**UNIT 3**

**IPv4**

* IP stands for Internet Protocol version v4 stands for Version Four (IPv4), is the most widely used system for identifying devices on a network.
* It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address. This address helps data find its way from one device to another over the internet.

**IP Address**

An IP address (Internet Protocol address) is a unique identifier assigned to each device connected to a network that uses the Internet Protocol for communication. It serves two main purposes:

* Identification: It uniquely identifies a device on a network.
* Location Addressing: It indicates where a device is located within a network, making data routing possible.

**IPv4 Address Format**

* An IPv4 address consists of 32 bit (binary digit), grouped into four section of known as octets or bytes. Each octet has 8 bits and these bits can be represented only in 0 or 1 form, and when they grouped together, they form a binary number.
* Since each octet has 8 bits, it can represent 256 numbers ranging from o to 255. These four octets are represented as decimal numbers, separated by periods known as dotted decimal notation. For example IPv4 address 185.107.80.231 consists of four octets.

**Binary Representation**

IPv4 is basically converted into binary form by computer although these are usually seen in decimal form for human readability. Each octet is converted into 8 bit binary number . For instance 185.107.80.231 in binary looks like:

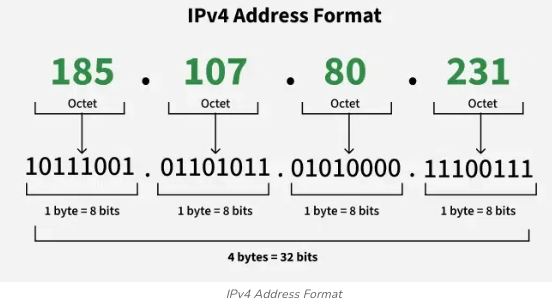
185: 10111001

107: 01101011

80: 01010000

231: 11100111

So 185.107.80.231 in binary is: 10111001.01101011.01010000.11100111



The [IPv4 address](https://www.geeksforgeeks.org/what-is-ipv4/) is divided into two parts: NID (Network ID) = 8bit, and HID (Host ID) = 24bit. So there are 28 which is 256 total networks created and 224 which is 16M Host per network.

**Classes of IP Addressing**

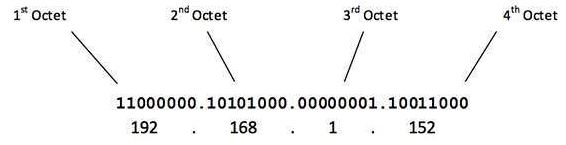
The 32-bit IP address is divided into five sub-classes. These are given below:

* 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.

All the five classes are identified by the first octet of IP Address.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address –



The number of networks and the number of hosts per class can be derived by this formula



Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

**Class A Addresses**

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2).

Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

**Class B Address**

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses. Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

**Class C Address**

The first octet of Class C IP address has its first 3 bits set to 110, that is –

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses. Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

**Class D Address**

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of 

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

**Class E Address**

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

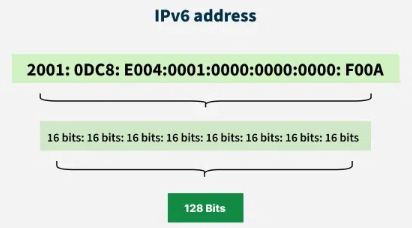
**Types of IPv4 Addressing**

IPv4 basically supports three different types of addressing modes:

* Unicast Addressing Mode: This addressing mode is used to specify single sender and single receiver. Example: Accessing a website.
* Broadcast Addressing Mode: This addressing mode is used to send messages to all devices in a network. Example: sending a message in local network to all the devices.
* Multicast Addressing Mode: This addressing mode is typically used within a local network or across networks and sends messages to a group of devices. Example: Streaming audio to multiple devices at once.

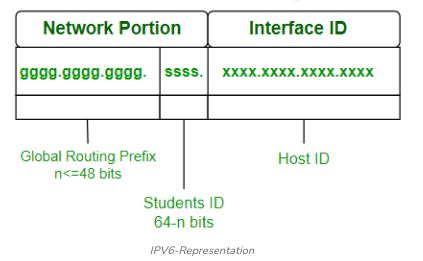
**IPv6**

* The next generation Internet Protocol (IP) address standard, known as IPv6, is meant to work in cooperation with IPv4.
* To communicate with other devices, a computer, smartphone, home automation component, Internet of Things sensor, or any other Internet-connected device needs a numerical IP address. Because so many connected devices are being used, the original IP address scheme, known as IPv4, is running out of addresses.
* This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456.



