


# The Network Layer – Unit 4

## Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.



Computer networks that provide connection-oriented services are called Virtual Circuits while those providing connection-less services are called Datagram networks.

## Virtual Circuits:

- 1.It is connection-oriented, meaning that there is a reservation of resources like buffers, CPU, bandwidth, etc. for the time in which the newly setup VC is going to be used by a data transfer session.
- 2.The first sent packet reserves resources at each server along the path. Subsequent packets will follow the same path as the first sent packet for the connection time.
- 3.Since all the packets are going to follow the same path, a global header is required. Only the first packet of the connection requires a global header, the remaining packets generally don't require global headers.
- 4.Since all packets follow a specific path, packets are received in order at the destination.
- 5.Virtual Circuit Switching ensures that all packets successfully reach the Destination. No packet will be discarded due to the unavailability of resources.
- 6.From the above points, it can be concluded that Virtual Circuits are a highly reliable method of data transfer.
- 7.The issue with virtual circuits is that each time a new connection is set up, resources and extra information have to be reserved at every router along the path, which becomes problematic if many clients are trying to reserve a router's resources simultaneously.

## Datagram Networks :

- 1.It is a connection-less service. There is no need for reservation of resources as there is no dedicated path for a connection session.
- 2.All packets are free to use any available path. As a result, intermediate routers calculate routes on the go due to dynamically changing routing tables on routers.
- 3.Since every packet is free to choose any path, all packets must be associated with a header with proper information about the source and the upper layer data.
- 4.The connection-less property makes data packets reach the destination in any order, which means that they can potentially be received out of order at the receiver's end.
- 5.Datagram networks are not as reliable as Virtual Circuits.

ISSUE	VIRTUAL CIRCUIT	DATAGRAM
Addressing	Each packet contains a short VC number	Each packet contains the source and the destination address
State Information	State information about each VC is maintained	Does not hold packet level state information
Routing	Route is chosen when VC is setup. All packets follow this route	Each packet is routed independently
Congestion control	Easy if enough buffers can be allocated in advance	Difficult
Resource failure	All VCs passing through the failed resource are terminated	Packets are lost only during resource failure
Suitability	Connection-oriented service	Connection-oriented and connectionless service

## 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

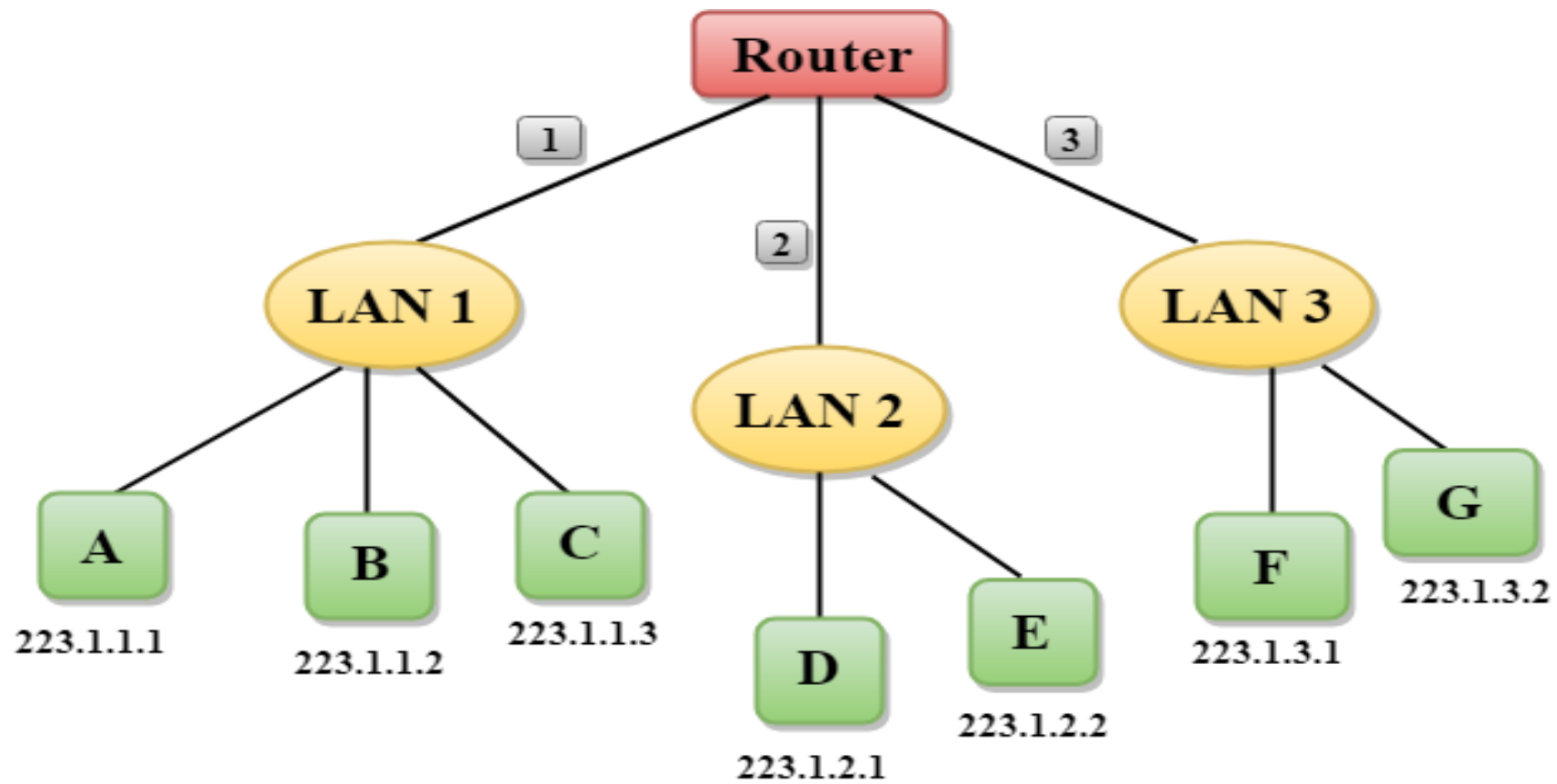
- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet 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.
- 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.

