# Network Layer Protocols

## ❖ 1.1Network Layer Protocol

- Network layer protocols are a vital part of the internet infrastructure, **responsible for routing and forwarding data packets** between devices on a network. These protocols are used to ensure that data is delivered to the correct destination and in a timely manner.

  - **There are several network layer protocols that are commonly used, each serving a specific purpose.**

- **Internet Protocol (IP):** This protocol is responsible for addressing and routing data packets across the internet. It works by assigning a unique numerical address, called an IP address, to each device on a network. This allows data packets to be forwarded to the correct device based on the IP address.
- **Internet Control Message Protocol (ICMP):** This protocol is used to transmit error messages and other information between devices on a network. It is often used to troubleshoot network issues or to send diagnostic information.
- **Address Resolution Protocol (ARP):** This protocol is used to map IP addresses to physical addresses, such as a device's media access control (MAC) address. This allows devices to communicate with each other on a network.
- **Routing Information Protocol (RIP):** The Routing Information Protocol (RIP) is another network layer protocol that is used to determine the best path for data packets to travel between devices on a network. It works by sending updates to other devices on the network, allowing them to update their routing tables and determine the best route for data packets.
- **Open Shortest Path First (OSPF) protocol:** This is a routing protocol that is used in large networks, such as enterprise networks or internet service providers. It works by using a link-state database to determine the best route for data packets and can quickly adapt to changes in the network.

## ❖ 1.2 IPV4 Addresses

### Address space

- An address space is a range of logical space on any part of a computer or peripheral device where data can be stored. For instance, on a memory chip, each byte of data has its own address whereit can be stored and then located later. The address can be limited by the physical limitations of the device, and arbitrary limits that separate certain types of data from one another.

### Classful addressing

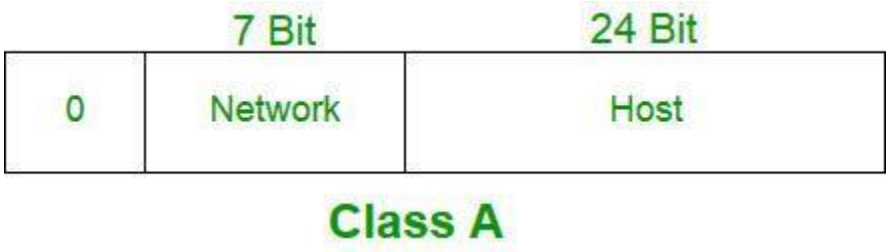
- Classful addressing is an IPv4 addressing architecture that divides addresses into five groups. Prior to classful addressing, the first eight bits of an IP address defined the network a given host was a part of. This would have had the effect of limiting the internet to just 254 networks.
- The 32-bit IP address is divided into five sub-classes.

**These are:**

1. **Class A**
2. **Class B**
3. **Class C**
4. **Class D**
5. **Class E**

### 1. Class A

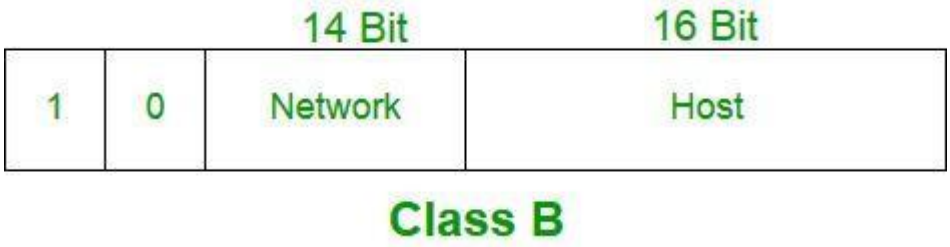
- IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine 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 subtracted 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 A

### 2. Class B

- IP address belonging to class B is assigned to networks that range 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 the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet 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.