**Representation of IPv6**

An IPv6 address consists of eight groups of four hexadecimal digits separated by ‘ . ‘ and each Hex digit representing four bits so the total length of IPv6 is 128 bits. Structure given below.



The first 48 bits represent Global Routing Prefix. The next 16 bits represent the student ID and the last 64 bits represent the host ID. The first 64 bits represent the network portion and the last 64 bits represent the interface id.

* Global Routing Prefix: The Global Routing Prefix is the portion of an IPv6 address that is used to identify a specific network or subnet within the larger IPv6 internet. It is assigned by an ISP or a regional internet registry (RIR).
* Student Id: The portion of the address used within an organization to identify subnets. This usually follows the Global Routing Prefix.
* Host Id: The last part of the address, is used to identify a specific host on a network.

Example: 3001:0da8:75a3:0000:0000:8a2e:0370:7334

**Types of IPv6 Address**

Now that we know about what is IPv6 address let’s take a look at its different types.

* **Unicast Addresses** : Only one interface is specified by the unicast address. A packet moves from one host to the destination host when it is sent to a unicast address destination.
* **Multicast Addresses**: It represents a group of IP devices and can only be used as the destination of a datagram.
* **Anycast Addresses:** The multicast address and the anycast address are the same. The way the anycast address varies from other addresses is that it can deliver the same IP address to several servers or devices. Keep in mind that the hosts do not receive the IP address. Stated differently, multiple interfaces or a collection of interfaces are assigned an anycast address.

**IPSEC (IP Security)**

* IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections.
* IPSec enhances the protocol security by introducing encryption and authentication. IPSec encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data.

Some of the important aspects why IPSec is Important:

* IPSec protects the data through **Data Encryption.**
* IPSec provides **Data Integrity.**
* IPSec is often used in Virtual Private Networks (VPNs) to create secure, private connections.
* IPSec protects from **Cyber Attacks.**

**Features of IPSec**

* **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
* **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
* **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
* **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
* **Tunneling**: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
* **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
* **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

**Working of IPSec**

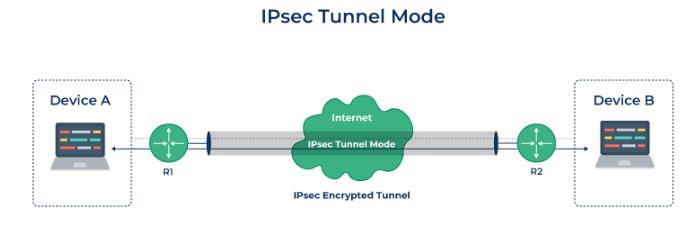
IPSec works by creating **secure connections** between devices, making sure that the information exchanged is kept safe from unauthorized access.

IPSec majorly operates in two ways i.e. **Transport Mode and Tunnel Mode.**

To provide security, IPSec uses two main protocols: **AH (Authentication Header) and ESP (Encapsulating Security Payload).** Both protocols are very useful as Authentication Header verifies the data that whether it comes from a **trusted source** and hasn’t been changed, and ESP has the work of performing **authentication and also encrypts** the data so that it becomes difficult to read.

For Encryption, IPSec uses cryptographic keys. It can be created and shared using a process called **IKE (Internet Key Exchange),** that ensures that both devices have the correct keys to establish a secure connection.

When two devices communicate using IPSec, the devices first initiate the connection by sending a request to each other. After that, they mutually decide on protection of data using passwords or digital certificates. Now, they establish the secure tunnel for communication. Once the tunnel is set up, data can be transmitted safely, as IPSec is encrypting the data and also checking the integrity of the data to ensure that data has not been altered. After the communication is finished, the devices can close the secure connection.



**IPSec Connection Establishment Process**

IPSec is a protocol suite used in securing communication using the Internet Protocol such that each packet communicated in the course of a particular session is authenticated and encrypted. The process of establishing an IPSec connection involves two main phases:

**Phase 1: Establishing the IKE (Internet Key Exchange) Tunnel**

In phase 1, the main aim is **to establish the secure channel the IKE tunnel**, which is used to further negotiations. Phase 1 can operate in one of two modes:

Main Mode: Main Mode is a **six-message exchange procedure** that is more secure than Basic Mode, although at the cost of a longer session, since identity information is transmitted during negotiations.

Aggressive Mode: Aggressive Mode takes lesser time with the exchange of **three messages** and is less secure since more information like identity is disclosed during the course of negotiation.

