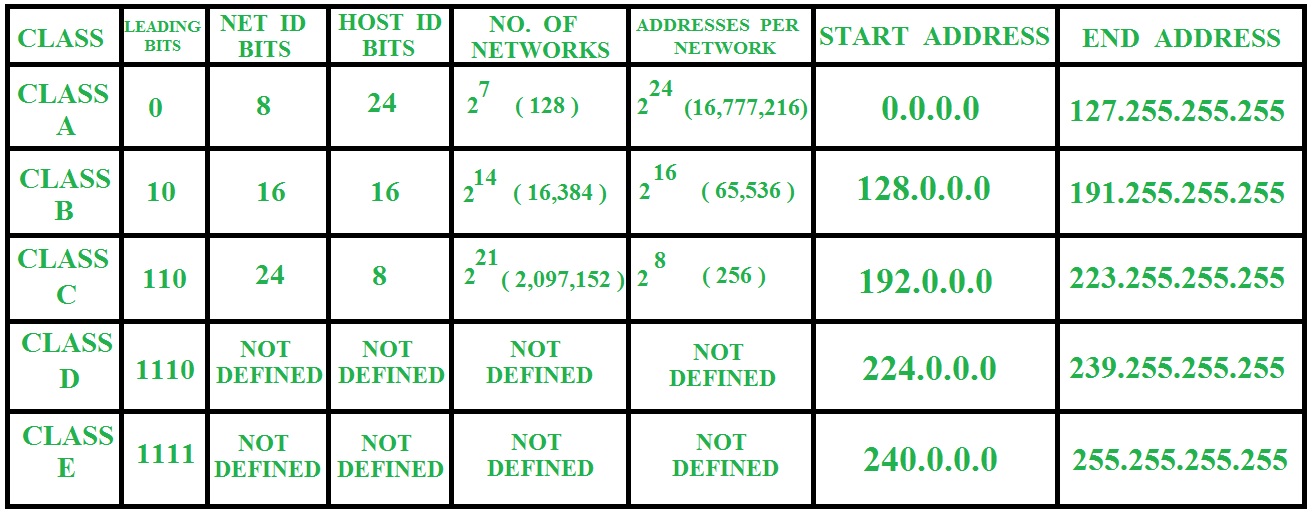
* + Within any network, the host ID must be unique to that network.
  + Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
  + Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

**Rules for assigning Network ID:**

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

* + The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
  + All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
  + All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren’t used.

**Summary of Classful addressing :**



**Problems with Classful Addressing:**

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in next post.

**9. What is IPv4?**

**IP** stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.   
IP version four addresses are 32-bit integers which will be expressed in decimal notation.   
Example- 192.0.2.126 could be an IPv4 address.

**Parts of IPv4**

**Network part:**

The network part indicates the distinctive variety that’s appointed to the network. The network part conjointly identifies the category of the network that’s assigned.

**Host Part:**

The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.

For each host on the network, the network part is the same, however, the host half must vary.