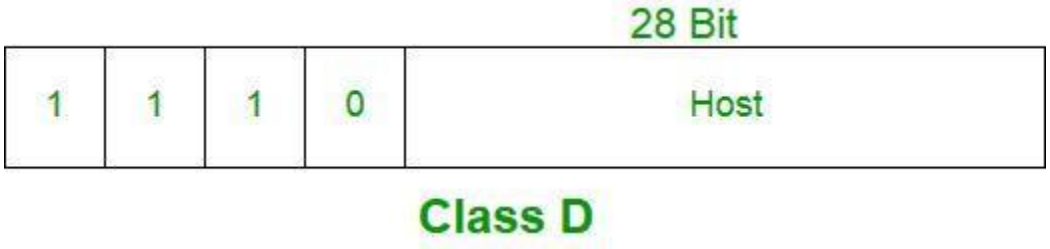



**3. Class C**

- IP addresses 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 is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet 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 range from 192.0.0.x – 223.255.255.x.

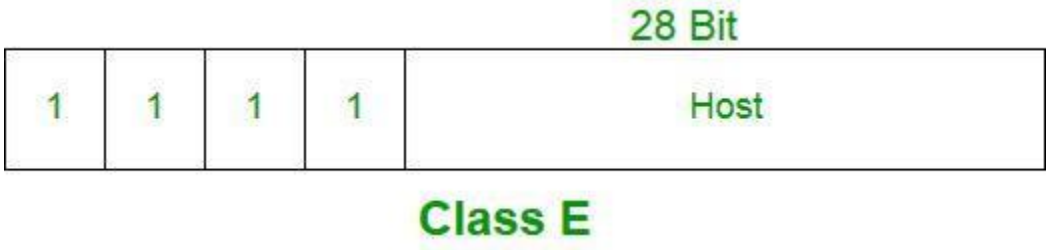

**4. Class D**

- IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



**5. Class E**

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the 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 IDs are used to identify a host within a network. The host ID is assigned based on the following rules:
- Within any network, the host ID must be unique to that network.
- A 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 the class A address and is reserved for internal loopback 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

| CLASS | LEADING BITS | NET ID BITS | HOST ID BITS | NO. OF NETWORKS | ADDRESSES PER NETWORK | START ADDRESS | END ADDRESS |
|---|---|---|---|---|---|---|---|
| CLASS A | 0 | 8 | 24 | $2^7$ ( 128 ) | $2^{24}$ (16,777,216) | 0.0.0.0 | 127.255.255.255 |
| CLASS B | 10 | 16 | 16 | $2^{14}$ ( 16,384 ) | $2^{16}$ ( 65,536 ) | 128.0.0.0 | 191.255.255.255 |
| CLASS C | 110 | 24 | 8 | $2^{21}$ ( 2,097,152 ) | $2^8$ ( 256 ) | 192.0.0.0 | 223.255.255.255 |
| CLASS D | 1110 | NOT DEFINED | NOT DEFINED | NOT DEFINED | NOT DEFINED | 224.0.0.0 | 239.255.255.255 |
| CLASS E | 1111 | NOT DEFINED | NOT DEFINED | NOT DEFINED | NOT DEFINED | 240.0.0.0 | 255.255.255.255 |

### Problems with Classful Addressing

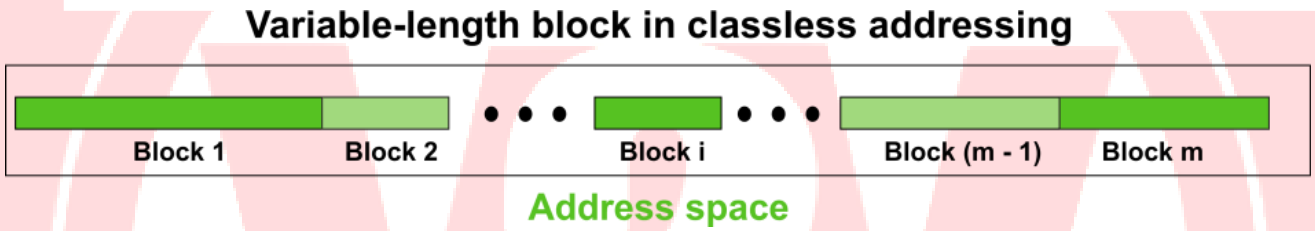
- The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routingand 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 the next post.
- The network ID is 24 bits long.
- The host ID is 8 bits long.
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address
- 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.
- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback 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.