**Phase 2: Establishing the IPSec Tunnel**

Phase 2 is called Quick Mode and its aim is **to negotiate the IPSec Security Associations** after the construction of a secure IKE tunnel has been made. There are two modes in Phase 2.

Tunnel Mode: This mode encapsulates t**he whole of the original IP packet including the header and data.** It is mostly deployed in the site to site VPNs.

Transport Mode: By this mode, **only the actual data to be transmitted is encrypted and the header part of the IP packets remain unaltered.** It is mainly employed in end to end communication between hosts.

**Difference Between IPSec Tunnel Mode and IPSec Transport Mode**

The IPSec tunnel mode is appropriate for sending data over public networks because it improves data security against unauthorised parties. The computer encrypts all data, including the payload and header, and adds a new header to it.

IPSec transport mode encrypts only the data packet’s payload while leaving the IP header unchanged. The unencrypted packet header enables routers to determine the destination address of each data packet. As a result, IPSec transport is utilized in a closed and trusted network, such as to secure a direct link between two computers.

**Protocols Used in IPSec**

It has the following components:

1. **Encapsulating Security Payload (ESP):** It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. **Authentication Header (AH):** It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

3. **Internet Key Exchange (IKE):** It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.

**EIGRP:**

Enhanced Interior Gateway Routing Protocol (EIGRP) is a **dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet.** EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the **best path** between two layer 3 devices (router or layer 3 switches) operating EIGRP. Administrative Distance for EIGRP are:-

It uses some messages to communicate with the neighbour devices that operate EIGRP. These are:-

1. **Hello message-**These messages are **kept alive messages** which are exchanged between two devices operating EIGRP. These messages are used for **neighbour discovery/recovery**, if there is any device operating EIGRP or if any device (operating EIGRP) coming up again.   
   These messages are used for **neighbor discovery if multicast** at 224.0.0.10. It contains values like AS (Autonomous System) number, k values, etc. These messages are used as **acknowledgement when unicast**. A hello with no data is used as the acknowledgement.
2. **NULL update-**It is used to calculate SRTT(Smooth Round Trip Timer) and RTO(Retransmission Time Out).   
   *SRTT:* The time is taken by a packet to reach the neighboring router and the acknowledgement of the packet to reach the local router.

*RTO:*If a multicast fails then unicast is being sent to that router. RTO is the time for which the local router waits for an acknowledgement of the packet.

1. **Full Update –**After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.
2. **Partial update-**These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.
3. **Query message-**These messages are multicast when the device is declared dead and it has no routes to it in its topology table.
4. **Reply message –**These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
5. **Acknowledgement message**   
   It is used to acknowledge EIGRP updates, queries, and replies. Acks are hello packets that contain no data.

**Note:-**Hello and acknowledgment packets do not require any acknowledgment.   
Reply, query, update messages are reliable messages i.e require acknowledgement.

**Composite matrix-**The EIGRP composite metric calculation can use up to 5 variables, but only 2 are used by default (K1 and K3). The composite metric values are :

***K1 (bandwidth)***  
***K2 (load)***  
***K3 (delay)***  
***K4 (reliability)***  
***K5 (MTU)***

The lowest bandwidth, load, delay, reliability, MTU (maximum transmission unit) along the path between the source and the destination is considered in the composite matrix in order to calculate the cost.   
**Note:-** Generally, only k1 and k3 values are used for metric calculation by EIGRP. The values are 10100 for k1, k2, k3, k4, k5 respectively.

To form EIGRP neighbourship, these criteria should be fulfilled:- 

1. k values should match.
2. Autonomous system number should match. (AS is a group of networks running under a single administrative control) .
3. authentication should match (if applied).
4. subnet mask should be the same.

**Internet Control Message Protocol**

* ICMP is used for **reporting errors and management queries.** It is a supporting protocol and is used by network devices like **routers for sending error messages and operations information.**
* Since the IP protocol lacks an error-reporting or [error-correcting](https://www.geeksforgeeks.org/error-correction-in-computer-networks/) mechanism, information is communicated via a message. For instance, when a message is sent to its intended recipient, it may be intercepted along the route from the sender. The sender may believe that the communication has reached its destination if no one reports the problem. If a middleman reports the mistake, **ICMP helps in notifying the sender about the issue.**
* For example, if a message can’t reach its destination, if there’s network congestion, or if packets are lost, ICMP sends back feedback about these issues. This feedback is essential for diagnosing and fixing network problems, making sure that communication can be adjusted or rerouted to keep everything running smoothly.