## **Limitations of IPv4**

- IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
- The world's supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple host, we need IP addresses of next class.
- Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security,



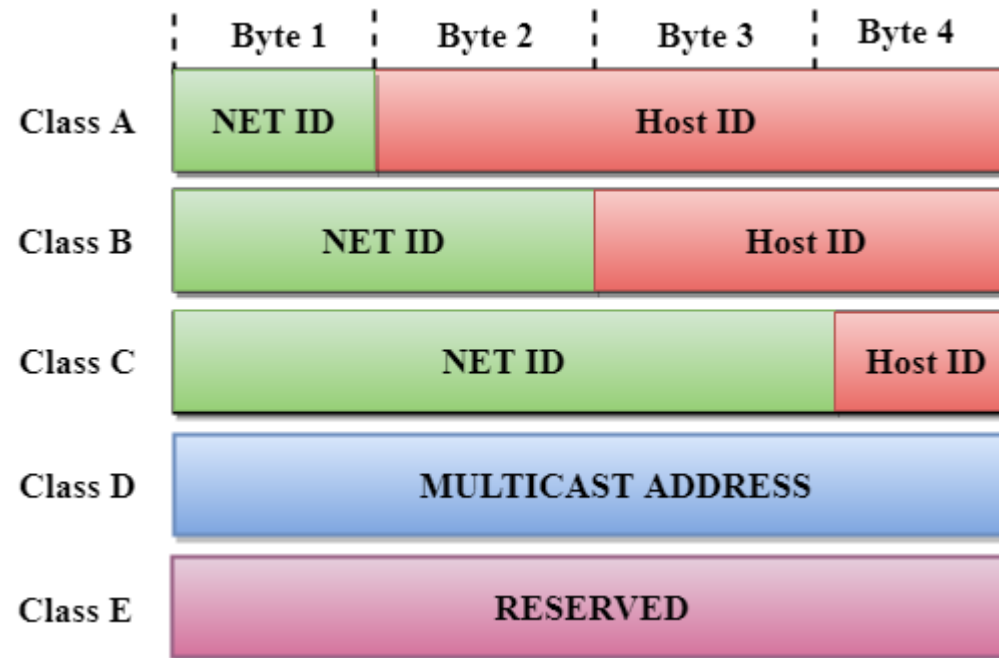
## Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- Network ID:** It represents the number of networks.
- Host ID:** It represents the number of hosts.



## Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

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

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A =  $2^7 = 128$  network address

The total number of hosts in Class A =  $2^{24} - 2 = 16,777,214$  host address

## Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining 14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B =  $2^{14} = 16384$  network address

The total number of hosts in Class B =  $2^{16} - 2 = 65534$  host address

## Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks =  $2^{21} = 2097152$  network address

The total number of hosts =  $2^8 - 2 = 254$  host address



## Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

## Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

## Classful Network Architecture

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	$2^7$	$2^{24}$	0.0.0.0 to 127.255.255.255
B	10	16	16	$2^{14}$	$2^{16}$	128.0.0.0 to 191.255.255.255
C	110	24	8	$2^{21}$	$2^8$	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

## Why IPv4 Datagram Fragmentation required?

Different Networks may have different maximum transmission unit (MTU), for example due to differences in LAN technology. When one network wants to transmit datagrams to a network with a smaller MTU, the routers on path may fragment and reassemble datagrams.

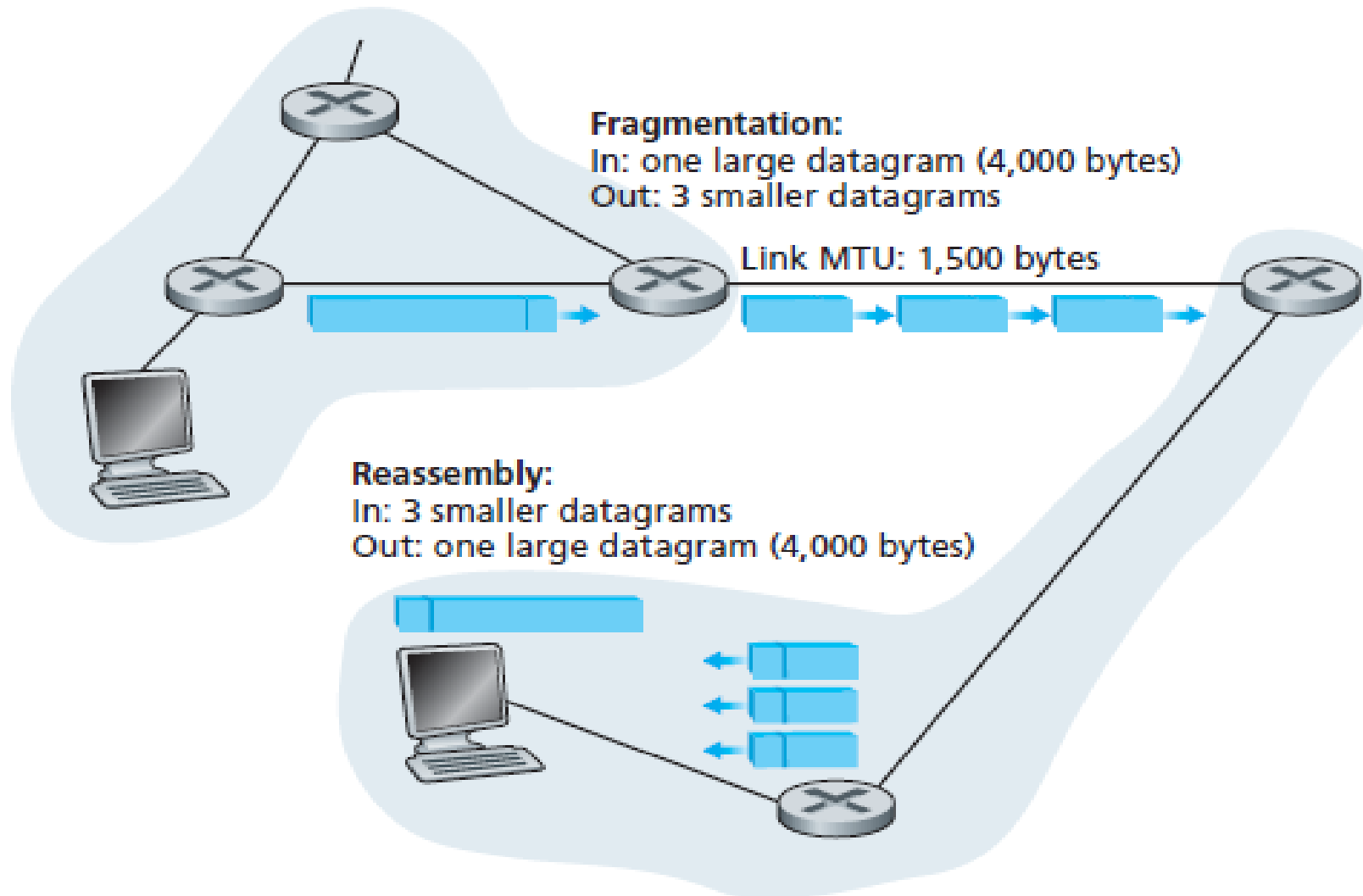
## How is Fragmentation done?

When a packet is received at the router, destination address is examined and MTU is determined. If size of the packet is bigger than the MTU, and the 'Do not Fragment (DF)' bit is set to 0 in header, then the packet is fragmented into parts and sent one by one. The maximum size of each fragment is the MTU minus the IP header size (Minimum 20 bytes and Maximum 60 bytes).

Each fragment is converted to a packet and the following changes happen in the datagram header:

1. The total length field is changed to the size of the fragment.
2. The More Fragment bit (MF bit) is set for all the fragment packets except the last one.
3. The fragment offset field is set, based on the number of fragment that is being set and the MTU.
4. Header Checksum is re-calculated.

The figure below shows an IP datagram fragmentation example .