**Subnet number:**

This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

**Characteristics of IPv4**

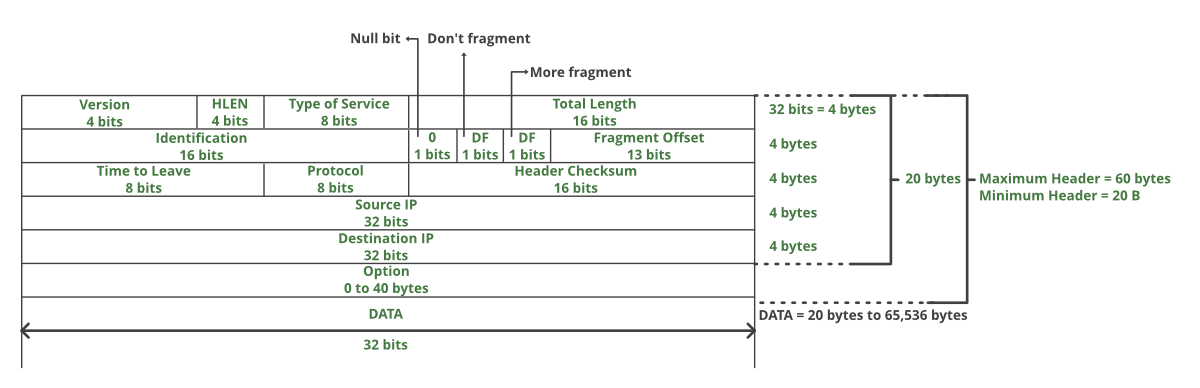
* IPv4 could be a 32-Bit IP Address.
* IPv4 could be a numeric address, and its bits are separated by a dot.
* The number of header fields is twelve and the length of the header field is twenty.
* It has Unicast, broadcast, and multicast style of addresses.
* IPv4 supports VLSM (Virtual Length Subnet Mask).
* IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
* RIP may be a routing protocol supported by the routed daemon.
* Networks ought to be designed either manually or with DHCP.
* Packet fragmentation permits from routers and causing host.

**Advantages of IPv4**

* IPv4 security permits encryption to keep up privacy and security.
* IPV4 network allocation is significant and presently has quite 85000 practical routers.
* It becomes easy to attach multiple devices across an outsized network while not NAT.
* This is a model of communication so provides quality service also as economical knowledge transfer.
* IPV4 addresses are redefined and permit flawless encoding.
* Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
* Data communication across the network becomes a lot of specific in multicast organizations.
  + Limits net growth for existing users and hinders the use of the net for brand new users.
  + Internet Routing is inefficient in IPv4.
  + IPv4 has high System Management prices and it’s labor-intensive, complex, slow & frequent to errors.
  + Security features are nonobligatory.
  + Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

**IPv4 Datagram Header:**

Size of the header is 20 to 60 bytes.



**VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4

**HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

**Type of service:** Low Delay, High Throughput, Reliability (8 bits)

**Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

**Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

**Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

**Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

**Time to live:** Datagram’s lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

**Protocol:** Name of the protocol to which the data is to be passed (8 bits)

**Header Checksum:** 16 bits header checksum for checking errors in the datagram header

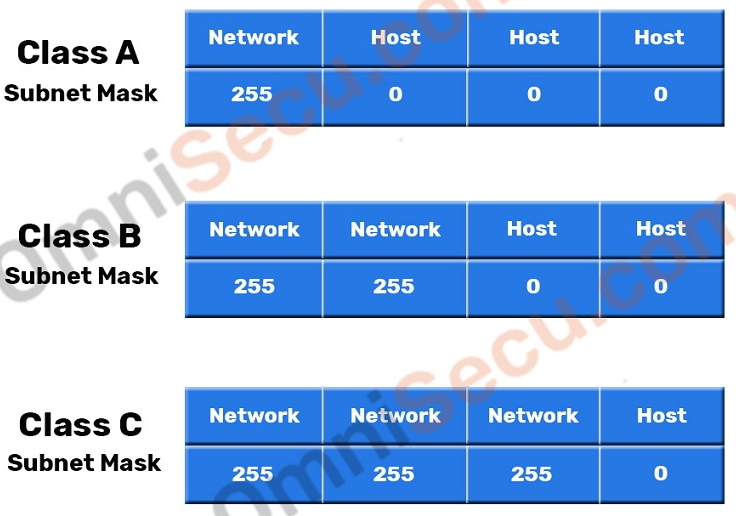
**Source IP address:** 32 bits IP address of the sender