## Uses of ICMP

ICMP is used for **error reporting** if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error.

Another important use of ICMP protocol is used to perform **network diagnosis** by making use of traceroute and ping utility.

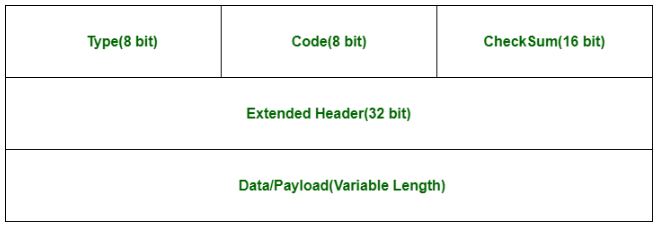
* **Traceroute:** [Traceroute](https://www.geeksforgeeks.org/traceroute-in-network-layer/) utility is used to know **the route between two devices connected over the internet.** It routes the journey from one router to another, and a traceroute is **performed to check network issues** before data transfer.
* **Ping:** [Ping](https://www.geeksforgeeks.org/what-is-ping/) is a simple kind of traceroute known as the **echo-request message**, it is used to **measure the time taken by data to reach the destination and return to the source,** these replies are known as echo-replies messages.

**Working of ICMP**

* ICMP is the primary and important protocol of the IP suite, but ICMP isn’t associated with any transport layer protocol [(TCP or UDP)](https://www.geeksforgeeks.org/differences-between-tcp-and-udp/) as **it doesn’t need to establish a connection with the destination device before sending any message as it is a connectionless protocol.**
* The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a [TCP Handshake](https://www.geeksforgeeks.org/tcp-3-way-handshake-process/).
* **ICMP packets are transmitted in the form of datagrams that contain an IP header** with ICMP data. ICMP datagram is similar to a packet, which is an independent data entity.

## ICMP Packet Format

In the ICMP packet format, the first 32 bits of the packet contain three fields:



* **Type (8-bit):** The initial 8-bit of the packet is for message type**, it provides a brief description of the messag**e so that receiving network would know what kind of message it is receiving and how to respond to it. Some common message types are as follows:
* Type 0 – Echo reply
* Type 3 – Destination unreachable
* Type 5 – Redirect Message
* Type 8 – Echo Request
* Type 11 – Time Exceeded
* Type 12 – Parameter problem
* **Code (8-bit**): Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type.
* **Checksum (16-bit):** Last 16 bits are for the checksum field in the ICMP packet header. **The**[**checksum**](https://www.geeksforgeeks.org/error-detection-code-checksum/)**is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.**
* The next 32 bits of the ICMP Header are Extended Header **which has the work of pointing out the problem in IP Message.**
* The last part of the ICMP packet is Data or Payload of variable length. The bytes included in IPv4 are 576 bytes and in IPv6, 1280 bytes.

## ICMP in DDoS Attacks

In [Distributed DOS (DDoS)](https://www.geeksforgeeks.org/what-is-ddosdistributed-denial-of-service/) attacks, attackers provide so much extra traffic to the target, so that it cannot provide service to users. There are so many ways through which an attacker executes these attacks, which are described below.

## Ping of Death Attack

**Whenever an attacker sends a ping, whose size is greater than the maximum allowable size, oversized packets are broken into smaller parts.** When the sender re-assembles it, **the size exceeds the limit which causes a**[**buffer overflow**](https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/)**and makes the machine freeze.** This is simply called a [Ping of Death Attack](https://www.geeksforgeeks.org/ping-flood-attack/). Newer devices have protection from this attack, but older devices did not have protection from this attack.

## ICMP Flood Attack

Whenever **the sender sends so many pings that the device on whom the target is done is unable to handle the echo request.** This type of attack is called an [ICMP Flood Attack](https://www.geeksforgeeks.org/icmp-flood-ddos-attack/). This attack is also called a **ping flood attack**. It stops the target computer’s resources and causes a denial of service for the target computer.

**IGMP(Internet Group Management Protocol)**

* IGMP is an 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.

**Applications:**

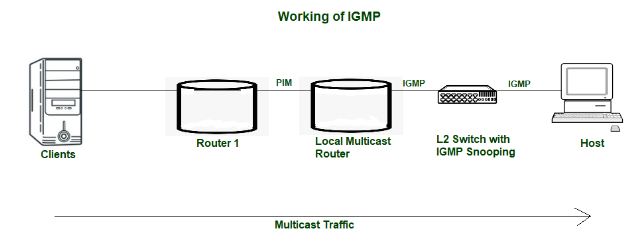
* Streaming – Multicast routing protocols are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.
* Gaming – Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.
* Web Conferencing 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.