**IPv4 Packet Structure:**

- Version: Version no. of Internet Protocol used (e.g. IPv4).
- IHL: Internet Header Length; Length of entire IP header.
- Type of service: This provides network service parameters.
- Total Length: Length of entire IP Packet (including IP header and IP Payload).
- Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.
- Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example, protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- Source Address: 32-bit address of the Sender (or source) of the packet.
- Destination Address: 32-bit address of the Receiver (or destination) of the packet.
- Options: This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

## IPv6 address

An IPv6 address is a 128-bit alphanumeric value that identifies an endpoint device in an Internet Protocol Version 6 (IPv6) network. IPv6 is the successor to a previous addressing infrastructure, IPv4, which had limitations IPv6 was designed to overcome. Notably, IPv6 has drastically increased address space compared to IPv4.

An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits. The groups are separated by colons (:). An example of an IPv6 address is: **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.

An IPv6 address (in hexadecimal)

**2001:0DB8:AC10:FE01:0000:0000:0000:0000**

↓ ↓ ↓ ↓ |

**2001:0DB8:AC10:FE01::** Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:  
0000000000000000:0000000000000000:0000000000000000:0000000000000000

## Advantages and disadvantages of IPv6 addresses

IPv6 addresses can bring a variety of benefits, including:

- More efficient routing with smaller routing.
- Simplified packet processing due to more streamlined packet headers.
- Support of multicast packet flows.
- Hosts can generate their own IP addresses.
- Eliminates the need for network address translation (NAT).
- Easier to implement services like peer-to-peer (P2P) networks, voice over IP (VoIP) and stronger security.

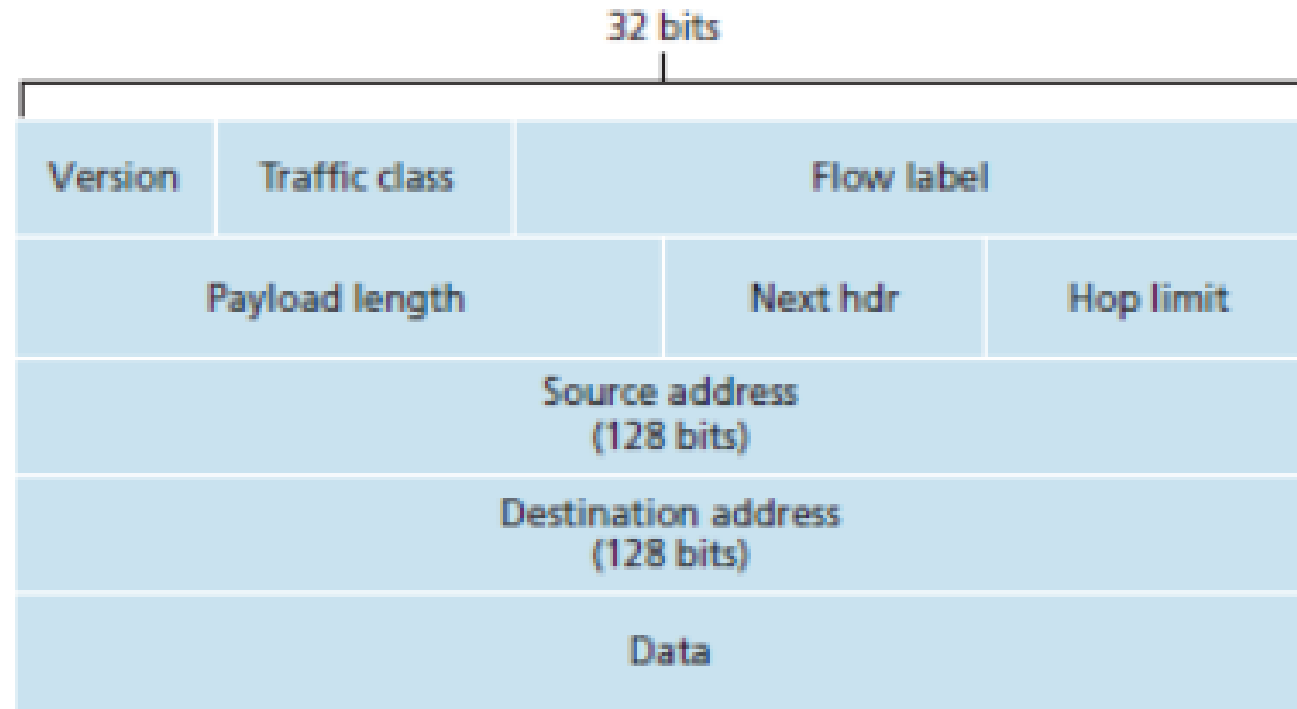


## IPv6 vs. IPv4: What are the differences?

The biggest and most notable difference between IPv4 and IPv6 is the increase in addresses. With IPv4 being a 32-bit IP address and IPv6 being a 128-bit IP address, the number of IP addresses available grows drastically.

Other differences between IPv4 and IPv6 include:

- IPv6 is based on an alphanumeric addressing method, while IPv4 is only numeric.
- IPv6 binary bits are separated by a colon, while IPv4 binary bits are separated by a period.
- IP security is required by IPv6, while it is optional in IPv4.
- IPv6 uses an IP security (IPsec) protocol, while IPv4 relies on applications.
- Networks can be automatically configured with IPv6, while IPv4 networks have to be configured either manually or through Dynamic Host Configuration Protocol (DHCP).

**IPv6 Header:**

## Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

## Distance Vector Routing Algorithm

The Distance-Vector routing algorithm is known by other names. Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm are generally distributed after the researchers create it (Bellman 1957, and Ford and Fulkerson, 1962).

### Features

Following are the features of the distance vector routing are –

- The routers send the knowledge of the whole framework.
- Sharing of data takes place only with the neighbors.
- Sending of data holds place at constant, ordinary intervals, declared every 30 seconds.

In this algorithm, each router evaluates **the distance between itself** and every achievable destination. This is accomplished by assessing the distance between a router and all of its immediate router neighbors and adding each neighboring routers computations for the distance between that neighbor and its close neighbors.

## Link State Routing:

The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. Each collection of best paths will then form each node's routing table. Link-state routing uses

link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Calculation of shortest path:

To find shortest path, each node needs to run the famous **Dijkstra algorithm**. Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph. This famous algorithm uses the following steps:

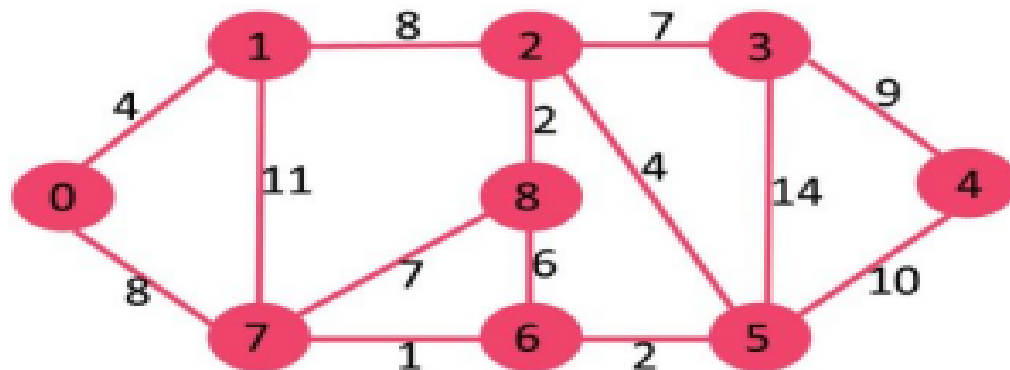
**Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