**Destination IP address:** 32 bits IP address of the receiver

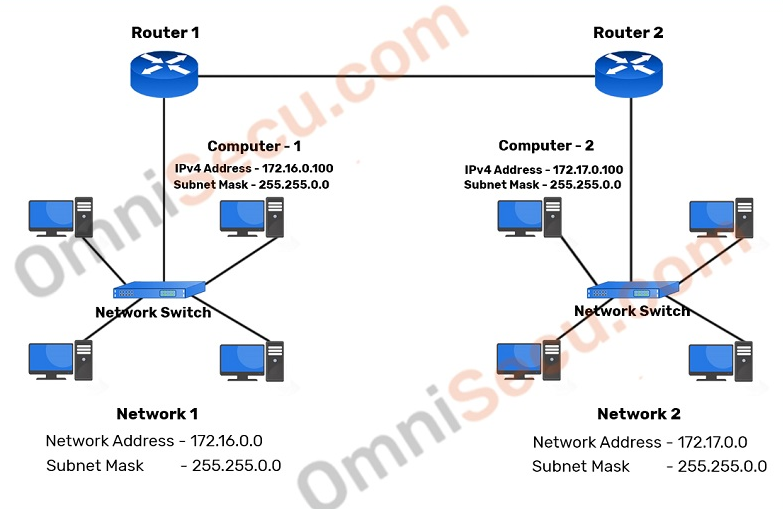
**Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

**9. What is Subnet Mask?**

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.



Consider below example of two Class B neworks. Two computers with IPv4 addresses 172.16.0.100/255.255.0.0 172.17.0.100/255.255.0.0 as shown in below image belong to two different networks, 172.16.0.0 and 172.17.0.0 network respectively. Computers located in different networks cannot communicate directly in IPv4. You need a [router](https://www.omnisecu.com/basic-networking/network-infrastructure-devices-what-is-a-router.php) to communicate between two different IPv4 networks. Please refer below image, which shows two different Class B networks connected together by [routers](https://www.omnisecu.com/basic-networking/network-infrastructure-devices-what-is-a-router.php).



We have two networks in above image, connected together by routers. As marked, the network address of one network ("Network 1") is 172.16.0.0 with a subnet mask of 255.255.0.0 and the network address of other network ("Network 2") is 172.17.0.0 with a subnet mask of 255.255.0.0.

Wherever "255" octet appears in the subnet mask, corresponding octet in IPv4 address belongs to the network part. Wherever "0" appears in the subnet mask, corresponding octet in IPv4 address belongs to the host part. In other words, "172.16" is the network address of "Network 1" and "172.17" is the network address of "Network 2". Please note that the previous example is shown in decimals but actual calculations are done using binary numbers.

**10. Internet Protocol version 6 (IPv6)**

IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion. IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes.



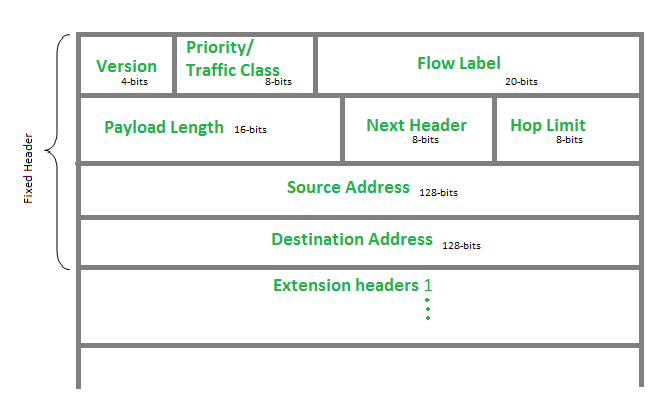
In IPv6 representation, we have three addressing methods :

* Unicast
* Multicast
* Anycast

**Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.

**Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.  
**Anycast Address:** Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

**IP version 6 Header Format :**



**Version (4-bits) :** Indicates version of Internet Protocol which contains bit sequence 0110.

**Traffic Class (8-bits) :** The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router then packets with least priority will be discarded.  
As of now only 4-bits are being used (and remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

**Flow Label (20-bits) :** Flow Label field is used by source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real time service. In order to distinguish the flow, intermediate router can use source address, destination address and flow label of the packets. Between a source and destination multiple flows may exist because many processes might be running at the same time. Routers or Host that do not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, source is also supposed to specify the lifetime of flow.

**Payload Length (16-bits) :** It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload. Payload Length field includes extension headers(if any) and upper layer packet. In case length of payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and jumbo payload option is used in the Hop-by-Hop options extension header.