**The IGMP uses several types of messages to manage multicast group memberships:**

* **IGMP Membership Query:** The Sent by routers to determine which multicast groups have members on a particular network segment. This query helps routers maintain accurate multicast group membership information.
* **IGMP Membership Report:** Sent by hosts to indicate their interest in joining a multicast group. This report informs the router of the presence of a host that wants to receive multicast traffic.
* **IGMP Leave Group:** Sent by hosts to indicate that they are leaving a multicast group. This message informs the router that the host no longer wants to receive traffic for that group.
* **IGMP V3 Membership Report (in IGMPv3):** This allows hosts to specify the exact multicast group addresses they want to join or leave and can include source-specific multicast (SSM) information.

**Working of IGMP**

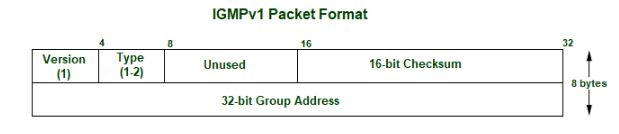
* IGMP works on devices that are capable of handling multicast groups and dynamic multicasting. These devices allow the host to join or leave the membership in the multicast group. These devices also allow to add and remove clients from the group.
* This communication protocol is operated between the host and the local multicast router. When a multicast group is created, the multicast group address is in the range of class D (224-239) [IP addresses](https://www.geeksforgeeks.org/what-is-an-ip-address/) and is forwarded as the 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.

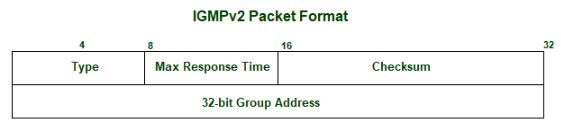
**Versions of IGMP**

**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 sum of IGMP messages.
* 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

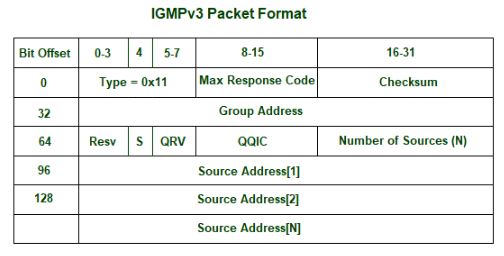
0x16 for IGMPv2 Membership Report

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 sum of IGMP message. It determines the entire payload of the IP datagram in which IGMP message is encapsulated.
* Group Address – It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries. The behavior of this field depends on the type of the message sent.

**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.

## Open Shortest Path First

* Open Shortest Path First (OSPF) is an IP routing protocol **that uses a mathematical algorithm** to calculate the most efficient path to direct traffic on IP networks. OSPF is an open standard and designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) within the family of TCP/IP protocols.
* Based on link-state or shortest path first (SPF) technology, **OSPF distributes routing information between routers in a single autonomous system (AS).** This capability differentiates OSPF from older TCP/IP routing protocols, which were designed for less complex networks than those used today.
* Using **Dijkstra's shortest path algorithm,** OSPF calculates the shortest path for all routers in an area of the AS to efficiently use network bandwidth and ensure scalability. **The AS may be divided into multiple interconnected networks, such as a wide area network (WAN).** The topology is visible only to the routers in the same area.
* As a dynamic routing protocol, **OSPF not only routes IP packets based on the destination IP address (given in the packet header), but it also detects topological changes in the AS.** After detecting changes, **OSPF calculates new, loop-free routes** after a short period (known as convergence time) in which routing traffic is kept to a minimum.
* All the routers in the same area of the OSPF network maintain the same **link-state database that** describes the area topology. Each router receives **link-state advertisement (LSA) messages** containing information about neighboring routers and path costs from the other routers in that area. Using these LSAs, each router generates the link-state database and uses the SPF algorithm to calculate a shortest-path spanning tree.

## Working of Open Shortest Path First

Two important concepts in OSPF are areas and neighbors.