**Step-2:** Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.

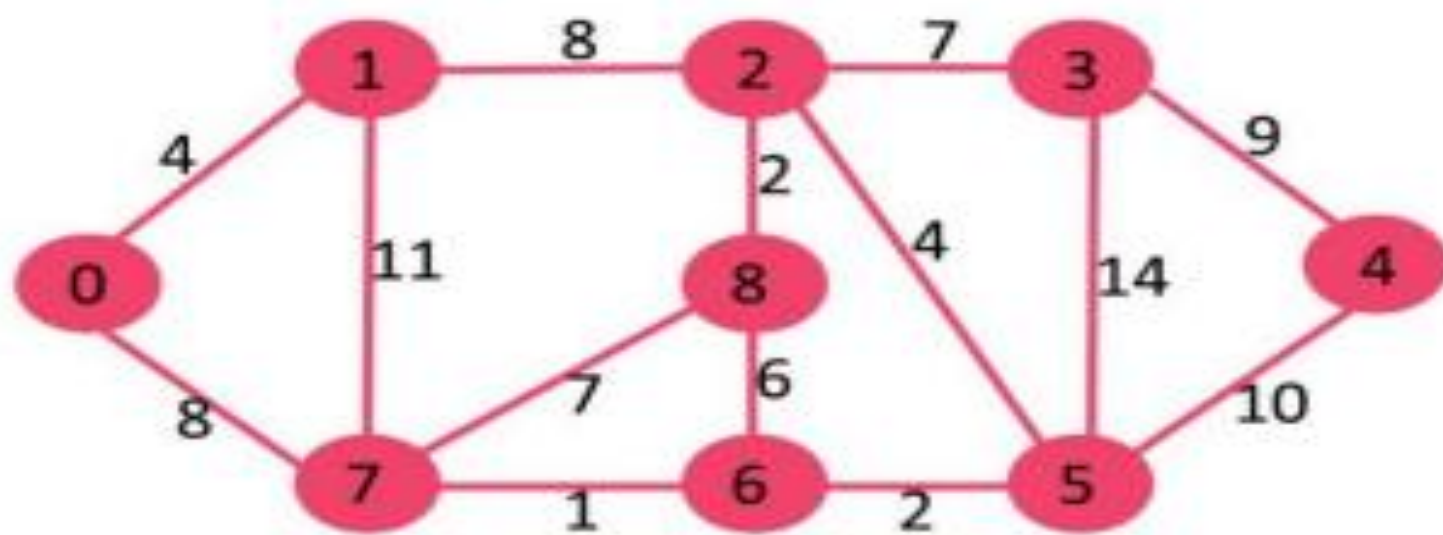
**Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

**Step-4:** The node repeats the Step 2 and Step 3 until all the nodes are added in the tree.

Let us understand with the following example:

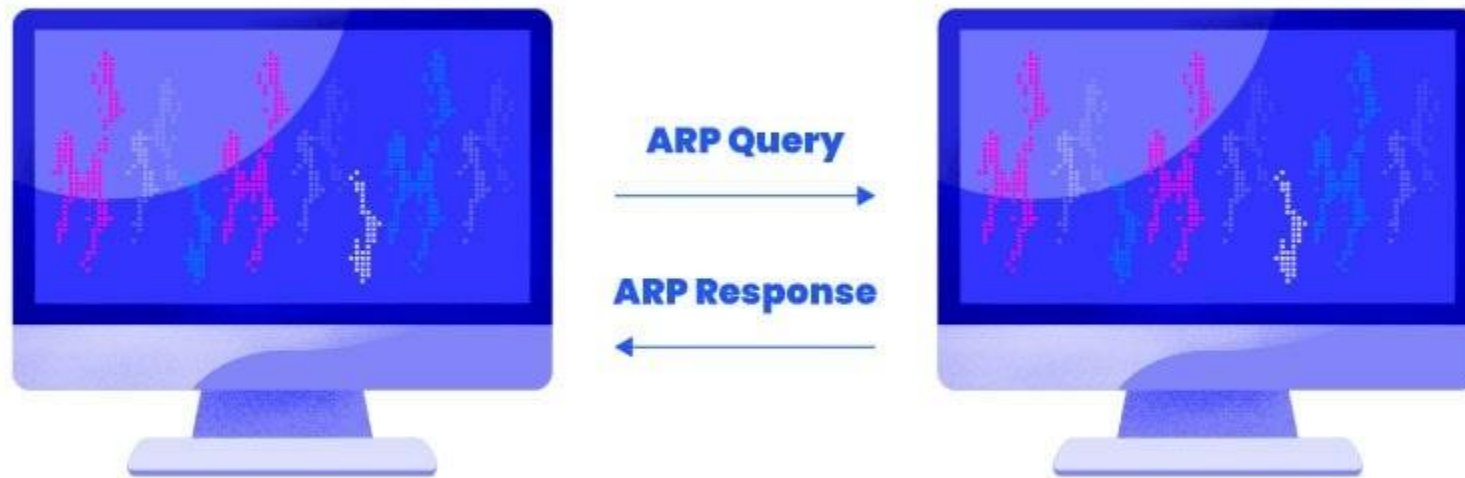



Let us understand with the following example:



<b>Distance Vector Routing</b>	<b>Link State Routing</b>
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkstra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