### CLASSLESS ADDRESSING

- The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques.
- As the Internet expanded, it became obvious that a bigger address space was required as a long-term

fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax.

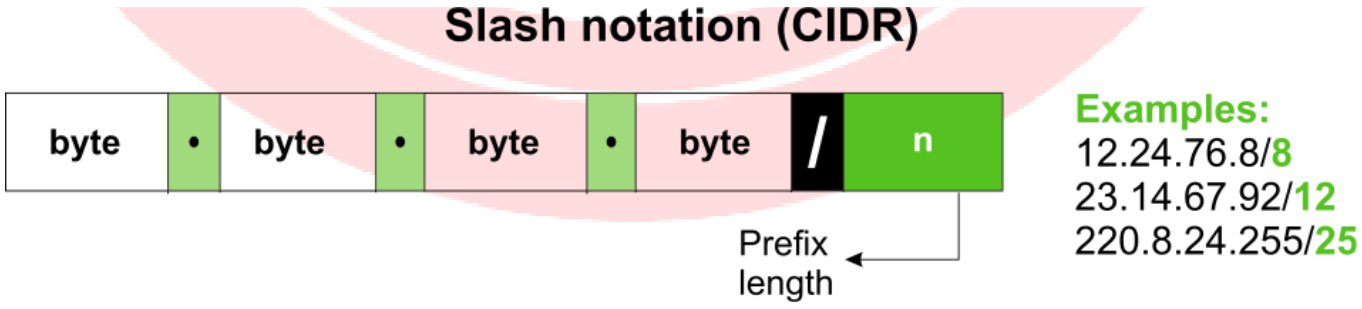
- The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. *Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses.*
- In order to make up for address depletion, the class privilege was taken out of the distribution.
- The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device).
- We are capable of having a block of 20, 21, 22 ,..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses.
- One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.




- In contrast to classful addressing, classless addressing allows for varying prefix lengths. Prefix lengths that vary from 0 to 32 are possible. The length of the prefix has an inverse relationship with network size. A smaller network has a large prefix; a larger one has a small prefix.
- We must stress that classful addressing is just as easily adaptable to the concept of classless addressing. Consider an address in class A as a classless address with a prefix length of 8. Class B addresses can be viewed as classless addresses with the prefix 16 and so on. Putting it another way, *classless addressing is a specific instance of classful addressing.*

*Prefix Length - Slash Notation*

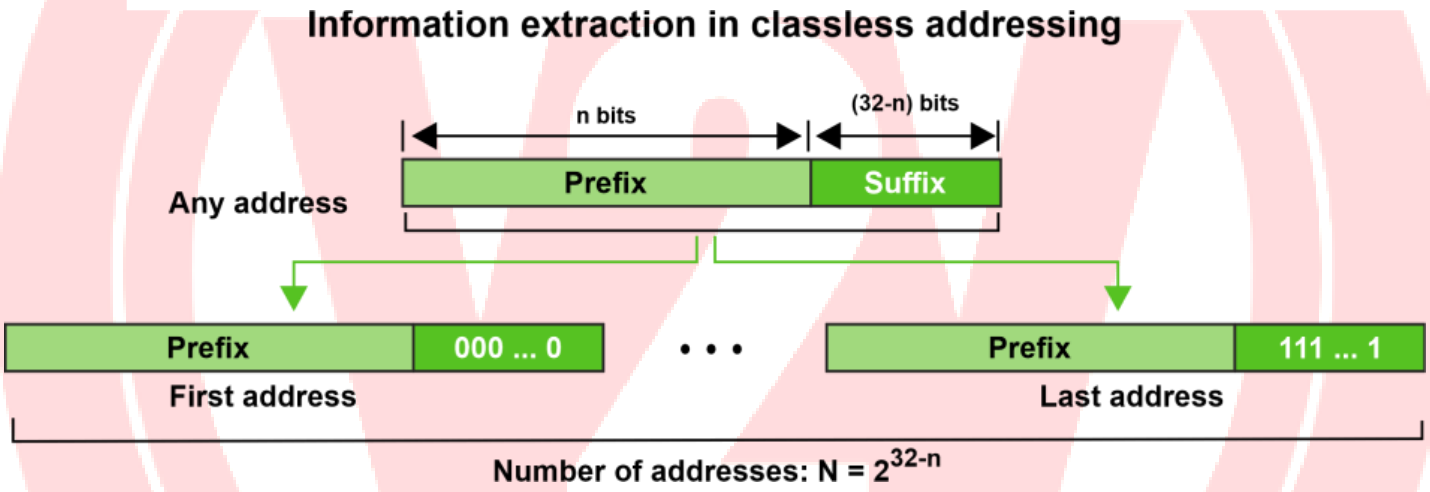
- In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n. Slash notation is the colloquial name for the notation, while classless inter domain routing or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.