* **Areas are groups of routers in an AS, essentially forming a collection of zones with logical boundaries.** Areas are typically identified with a number. **Area 0** is always the backbone, to which all other areas connect.
* OSPF-enabled routers in the **same area establish "neighbor" relationships using a**[**HELLO packet**](https://www.techtarget.com/searchnetworking/definition/HELLO-packet)**to exchange routing information.**
* In OSPF, the routers do not need to send the entire [routing table](https://www.techtarget.com/searchnetworking/definition/routing-table) to neighboring routers every few seconds. Instead, **information is sent only when a change has taken place.**
* When an OSPF router in a given area of the AS that learns of a **routing table change or detects a change** in the network immediately [multicasts](https://www.techtarget.com/searchnetworking/definition/multicast) **the information to all other OSPF-enabled nodes in the area. Multicasting is a way to ensure every router in that area has the same information about the AS topology, a concept known as**[**flooding**](https://www.techtarget.com/searchnetworking/definition/flooding)**.** This information is used to calculate the best end-to-end path to the eventual destination in the AS.
* Notably, **the multicast contains only the latest update**. Routing tables can be incredibly large, and retransmitting them in full every time can degrade network performance. When routes change -- which can occur due to equipment failure or the addition of new devices -- the time it takes OSPF routers to reconcile these changes and identify the best new, loop-free path between endpoints is called convergence time.

## RPL

* RPL stands for Routing Protocol for Low Power and Lossy Networks for heterogeneous traffic networks. It is a routing protocol for **Wireless Networks.** This protocol is based on the same standard as by Zigbee and 6 Lowpan is IEEE 802.15.4 **It holds both many-to-one and one-to-one communication.**
* It is a Distance Vector Routing Protocol that **creates a tree-like routing topology** called the Destination Oriented Directed Acyclic Graph (DODAG), rooted towards one or more nodes called the root node or sink node.
* The Directed Acyclic Graphs (DAGs) are **created based on user-specified specific Objective Function (OF)**. The OF defines the method **to find the best-optimized route among the number of sensor devices.**
* RPL is based on the concept of a Directed Acyclic Graph (DAG). **A DAG is Directed Graph where no cycle exists.** This means that from any vertex or point in the graph, we cannot follow an edge or a line back to this same point. All of the edges are arranged in a path oriented toward and terminating at one or more root nodes.
* A basic RPL process involves building a Destination Oriented Directed Acyclic Graph (DODAG). A DODAG is a DAG rooted in one destination. **In RPL this destination occurs at a border router known as the DODAG root**. In a DODAG, **three parents maximum a**re maintained by each node that provides a path to the root. Typically one of these parents is the preferred parent, which means it is the preferred next hop for upward roots towards the root. The routing graph created by the set of DODAG parents across all nodes defines the full set of upwards roots. RPL protocol information should ensure that routes are **loop-free** by disallowing nodes from selected DODAG parents positioned further away from a border router.

## Main Features and Advantages of RPL

The IPv6 Routing Protocol for RPL, is an efficient and effective protocol for data routing in resource-constrained scenarios, such Internet of Things devices as per requirement. Its many essential features include the below points:

* **Scalability:** The protocol can accommodate such type of big networks with low power and lossy connectivity, which makes it appropriate for a range of Internet of Things applications.
* **Multipoint-to-point traffic generation:** RPL offers a way to send data to a single destination point from several devices within the LLN as per requirement.
* **Quality of Service (QoS)** – The protocol guarantees QoS by offering various types of methods for reliable packet delivery system and congestion control systetm.
* **Adaptive** – RPL modifies the required routes in response to link quality and energy availability changes in the network environment or system.
* **Security system:** To guarantee various types of secure communication within the LLN as per requirement, RPL incorporates techniques for integrity protection, authentication, confidentiality, and encryption for better performance.

**TCP (Transmission Control Protocol)**

Transmission Control Protocol (TCP) **is a connection-oriented protocol for communications** that helps in the exchange of messages between different devices over a network. It is one of the main protocols of the TCP/IP suite. In OSI model, it operates **at the transport layer(Layer 4**). It lies **between the Application and Network Layers** which are used in providing reliable delivery services. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

TCP establishes a reliable connection between sender and receiver using the three-way handshake (SYN, SYN-ACK, ACK) and it uses a four-step handshake (FIN, ACK, FIN, ACK) to close connections properly.

* It ensures error-free, in-order delivery of data packets.
* It uses acknowledgments (ACKs) to confirm receipt.
* It prevents data overflow by adjusting the data transmission rate according to the receiver’s buffer size.
* It prevents network congestion using algorithms like Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery.
* TCP header uses checksum to detect corrupted data and requests retransmission if needed.
* It is used in applications requiring reliable and ordered data transfer, such as web browsing, email, and remote login.