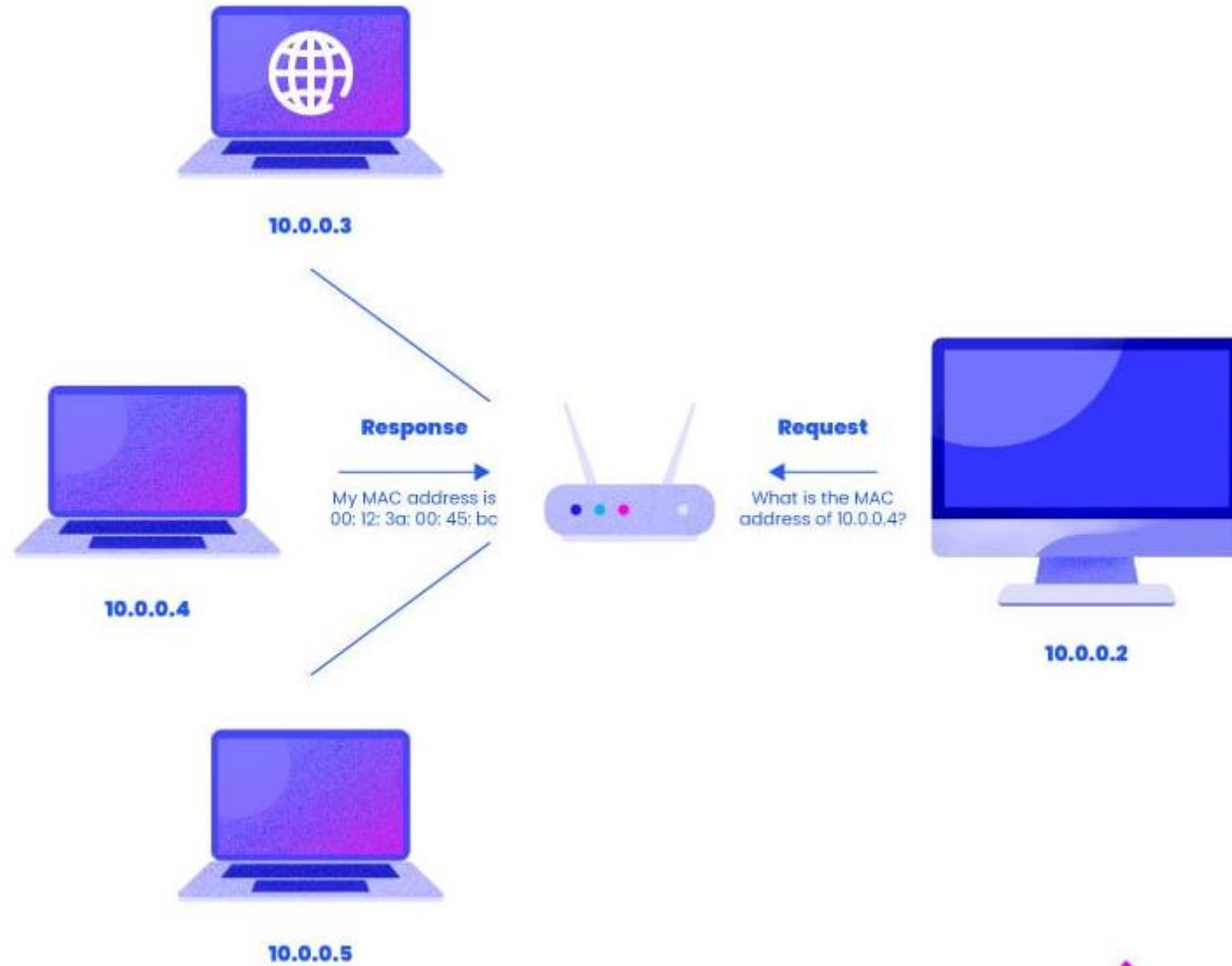






The **Address Resolution Protocol (ARP)** is a communication protocol that maps the **Internet Protocol (IP) address** to the **Media Access Control (MAC)** address. This protocol facilitates the communication of the devices connected to the network.

Applications and software connected to the internet use IP addresses to send information. Meanwhile, the communication between systems happens through hardware addresses, also known as MAC or physical addresses. Without ARP, software and devices would not be able to send data to each other.



## What is RARP ?

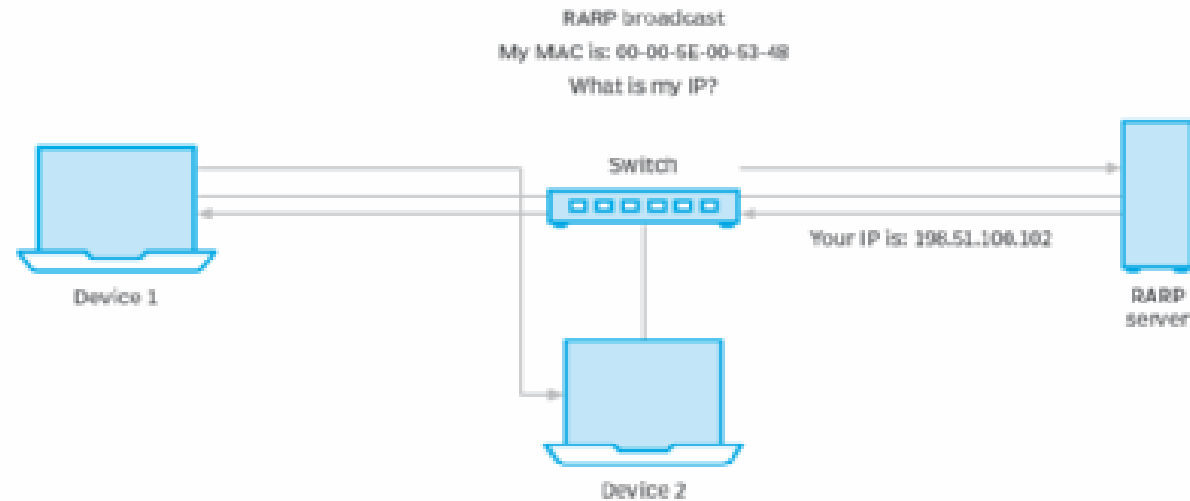
Reverse Address Resolution Protocol (RARP) is a protocol a physical machine in a local area network (LAN) can use to request its IP address. It does this by sending the device's physical address to a **specialized RARP server** that is on the same LAN and is actively listening for RARP requests.

### How does RARP work?

A **network administrator creates** a table in a RARP server that maps the physical interface or media access control (MAC) addresses to corresponding IP addresses.

Table can be referenced by devices seeking to dynamically learn their IP address. When a new RARP-enabled device first connects to the network, its RARP client program sends its physical MAC address to the RARP server for the purpose of receiving an IP address in return that the device can use to communicate with other devices on the IP network.

# The IP lookup process



RARP LOOKUP TABLE	
MAC	IP address
00-00-5E-00-53-48 -F3	198.51.100.101
00-00-5E-00-53-48 -09	198.51.100.102
00-00-5E-00-53-48 -7C	198.51.100.103

## Internet Control Message Protocol (ICMP)

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.