- To put it another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

### Extracting Information from an Address

- With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n, is known.
- The block has N = 232n addresses, according to the calculation.
- The n leftmost bits are kept, and the (32 - n) rightmost bits are all set to zeroes to determine the first address.
- The n leftmost bits are kept, while the (32 - n) rightmost bits are all set to 1s to determine the last address.




***For Example*** - The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are $2^{32-n} = 2^5 = 32$ addresses in all.

The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.

**Address**: 167.199.170.82/27 10100111 11000111 10101010 01010010

**First address**: 167.199.170.64/27 10100111 11000111 10101010 01000000

*Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.*

**Address**: 167.199.170.82/27 10100111 11000111 10101010 01011111

**Last address**: 167.199.170.95/27 10100111 11000111 10101010 01011111

---

### Difference between Classful and Classless Addressing

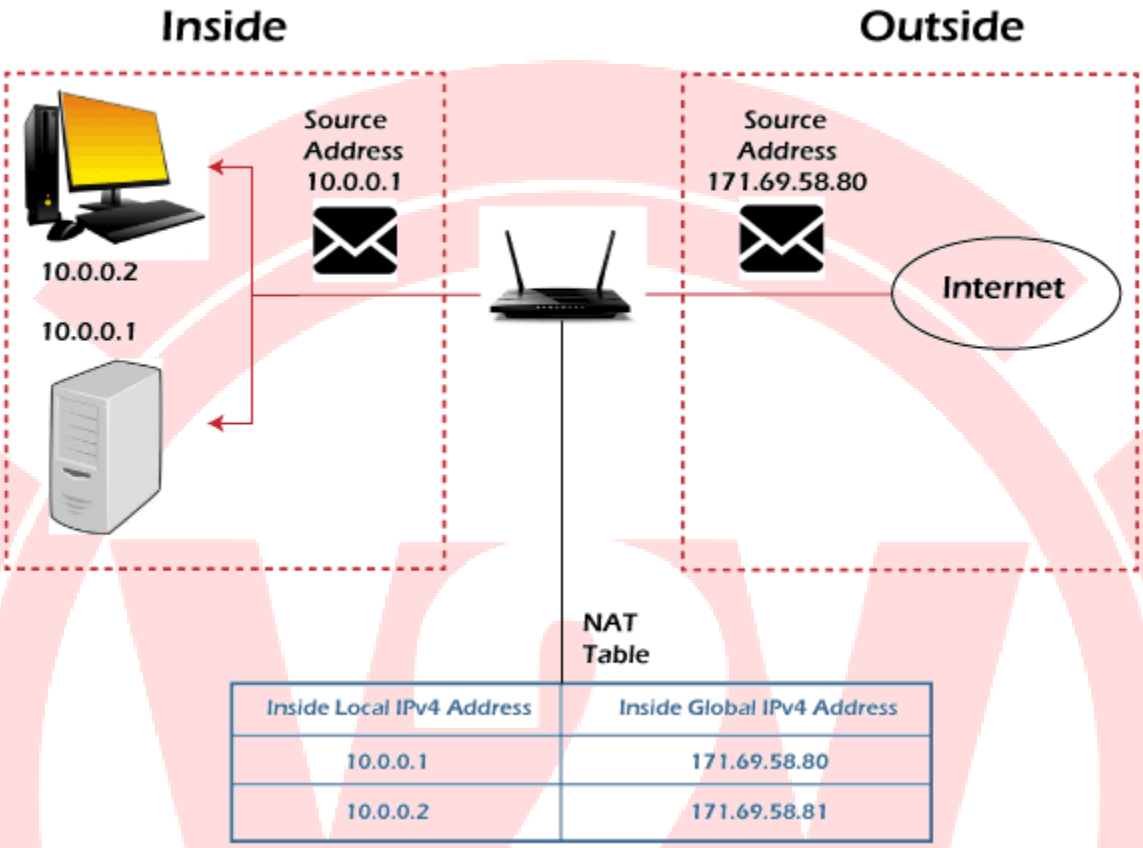
- IP addresses are divided into five groups using the classful addressing approach when they are assigned. In order to prevent the depletion of IP addresses, classless addressing is used. It is a method of IP address allocation that will eventually replace classful addressing.
- A further distinction is the usefulness of classful and classless addressing. Comparatively speaking, classless addressing is more beneficial and useful than classful addressing.
- In classful addressing, the network ID and host ID are adjusted according to the classes. However, the distinction between network ID and host ID does not exist with classless addressing. This opens up the possibility of making yet another contrast between both addressing.