**Working of Transmission Control Protocol (TCP)**

* Transmission Control Protocol (TCP) **model breaks down the data into small bundles and afterward reassembles the bundles into the original message on the opposite end to make sure that each message reaches its target location intact**. Sending the information in little bundles of information makes it simpler to maintain efficiency as opposed to sending everything in one go.
* **After a particular message is broken down into bundles, these bundles may travel along multiple routes if one route is jammed but the destination remains the same.**
* Now, **the TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer.** The packets are then sent to the destination through different routes.
* **The TCP layer in the user’s system waits for the transmission to get finished and acknowledges once all packets have been received.**

**Features of TCP**

Some of the most prominent features of Transmission control protocol are mentioned below.

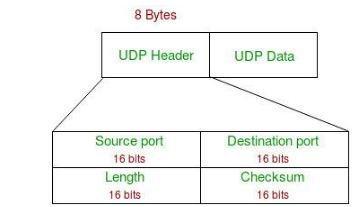
* **Segment Numbering System:** **TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.** A specific **Byte Number** is assigned to **data bytes** that are to be transferred while **segments are assigned sequence numbers**. Acknowledgment Numbers are assigned to received segments.
* **Connection Oriented**: It means sender and receiver **are connected to each other till the completion of the process.** The order of the data is maintained i.e. order remains same before and after transmission.
* **Full Duplex:** In TCP data can be transmitted from receiver to the sender or vice – versa at the same time. It increases efficiency of data flow between sender and receiver.
* **Flow Control**: Flow **control limits the rate at which a sender transfers data**. This is done to ensure reliable delivery. The receiver continually hints to the sender on how much data can be received (using a sliding window).
* **Error Control:** TCP implements an **error control mechanism** for reliable data transfer. Error control is byte-oriented. Segments are checked for error detection. **Error Control includes – Corrupted Segment & Lost Segment Management, Out-of-order segments, Duplicate segments, etc.**
* **Congestion Control:** TCP takes into account the level of congestion in the network. Congestion level is determined by the amount of data sent by a sender.

## User Datagram Protocol

User Datagram Protocol (UDP) is one of the core protocols of the Internet Protocol (IP) suite. **It is a communication protocol used across the internet for time-sensitive transmissions such as video playback or**[**DNS lookups**](https://www.geeksforgeeks.org/dns-look-up/)**.** Unlike Transmission Control Protocol (TCP), UDP is **connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.**

## UDP Header

UDP header is an **8-byte**fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. **The first 8 Bytes contain all necessary header information and the remaining part consists of data.** UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



* **Source Port:** Source Port is a 2 Byte long field used to identify the [port number](https://www.geeksforgeeks.org/what-is-ports-in-networking/)of the source.
* **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
* **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
* **Checksum:** Checksum is 2 Bytes long field. **It is the 16-bit one’s complement of the one’s complement sum of the UDP header**, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

## Applications of UDP

* Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
* It is a suitable protocol **for multicasting as UDP supports packet switching**.
* UDP is used for some routing update protocols like[RIP(Routing Information Protocol).](https://www.geeksforgeeks.org/routing-information-protocol-rip/)
* Normally used **for real-time applications which can not tolerate uneven delays between sections of a received message.**
* [VoIP (Voice over Internet Protocol)](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/) services, **such as Skype and WhatsApp, use UDP** for real-time voice communication. The delay in voice communication can be noticeable if packets are delayed due to congestion control, so UDP is used to ensure fast and efficient data transmission.
* [**DNS (Domain Name System)**](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/)**also uses UDP for its query/response messages.** DNS queries are typically small and require a quick response time, making UDP a suitable protocol for this application.
* [**DHCP (Dynamic Host Configuration Protocol)**](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/)**uses UDP to dynamically assign IP addresses to devices on a network.** DHCP messages are typically small, and the delay caused by packet loss or retransmission is generally not critical for this application.