**Next Header (8-bits) :** Next Header indicates type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packet, such as TCP, UDP.

**Hop Limit (8-bits) :** Hop Limit field is same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and packet is discarded if value decrements to 0. This is used to discard the packets that are stuck in infinite loop because of some routing error.

**Source Address (128-bits) :** Source Address is 128-bit IPv6 address of the original source of the packet.

**Destination Address (128-bits) :** Destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

**Extension Headers :** In order to rectify the limitations of *IPv4 Option Field*, Extension Headers are introduced in IPversion 6. The extension header mechanism is very important part of the IPv6 architecture. Next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

| **IPv4** | **IPv6** |
| --- | --- |
| IPv4 has 32-bit address length | IPv6 has 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end connection integrity is Unachievable | In IPv6 end to end connection integrity is Achievable |
| It can generate 4.29×109 address space | Address space of IPv6 is quite large it can produce 3.4×1038 address space |
| Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by sender |
| In IPv4 Packet flow identification is not available | In IPv6 packetflow identification are Available and uses flow label field in the header |
| In IPv4 checksumfield is available | In IPv6 checksumfield is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has header of 20-60 bytes. | IPv6 has header of 40 bytes fixed |

**11. Network Address Translation**

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

**Network Address Translation (NAT) working –**

Generally, the border router is configured for NAT i.e the router which has one interface in local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

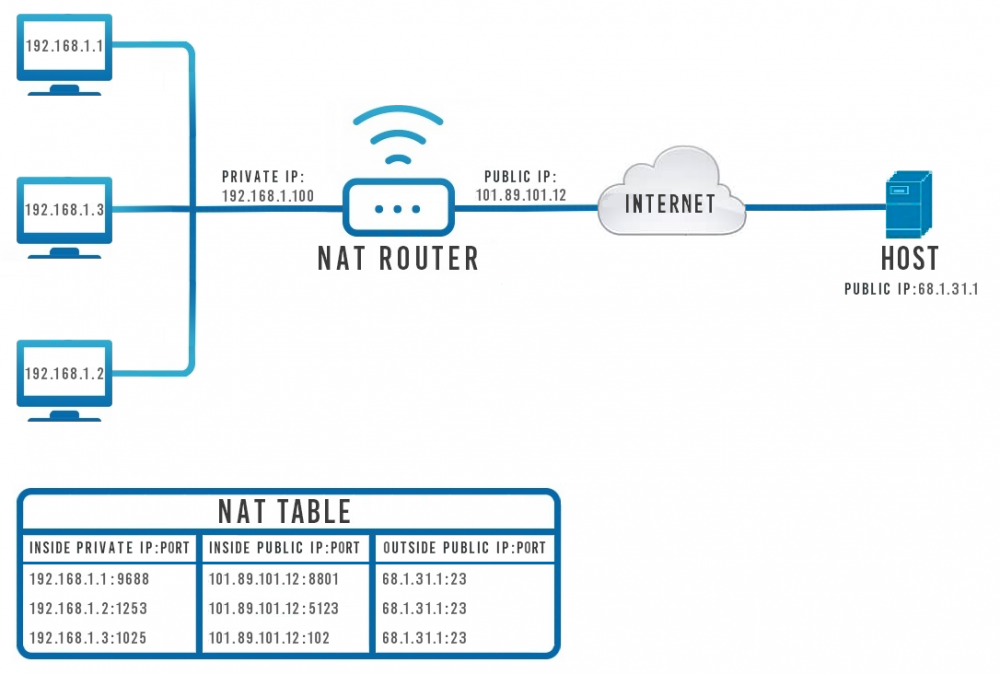
If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

**Why mask port numbers?**

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does an only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

**NAT inside and outside addresses –**

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organisation. These are the network Addresses in which the translation of the addresses will be done.



* **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.
* **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
* **Outside local address –** This is the actual IP address of the destination host in the local network after translation.
* **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

**Network Address Translation (NAT) Types –**

There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.

Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.

1. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool. 

1. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

**Advantages of NAT –**

* NAT conserves legally registered IP addresses .
* It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
* Eliminates address renumbering when a network evolves.

**Disadvantage of NAT –**

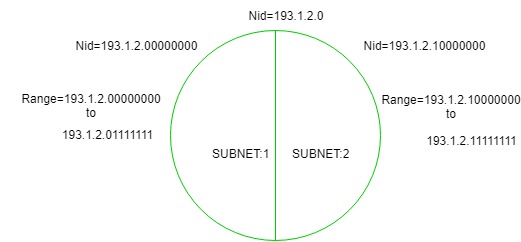
* Translation results in switching path delays.
* Certain applications will not function while NAT is enabled.
* Complicates tunneling protocols such as IPsec.
* Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

**12. Subnetting**

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, maintenance is easier for smaller networks.

**Now, let’s talk about dividing a network into two parts:**

so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets. **Note:** It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

* **For Subnet-1:**

The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1’s in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet-1:

193.1.2.0 to 193.1.2.127

* **For Subnet-2:**

The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1’s in the host ID part i.e, 193.1.2.11111111).

Thus, the range of subnet-2:

193.1.2.128 to 193.1.2.255

**Note:**

1. To divide a network into four (22) parts you need to choose two bits from host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (23) parts you need to choose three bits from host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.

13. **Classless Inter Domain Routing (CIDR)**

As we have already learned about Classful Addressing, so in this article, we are going to learn about Classless Inter-Domain Routing. which is also known as Classless addressing. In the Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.

Class A network contains 224 Hosts,

Class B network contains 216 Hosts,

Class C network contains 28 Hosts

Now, let’s suppose an Organization requires 214 hosts, then it must have to purchase a Class B network. In this case, 49152 Hosts will be wasted. This is the major drawback of Classful Addressing.

In order to reduce the wastage of IP addresses a new concept of **Classless Inter-Domain Routing** is introduced. Now a days *IANA* is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.

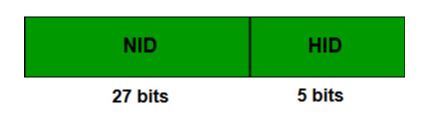
**Representation:** It is as also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.

Where, n is number of bits that are present in Block Id / Network Id.  
**Example:**

20.10.50.100/20

**Rules for forming CIDR Blocks:**

1. All IP addresses must be contiguous.
2. Block size must be the power of 2 (2n).
3. If the size of the block is the power of 2, then it will be easy to divide the Network. Finding out the Block Id is very easy if the block size is of the power of 2.  
   **Example:**  
   If the Block size is 25 then, Host Id will contain 5 bits and Network will contain 32 – 5 = 27 bits.



1. First IP address of the Block must be evenly divisible by the size of the block. in simple words, the least significant part should always start with zeroes in Host Id. Since all the least significant bits of Host Id is zero, then we can use it as Block Id part.

**Example:**  
Check whether 100.1.2.32 to 100.1.2.47 is a valid IP address block or not?

1. All the IP addresses are contiguous.
2. Total number of IP addresses in the Block = 16 = 24.
3. 1st IP address: 100.1.2.00100000
4. Since, Host Id will contains last 4 bits and all the least significant 4 bits are zero. Hence, first IP address is evenly divisible by the size of the block.

All the three rules are followed by this Block. Hence, it is a valid IP address block.