### CONCLUSION

- IP addressing includes two types: classful and classless.
- Classless addressing offers a more effective method of allocating IP addresses than classful addressing, which is the main difference between the two.
- To put it briefly, classless addressing prevents the issue of IP address exhaustion that can occur with classful addressing.

### ➢ Network Address Resolution (Translation)

- **NAT (Network Address Translation)** connects two networks and maps the private (inside local) addresses into public addresses (inside global).
- Inside local denotes that the best address belonged to an internal network and was not assigned by a *Network Information Centre* or *service power*.
- The inside global signifies that the address is a valid address assigned by the **NIC** or service provider, and one or more inside local addresses to the outside world.




- NAT **is a method of converting a private IP address or a local address into a public IP address. NAT is a technique for reducing the rate at which available IP addresses are depleted by translating a local IP or private IP address into a global or public IP address. The NAT relation might be one-to-one or many-to-one.**
- **Furthermore, NAT can only configure one address in order to represent the entire network to the outside world. As a result, the translation process is transparent. NAT can be used to migrate and merge networks, share server loads, and create virtual servers, etc.**

**Types of NAT :**There are three types of NAT

1. **Static NAT**

   In static NAT, a local address is mapped to a global address. In this type of NAT, the relationship is one-to-one. Static NAT is used if a host needs a consistent address that must be acceded from the internet. For example, networking devices or enterprise servers.

2. **Dynamic NAT**

   Unregistered private IP addresses can be converted to registered public IP numbers from a pool of public IP addresses using dynamic NAT.

3. **Dynamic NAT**

Unregistered private IP addresses can be converted to registered public IP numbers from a pool of public IP addresses using dynamic NAT

- **Advantages of NAT**

The following are the advantages of NAT:

- NAT protects the public addresses that have been registered and slow down the IP address space exhaustion.
- Removes the address renumbering process that occurs when switching networks
- The occurrence of address overlap was significantly reduced.
- Increases flexibility of the connection establishment.

- **Disadvantages of NAT**

The following are the disadvantages of NAT:

- Lack of end-to-end traceability
- Certain applications are not compatible with NAT
- Switching path delays are the outcome of the translation

## ❖ 1.3 Forwarding of IP Packets

- The process of packet forwarding simply implies the forwarding of incoming packets to their intended destination.
- Internet is made up of generally two terms- Interconnection and Network. So, it is a connection to a large collection of networks. A packet that is to be forwarded may be associated with the same network as the source host or may belong to a destination host in a different network. Thus, it dependson the destination how much a packet may need to travel before arriving at its destination.
- The router is responsible for the process of packet forwarding. It accepts the packet from the origin host or another router in the packet's path and places it on the route leading to the target host.
- The routing table is maintained by the router which is used for deciding the packet forwarding.