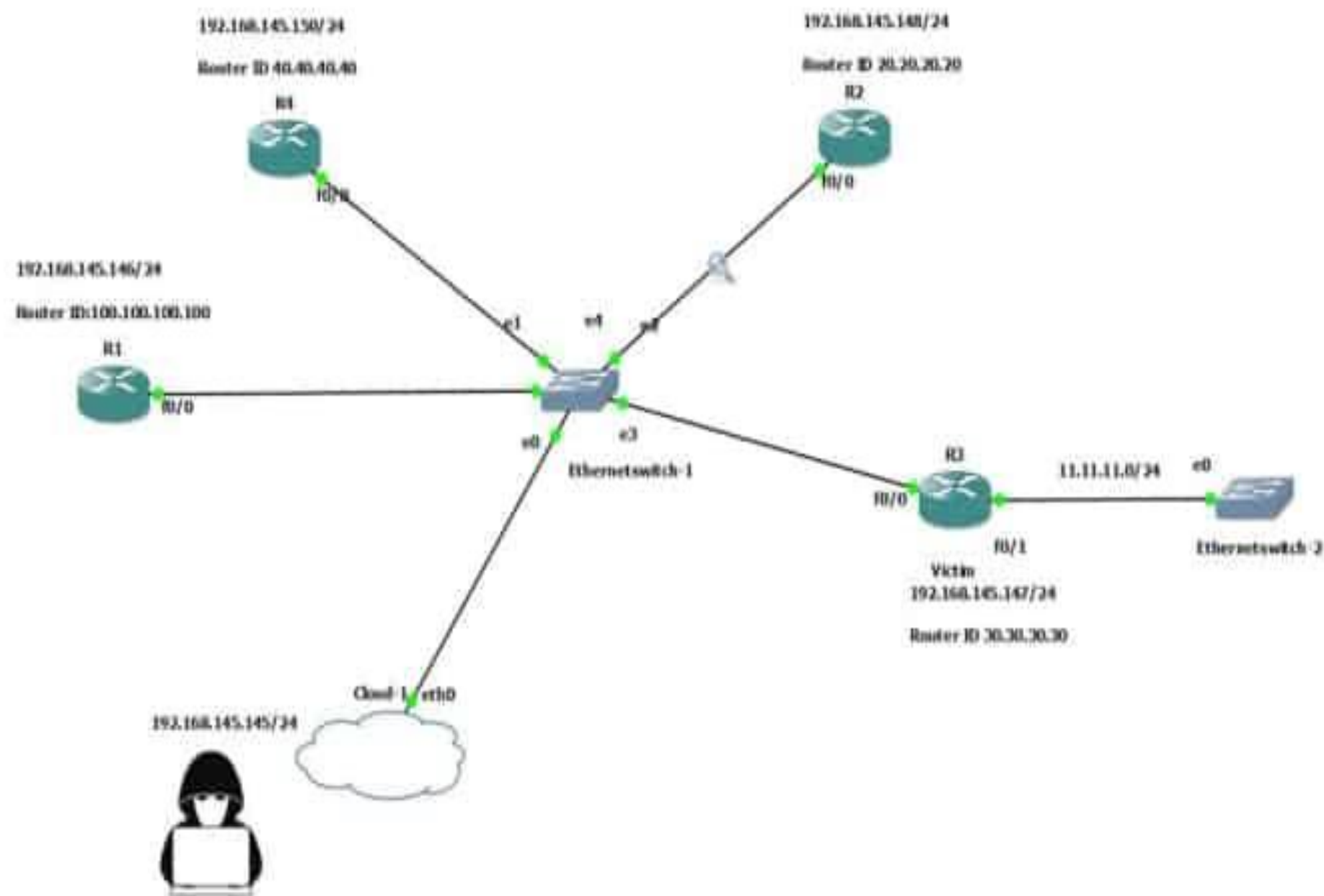
It is a supporting protocol and is used by networks devices like routers for sending error messages and operations information., e.g. the requested service is not available or that a host or router could not be reached.

## Open Shortest Path First (OSPF) protocol States

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First).

OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.

It is a network layer protocol which works on protocol number 89.





## Border Gateway Protocol (BGP)

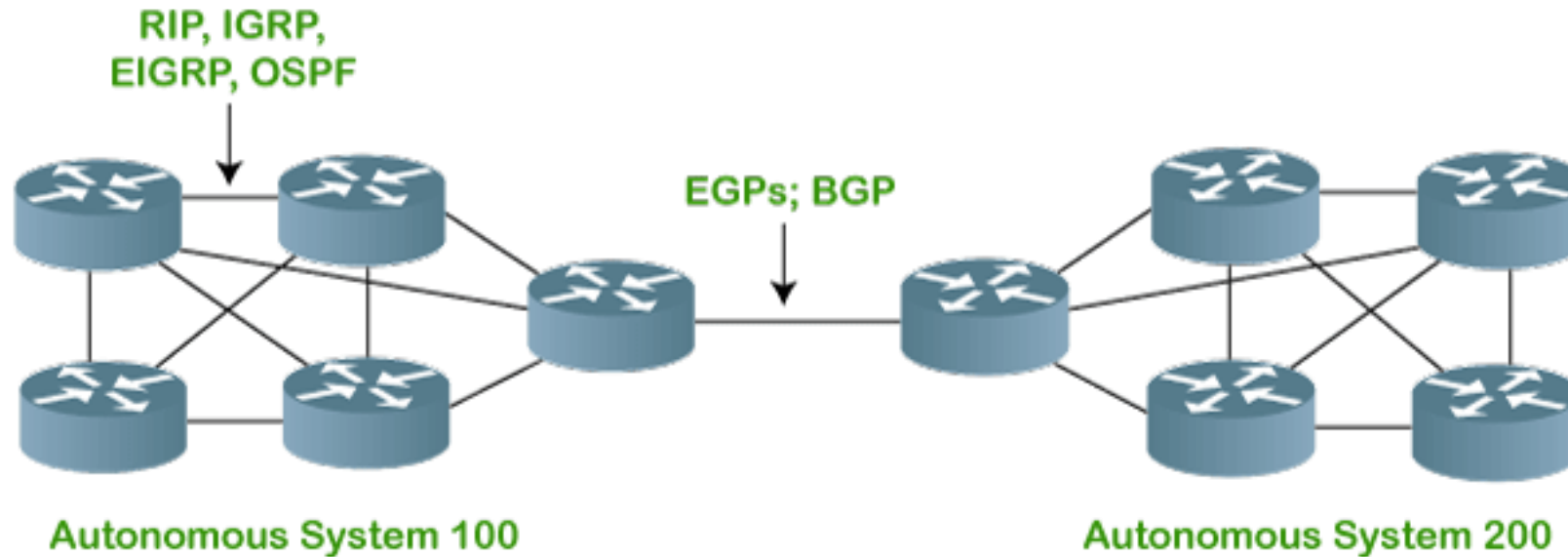
Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different areas.

BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

### What is an autonomous system?

[The Internet](#) is a network of networks\*, and autonomous systems are the big networks that make up the Internet. More specifically, an autonomous system (AS) is a large network or group of networks that has a unified [routing](#) policy. Every computer or device that connects to the Internet is connected to an AS.