**14. Internet Control Message Protocol** (**ICMP**)

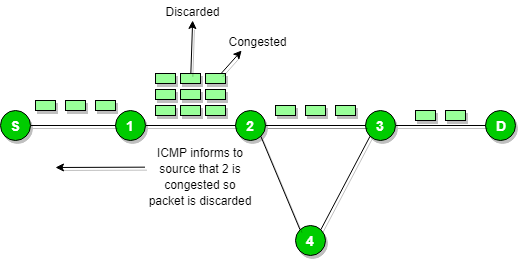
The **Internet Control Message Protocol** (**ICMP**) is a supporting [protocol](https://en.wikipedia.org/wiki/Communications_protocol) in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). It is used by [network devices](https://en.wikipedia.org/wiki/Network_device), including [routers](https://en.wikipedia.org/wiki/Router_(computing)), to send error messages and operational information indicating success or failure when communicating with another [IP address](https://en.wikipedia.org/wiki/IP_address), for example, an error is indicated when a requested service is not available or that a [host](https://en.wikipedia.org/wiki/Host_(network)) or router could not be reached.[[2]](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol#cite_note-Forouzan-2) ICMP differs from [transport protocols](https://en.wikipedia.org/wiki/Transport_protocol) such as [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) and [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like [ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)) and [traceroute](https://en.wikipedia.org/wiki/Traceroute)).

ICMP for [IPv4](https://en.wikipedia.org/wiki/IPv4) is defined in RFC 792. A separate [ICMPv6](https://en.wikipedia.org/wiki/ICMPv6), defined by RFC 4443, is used with [IPv6](https://en.wikipedia.org/wiki/IPv6).

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.   
e.g. the requested service is not available or that a host or router could not be reached.

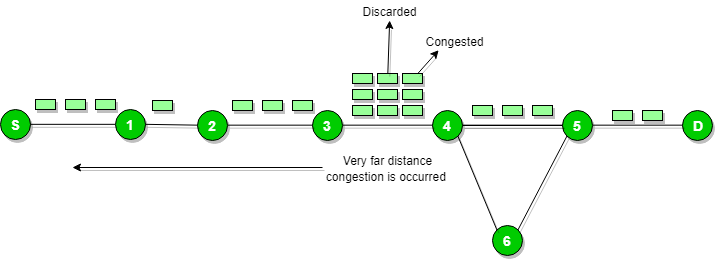
**Source quench message :**

Source quench message is request to decrease traffic rate for messages sending to the host(destination). Or we can say, when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost. ICMP will take source IP from the discarded packet and informs to source by sending source quench message.



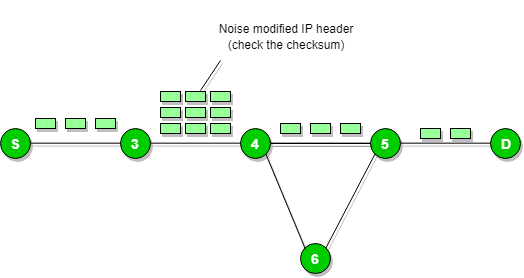
Then source will reduce the speed of transmission so that router will free from congestion.

When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.



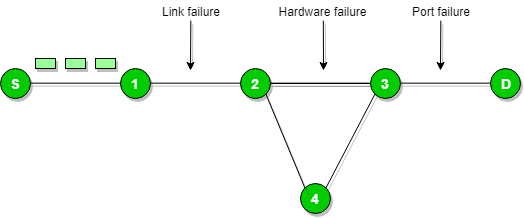
**Parameter problem :**

Whenever packets come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by the router. If there is mismatch packet will be dropped by the router.  ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.



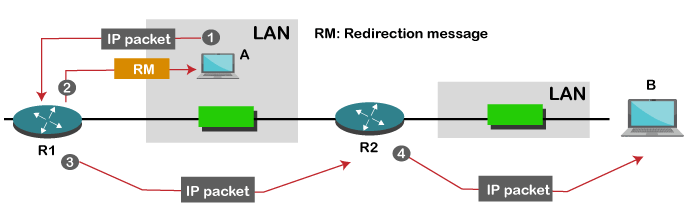
**Destination un-reachable :**

Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason. There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure,hardware failure,port failure etc) happen in the network.