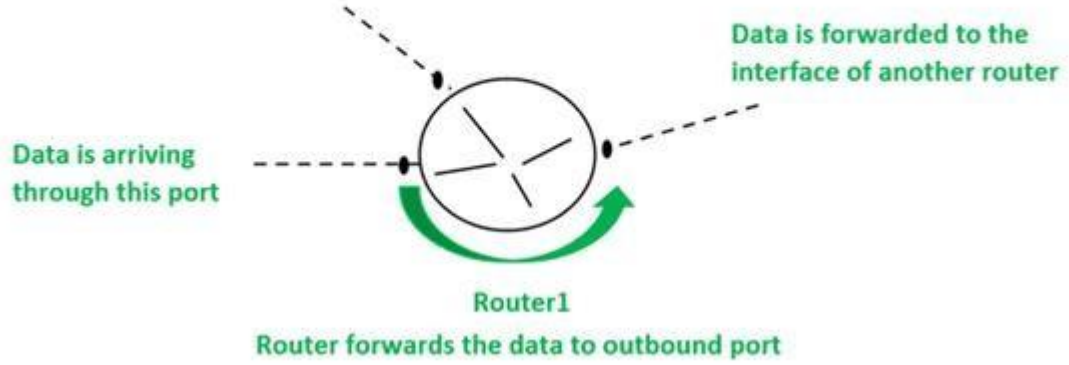
- **Packet Forwarding in Router:**

- Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves the packet forwarding from an entry interface out to an exit interface.

- **Working:**

- The following steps are included in the packet forwarding in the router-
- The router takes the arriving packet from an entry interface and then forwards that packet to another interface.

- The router needs to select the best possible interface for the packet to reach the intended destination as there exist multiple interfaces in the router.
- The forwarding decision is made by the router based on routing table entries. The entries in the routing table comprise destination networks and exit interfaces to which the packet is to be forwarded.
- The selection of exit interface relies on- firstly, the interface must lead to the target network to which the packet is intended to send, and secondly, it must be the best possible path leading to the destination network.