## BGP Autonomous Systems

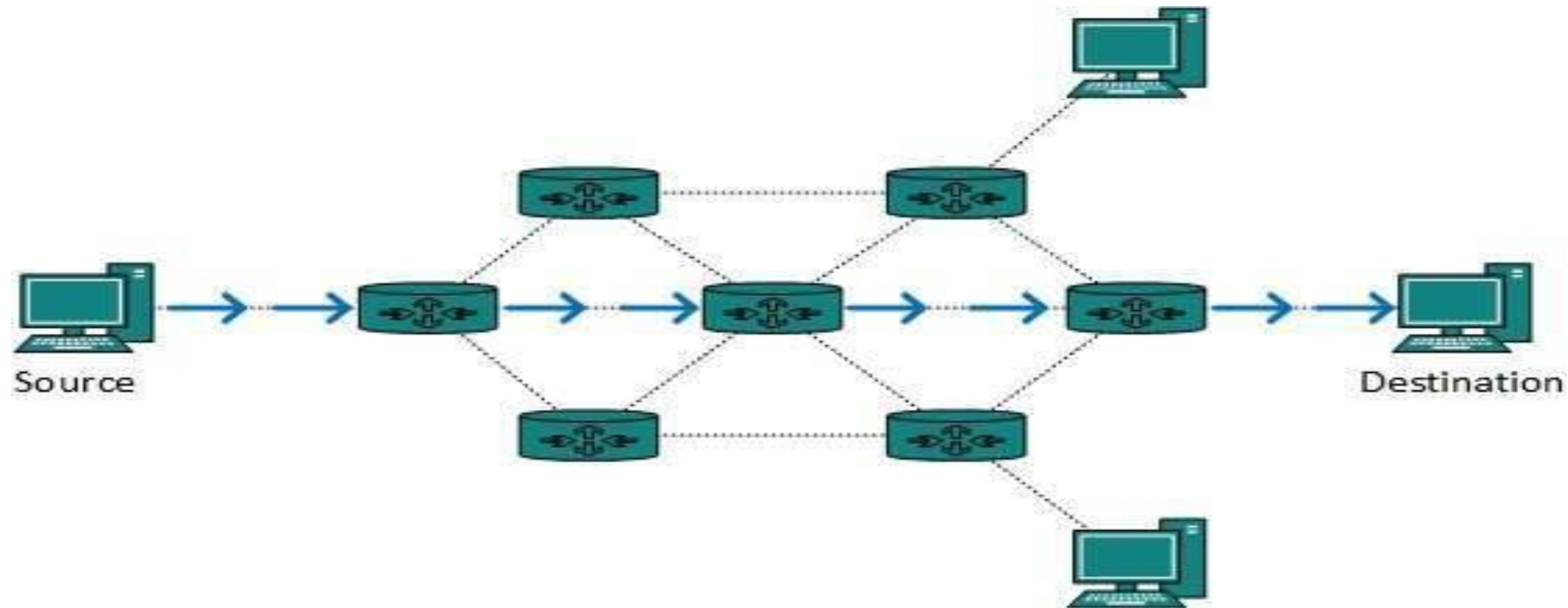


Exterior Gateway Protocol (EGP) is a Routing Protocol which is used to find network path information between different networks. It is commonly used in the Internet to exchange routing table information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems.

## Unicast routing

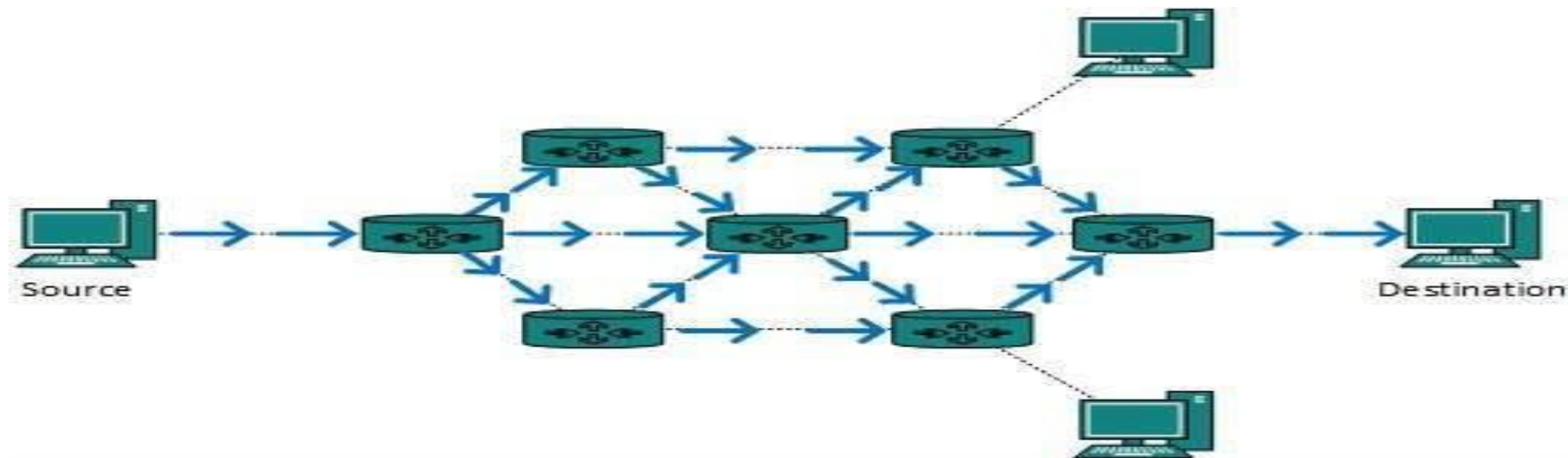
Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination.

Routing unicast data over the internet is called unicast routing. **It is the simplest form of routing because the destination is already known.** Hence the router just has to look up the routing table and forward the packet to next hop.



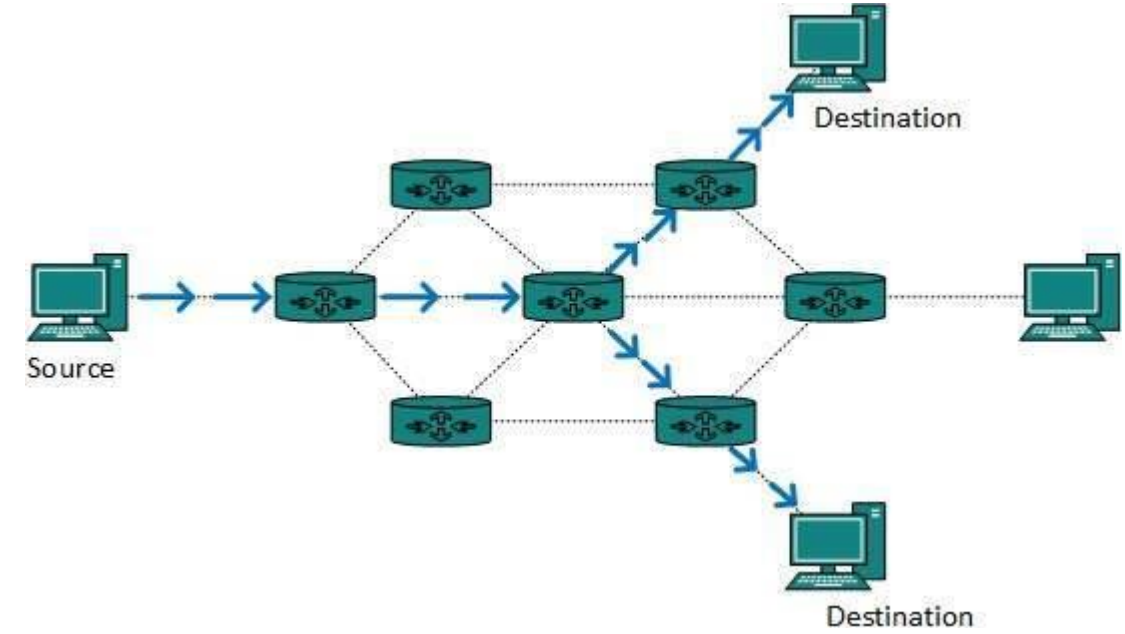
## Broadcast routing

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses.
- All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.
- This method consumes lots of bandwidth and router must destination address of each node.
- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.



## Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. **In broadcast routing, packets are sent to all nodes even if they do not want it.** But in Multicast routing, the data is sent to only nodes which wants to receive the packets.



The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path.