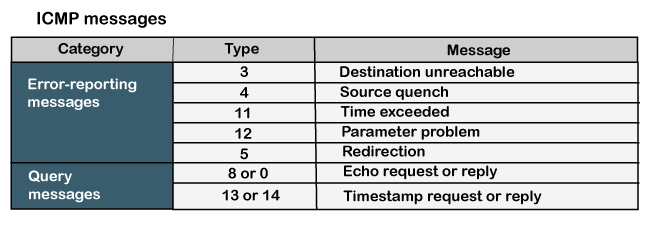


**Redirection message :**

Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).  When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message. For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and redirection message to A so that A can update its routing table.

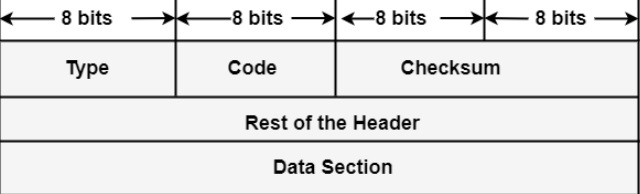


**The ICMP messages are usually divided into two categories:**



**ICMP Message Format**

AN ICMP message includes an 8-byte header and a variable size data format.



* **Type:** It is an 8-bit field. It represents the ICMP message type. The values area from 0 to 127 are described for ICMPv6, and the values from 128 to 255 are the data messages.
* **Code:** It is an 8-bit field that represents the subtype of the ICMP message.
* **Checksum:** It is a 16-bit field to recognize whether the error exists in the message or not.

**15. Internet Group Management Protocol**

**IGMP** is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3.

The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.

**Applications:**

* **Streaming –**

Multicast routing protocol are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.

* **Gaming –**

Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.

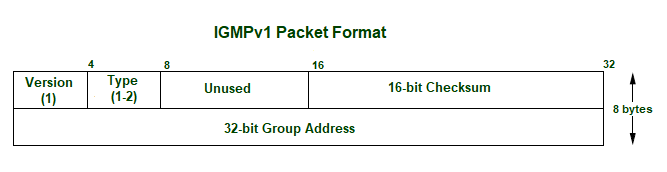
* **Web Conferencing tools –**

Video conferencing is a new method to meet people from your own convenience and IGMP connects to the users for conferencing and transfers the message/data packets efficiently.

**Types:**  
There are 3 versions of IGMP. These versions are backward compatible.

**IGMPv1 :**

The version of IGMP communication protocol allows all the supporting hosts to join the multicast groups using membership request and include some basic features. But, host cannot leave the group on their own and have to wait for a timeout to leave the group.  
The message packet format in IGMPv1:

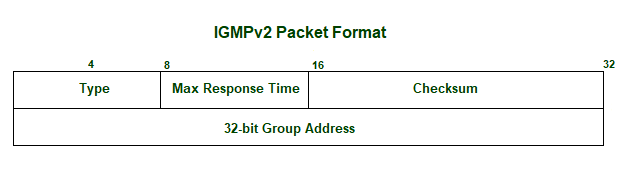


* **Version –**Set to 1.
* **Type–**1 for Host Membership Query and Host Membership Report.
* **Unused–**8-bits of zero which are of no use.
* **Checksum –**It is the one’s complement of the one’s complement of the sum of IGMP message.
* **Group Address –**The group address field is zero when sent and ignored when received in membership query message. In a membership report message, the group address field takes the IP host group address of the group being reported.

**IGMPv2 :**

IGMPv2 is the revised version of IGMPv1 communication protocol. It has added functionality of leaving the multicast group using group membership.

The message packet format in IGMPv2:



* **Type –**

0x11 for Membership Query

0x12 for IGMPv1 Membership Report

0x16 for IGMPv2 Membership Report

0x22 for IGMPv3 Membership Report

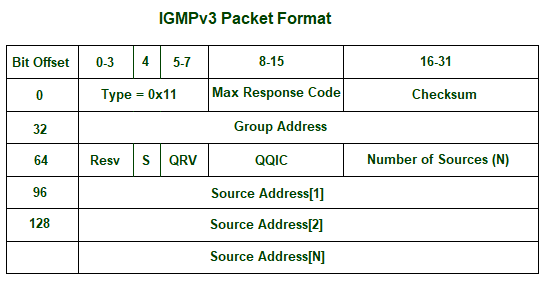
0x17 for Leave Group

* **Max Response Time –**This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
* **Checksum –**It is the one’s complement of the one’s complement of the sum of IGMP message.
* **Group Address –**It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.