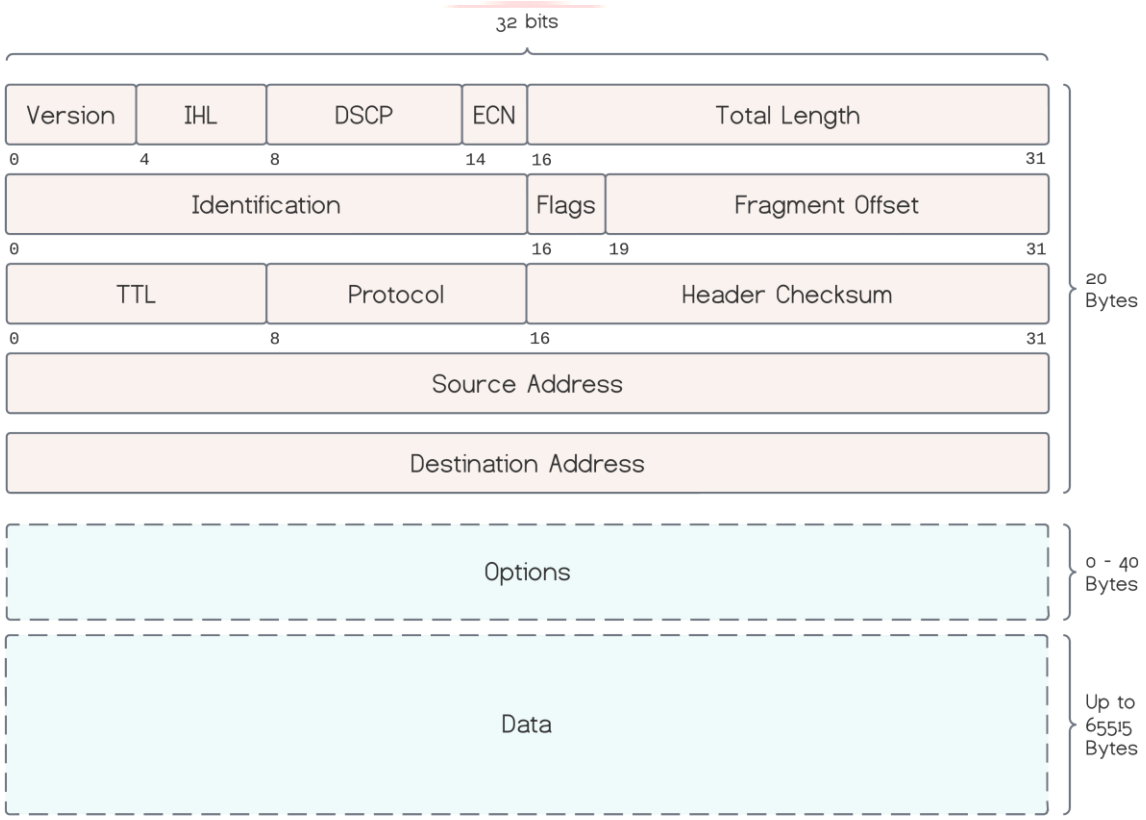

- **Forwarding based on destination address**

**Following are the packet forwarding techniques based on the destination host:**

- **Next-Hop Method:** By only maintaining the details of the next hop or next router in the packet's path, the next-hop approach reduces the size of the routing table. The routing table maintained using this method does not have the information regarding the whole route that the packet must take.
- **Network-Specific Method:** In this method, the entries are not made for all of the destination hosts in the router's network. Rather, the entry is made of the destination networks that are connected to the router.
- **Host-Specific Method:** In this method, the routing table has the entries for all of the destination hosts in the destination network. With the increase in the size of the routing table, the efficiency of the routing table decreases. It finds its application in the process of verification of route and security purposes.
- **Default Method:** Let's assume- A host in network N1 is connected to two routers, one of which (router R1) is connected to network N2 and the other router R2 to the rest of the internet. As a result, the routing table only has one default entry for the router R2.

## ❖ 1.4 Internet Protocol

- IPv4 was developed in 1981, and it's still widely used. It uses 32-bit address space.




### 1. Version

- IP version field set to 4 for IPv4.

### 2. Internet Header Length

- IHL is the number of 32-bit words making up the header field. As the first 20 bytes are mandatory, the minimum number is 5, and the maximum is 15.

### 3. Differentiated Services Code Point (DSCP)

- It specifies the type of service for differentiated services, such as voice-over IP.

**4. Explicit Congestion Notification (ECN)**

- ECN carries a network congestion notification without dropping packets or wasting bandwidth when supported.

**5. Total Length**

- It represents the total size of the datagram, including the header and the data segment.

**6. Identification**

- This field uniquely identifies the group of fragments of a single IP datagram.

**7. Flags**

- Different combinations of the flags control the fragmentation and indicate fragmented datagrams.
- For example, if the *don't fragment flag* (bit 1) is set to 1, and the destination host can't assemble the fragmented packets, it will drop them.

**8. Fragment Offset**

- It contains the offset of a fragmented packet.

**9. Time to Live (TTL)**

- The number of hops a packet lives. Each router decrements the TTL field and discards the packet when it reaches 0. This way, looping packets are eliminated.

**10. Protocol**

- It's the protocol for the data part.

**11. Header Checksum**

- It's a checksum for error detection, covering only the header field. Each router checks this value and discards the packet if an error is detected. Uncorrupted packets return 0 when summing the whole header, including the checksum itself.

**12. Source Address**

- Source host IPv4 address.

**13. Destination Address**

- Destination host IPv4 address.

**14. Options**

- Additional options are stored in this field when present.

### Security of IPv4 Datagrams

- Pv4 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.

## ❖ 1.5 ICMPv4

- Internet Control Message Protocol (ICMP) works in the network layer of the OSI model and the internet layer of the TCP/IP model. It is used to send control messages to network devices and hosts. Routers and other network devices monitor the operation of the network. When an error occurs, these devices send a message using ICMP. Messages that can be sent include "destination unreachable", "time exceeded", and "echo requests".
- ICMP is a network layer protocol.
- ICMP messages are not passed directly to the data link layer. The message is first encapsulated inside the IP datagram before going to the lower layer.

### Debugging tools

The following tools are used in debugging tools:

- **ICMP ping scan:** When checking any device on a network, the first thing that comes to mind is to test ICMP-based scanning. The way it works is that you send an ICMP request packet and expect ICMP echo to reply. The basic idea behind this is to get the live host on the network and then launch a port scanner against those live hosts. Angry IP Scanner is a very popular tool used for network scanning. The problem with ICMP is a network administrator can block ICMP on the network or host layers. You

can also easily create a script for an IP scanner which can scan IPs for their defined range.