## TCP vs UDP

| Basis | Transmission Control Protocol (TCP) | User Datagram Protocol (UDP) |
| --- | --- | --- |
| Type of Service | [TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/)is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data. | [UDP](https://www.geeksforgeeks.org/user-datagram-protocol-udp/)is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission. |
| Reliability | TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| Error checking mechanism | TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data. | UDP has only the basic error-checking mechanism using checksums. |
| Acknowledgme nt | An acknowledgment segment is present. | No acknowledgment segment. |
| Sequence | Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| Speed | TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| Retransmission | Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| Header Length | TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| Weight | TCP is heavy-weight. | UDP is lightweight. |
| Handshaking Techniques | Uses handshakes such as SYN, ACK, SYN-ACK | It’s a connectionless protocol i.e. No handshake |
| Broadcasting | TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |
| Protocols | TCP is used by [HTTP, HTTPs](https://www.geeksforgeeks.org/difference-between-http-and-https-2/), [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/), [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/)and [Telnet](https://www.geeksforgeeks.org/introduction-to-telnet/). | UDP is used by DNS, DHCP, TFTP, [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/), RIP, and VoIP. |
| Stream Type | The TCP connection is a byte stream. | UDP connection is a message stream. |
| Overhead | Low but higher than UDP. | Very low. |
| Applications | This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services. | This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc. |

**Network and Service Layer in IoT: Use Cases and Services**

The **Network Layer** and **Service Layer** play crucial roles in the Internet of Things (IoT) architecture, enabling connectivity, communication, and intelligent processing. Let's explore their functions, use cases, and services.

**1. Network Layer in IoT**

The **Network Layer** is responsible for transmitting data between IoT devices, gateways, cloud platforms, and user interfaces. It ensures reliable communication using various networking technologies.

**Functions of the Network Layer**

* Data transmission between IoT devices and cloud/server.
* Routing and addressing of data packets.
* Handling different network protocols (IP, MQTT, CoAP, LoRaWAN, etc.).
* Ensuring secure communication using encryption methods.
* Managing mobility and scalability of IoT devices.

**Use Cases of the Network Layer**

1. **Smart Homes:** IoT devices like smart thermostats, security cameras, and voice assistants communicate via Wi-Fi, Zigbee, or Bluetooth.
2. **Industrial IoT (IIoT):** Wireless sensor networks (WSN) in manufacturing plants use industrial protocols like WirelessHART and ISA100.11a.
3. **Smart Agriculture:** IoT sensors collect soil moisture and temperature data, transmitting it over LPWAN (LoRa, NB-IoT) for precision farming.
4. **Healthcare Monitoring:** Wearable devices send real-time patient health data to cloud-based servers via 5G or Wi-Fi.
5. **Smart Cities:** Traffic monitoring systems use cellular or LPWAN to send vehicle flow data for optimizing city traffic.

**Services Provided by the Network Layer**

* **Device Connectivity:** Ensures seamless communication between devices and servers.
* **Protocol Translation:** Converts data between different communication standards (MQTT, CoAP, HTTP).
* **Data Security:** Uses encryption (TLS, DTLS) to protect transmitted data.
* **Network Management:** Optimizes bandwidth, energy consumption, and network topology.
* **Routing & Addressing:** Assigns unique identifiers (IP addresses) to IoT devices.

**2. Service Layer in IoT**

The **Service Layer** is responsible for processing and analyzing IoT data, providing meaningful insights and automation. It acts as a bridge between the network and application layers.

**Functions of the Service Layer**

* **Data Processing & Storage:** Aggregates, filters, and stores IoT data for further analysis.
* **Security & Authentication:** Ensures only authorized devices and users access the IoT system.
* **AI & Analytics Integration:** Uses machine learning (ML) and artificial intelligence (AI) for predictive insights.
* **Interoperability:** Facilitates seamless communication between different IoT platforms and devices.
* **Device & Service Management:** Monitors device health, firmware updates, and fault detection.

**Use Cases of the Service Layer**

1. **Predictive Maintenance:** AI-powered analytics predict equipment failures in industries, reducing downtime.
2. **Smart Healthcare:** Patient health data is analyzed to detect anomalies and alert doctors.
3. **Autonomous Vehicles:** Cloud-based AI processes vehicle sensor data for real-time decision-making.
4. **Energy Management:** IoT platforms analyze power consumption data to optimize energy usage.
5. **Supply Chain Optimization:** AI-driven IoT systems monitor logistics and warehouse inventory in real time.

**Services Provided by the Service Layer**

* **Data Aggregation & Filtering:** Reduces redundant data and optimizes storage.
* **Real-Time Processing:** Enables instant decision-making in critical applications.
* **Device Authentication & Security:** Uses encryption, authentication, and role-based access control.
* **Machine Learning & AI Integration:** Predicts trends, detects anomalies, and optimizes operations.
* **APIs for Application Development:** Provides APIs for integrating IoT data into third-party apps