**IGMPv3 :**

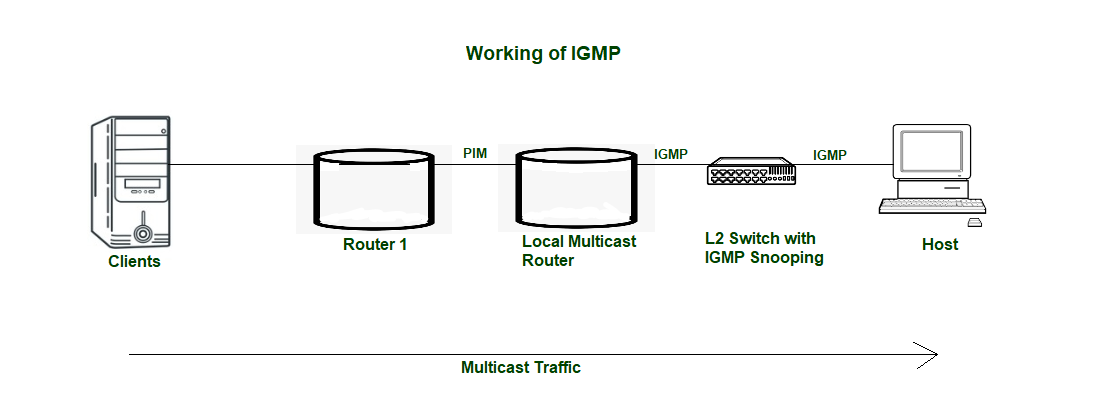
IGMPv2 was revised to IGMPv3 and added source-specific multicast and membership report aggregation. These reports are sent to 224.0.0.22.

The message packet format in IGMPv3:



* **Max Response Time –**This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
* **Checksum –**It is the one’s complement of the one’s complement of the sum of IGMP message.
* **Group Address –**It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.
* **Resv –**It is set zero of sent and ignored when received.
* **S flag –**It represents Suppress Router-side Processing flag. When the flag is set, it indicates to suppress the timer updates that multicast routers perform upon receiving any query.
* **QRV –**It represents Querier’s Robustness Variable. Routers keeps on retrieving the QRV value from the most recently received query as their own value until the most recently received QRV is zero.
* **QQIC –**It represents Querier’s Query Interval Code.
* **Number of sources –**It represents the number of source addresses present in the query. For general query or group-specific query, this field is zero and for group-and-source-specific query, this field is non-zero.
* **Source Address[i] –**It represents the IP unicast address for N fields.

**Working:**  
IGMP works on devices that are capable of handling multicast groups and dynamic multicasting. These devices allows the host to join or leave the membership in the multicast group. These devices also allows to add and remove clients from the group. This communication protocol is operated between host and local multicast router. When a multicast group is created, the multicast group address is in range of class D (224-239) IP addresses and is forwarded as destination IP address in the packet.



L2 or Level-2 devices such as switches are used in between host and multicast router for IGMP snooping. IGMP snooping is a process to listen to the IGMP network traffic in controlled manner. Switch receives the message from host and forwards the membership report to the local multicast router. The multicast traffic is further forwarded to remote routers from local multicast routers using PIM (Protocol Independent Multicast) so that clients can receive the message/data packets. Clients wishing to join the network sends join message in the query and switch intercepts the message and adds the ports of clients to its multicast routing table.

**Advantages:**

* IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimized performance.
* Bandwidth is consumed totally as all the shared links are connected.
* Hosts can leave a multicast group and join another.

**Disadvantages:**

* It does not provide good efficiency in filtering and security.
* Due to lack of TCP, network congestion can occur.
* IGMP is vulnerable to some attacks such as DOS attack (Denial-Of-Service).