- **TCP ping scan**: We have learned that ICMP can be blocked and is therefore not very reliable nowadays.

---

- **Packet Capture Tools (Wireshark, tcpdump)**: Packet capture tools can capture and analyze network traffic, including ICMP packets. This can help you diagnose issues at a more granular level.
- Example (using tcpdump):

```
tcpdump -i <interface> icmp
```

**Types of ICMP messages**

- **Packet Capture Tools (Wireshark, tcpdump): Packet capture tools can capture and analyze network traffic, including ICMP packets. This can help you diagnose issues at a more granular level.**
- **Example (using tcpdump):**
- **Query Message** − It helps a router or a network manager to get specific information from a router or another host.

```
tcpdump -i <interface> icmp
```

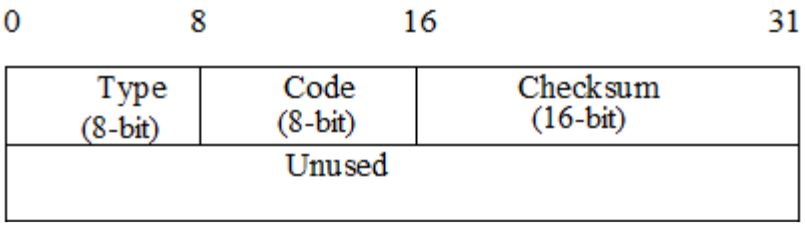
| Category | Type | Message |
|---|---|---|
| **Error-Reporting Messages** | 3 | Destination unreachable |
| | 4 | Source quench |
| | 11 | Time Exceeded |
| | 12 | Parameter Problem |

| | | |
|---|---|---|
| | 5 | Redirection |
| **Query Message** | 8 or 0 | Echo request or reply |
| | 13 or 14 | Timestamp request or reply |
| | 17 or 18 | Address mask request or reply |
| | 10 or 9 | Router Solicitation or advertisement |

- **Source Quench** − It requests to decrease the traffic rate of message sending from source to destination.
- **Time Exceeded** − When fragments are lost in a network the fragments hold by the router will be dropped and then ICMP will take the source IP from the discarded packet and inform the source, that datagram is discarded due to the time to live field reaches zero, by sending time exceeded message.
- **Fragmentation Required** − When a router is unable to forward a datagram because it exceeds the MTU of the next-hop network and the DF (Don't Fragment) bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating fragmentation is needed and DF (Don't Fragment) set.
- **Destination Unreachable** − This error message indicates that the destination host, network, or port number that is specified in the IP packet is unreachable. This may happen due to the destination host device is down, an intermediate router is unable to find a path to forward the packet, and a firewall is configured to block connections from the source of the packet.
- **Redirect Message** − A redirect error message is used when a router needs to tell a sender that it should use a different path for a specific destination. It occurs when the router knows a shorter path to the destination.

### ICMP Basic Error Message Format

A basic ICMP error message would have the following format −




- **Type** − The type field identifies the type of the message.

- **Code** − The code field in ICMP describes the purpose of the message.
- **Checksum** − The checksum field is used to validate ICMP messages.

---

### ICMP checksum

- **Message Data:** The ICMP checksum covers the entire ICMP message, including the ICMP header and any data payload. The data payload can vary depending on the type and code of the ICMP message. For example, in an ICMP Echo Request (ping) packet, the data payload typically includes a sequence number and a timestamp.
- **Pseudo-Header:** In addition to the ICMP message itself, the checksum calculation includes a pseudo-header, which is derived from the IP packet header of the packet carrying the ICMP message. This pseudo-header includes the source IP address, destination IP address, and a fixed field (all set to 0x00) for protocol type (ICMP).
- **Calculation:** To calculate the checksum, the data in the ICMP message and the pseudo-header is treated as a series of 16-bit words. The checksum is initially set to 0x0000. Then, each 16-bit word is added to the checksum, and any overflow from the addition is wrapped around. Finally, the checksum is complemented (bitwise NOT) to get the final checksum value.
- **Placement:** The calculated checksum value is then placed in the ICMP checksum field within the ICMP header.

---