## IPv4 ADDRESSING SCHEME

IP addresses falls into two types:

- Classful IP addressing is a legacy scheme which divides the whole IP address pools into 5 distinct classes—A, B, C, D and E.
- Classless IP addressing has an arbitrary length of the prefixes.

### Classful Addressing

#### Class A

The first octet denotes the network address, and the last three octets are the host portion. Any IP address whose first octet is between 1 and 126 is a Class A address. Note that 0 is reserved as a part of the default address and 127 is reserved for internal loopback testing.

Format: network.host.host.host

Default subnet mask = 255.0.0.0 or (slash notation) /8

#### Class B

### *Netid and Hostid*

In classful addressing, an IP address in class A, B, or C is divided into **netid** and **hostid**. These parts are of varying lengths, depending on the class of the address. Figure 19.2 shows some netid and hostid bytes. The netid is in color, the hostid is in white. Note that the concept does not apply to classes D and E.

In class A, one byte defines the netid and three bytes define the hostid. In class B, two bytes define the netid and two bytes define the hostid. In class C, three bytes define the netid and one byte defines the hostid.

### *Mask*

Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a **mask** (also called the **default mask**), a 32-bit number made of

## CHAPTER 19 NETWORK LAYER: LOGICAL ADDRESSING

contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown in Table 19.2. The concept does not apply to classes D and E.

**Table 19.2** *Default masks for classful addressing*

<i>Class</i>	<i>Binary</i>	<i>Dotted-Decimal</i>	<i>CIDR</i>
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.



contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown in Table 19.2. The concept does not apply to classes D and E.

**Table 19.2** Default masks for classful addressing

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.

The last column of Table 19.2 shows the mask in the form /*n* where *n* can be 8, 16, or 24 in classful addressing. This notation is also called slash notation or **Classless Interdomain Routing (CIDR)** notation. The notation is used in classless addressing, which we will discuss later. We introduce it here because it can also be applied to classful addressing. We will show later that classful addressing is a special case of classless addressing.



### *Subnetting*

During the era of classful addressing, **subnetting** was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called **subnets**) or, in rare cases, share part of the addresses with neighbors. Subnetting increases the number of 1s in the mask, as we will see later when we discuss classless addressing.

### *Supernetting*

The time came when most of the class A and class B addresses were depleted; however, there was still a huge demand for midsize blocks. The size of a class C block with a maximum number of 256 addresses did not satisfy the needs of most organizations. Even a midsize organization needed more addresses. One solution was **supernetting**. In supernetting, an organization can combine several class C blocks to create a larger range of addresses. In other words, several networks are combined to create a super-network or a **supernet**. An organization can apply for a set of class C blocks instead of just one. For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one supernet. Supernetting decreases the number of 1s in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22. We will see that classless addressing eliminated the need for supernetting.

### *Address Depletion*

The flaws in classful addressing scheme combined with the fast growth of the Internet led to the near depletion of the available addresses. Yet the number of devices on the Internet is much less than the  $2^{32}$  address space. We have run out of class A and B addresses, and

### Classless IP addresses

Classful IP addresses is no longer popular and instead has been replaced with the concept of classless IP address, where there is no concept of IP address classes and no strict network and host boundaries. In classless IP addressing, there is no concept of Classful addressing like Classes A, B, C, D and E. IPv4 address range 0.0.0.0 to 223.255.255.255 treated as a single class. No strict 8-byte boundaries for the network and host portions. A Subnet masks defines network & host boundaries. This approach is very useful for optimizing address usage.

#### Examples of Classless Addressing

Network address – 22.10.0.0 /16

Network address – 173.2.224.0 / 21

### **FLSM vs VLSM:**

FLSM stands for Full Length Subnet Mask. It means all the subnets are of the same size. In FLSM, the subnet mask remains the same for all the subnets.

VLSM stands for Variable Length Subnet Mask. It means the size of the subnet varies according to the needs. In VLSM, the subnet mask is different normally but it can be same for any two or more subnets depending upon the situation.

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 100 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator has 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology, the administrator cannot fulfill all the requirements of the network.

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

**Numerically, we can show the VLSM subnetting process as:**

The given network address is: 192.168.1.0/24

Given requirement in descending order is:

Sales 100

Purchase 50

Accounts 25

Management 5

The complete range of the address in the above provided network is:

192.168.1.0 to 192.168.1.255

Divide the given network consisting 256 hosts into 2 networks with 128 hosts each:

192.168.1.0-192.168.1.127      (192.168.1.0/25)

192.168.1.128-192.168.1.255      (192.168.1.128/25)

The largest network requirement is of 100 hosts for Sales department. For this, we need to assign subnetwork with 128 hosts.

Let us assign the first divided subnetwork 192.168.1.0/25 to Sales Department.

We now have remaining subnetwork 192.168.1.128/25.

Dividing this subnetwork, two subnetworks with 64 hosts each are formed.

192.168.1.128 to 192.168.1.191      (192.168.1.128/26)

192.168.1.192 to 192.168.1.255      (192.168.1.192/26)

Our second network requirement is of 50 hosts for Purchase department. We need to assign subnetwork consisting of 64 hosts.

Assigning 192.168.1.128/26 to Purchase department.

The remaining subnetwork available is 192.168.1.192/26.

Dividing this subnetwork, two subnetworks with 32 hosts each are formed.

We can Assign either of the subnetwork to Management department.

Summarizing the subnetting results,

Network Name	Network ID	Subnet mask	No. of usable hosts	Usable Host ID Range	Broadcast address
Sales	192.168.1.0	/25	126	192.168.1.1 to 192.168.1.126	192.168.1.127
Purchase	192.168.1.128	/26	62	192.168.1.129 to 192.168.1.190	192.168.1.191
Account	192.168.1.192	/27	30	192.168.1.193 to 192.168.1.222	192.168.1.223
Management	192.168.1.240	/29	6	192.168.1.241 to 192.168.1.246	192.168.1.247
Unused	192.168.1.224/28 (192.168.1.224 to 192.168.1.239)				
Unused	192.168.1.247/29 (192.168.1.247 to 192.168.1.255)				



### FLSM Numerical Example:

**Q1. If you are given a network 210.25.23.0 with the subnet mask 255.255.255.0, assign the networks to four different departments with 50 hosts each.**

Ans: The complete range of the address in the above provided network is:

210.25.23.0 to 210.25.23.255

Total no of hosts available: 256 hosts

Each subnetwork requires 50 usable hosts. So, we need to assign n/w with 64 hosts each to the four departments.

Since we are using FLSM, the divided networks will be of same size. The given network consists of 256 hosts which needs to be divided into four subnetworks with 64 hosts each.

The process is as follows:

First of all, divide the given network range into four equal parts.

210.25.23.0 to 210.25.23.63                      (210.25.23.0/26)

210.25.23.64 to 210.25.23.127                      (210.25.23.64/26)

210.25.23.128 to 210.25.23.191                      (210.25.23.128/26)

210.25.23.192 to 210.25.23.255                      (210.25.23.192/26)

Now, as per the requirement, there are four networks required and we can assign the above networks

Network Name	Network ID	Subnet mask	No. of usable hosts	Usable Host ID Range	Broadcast address
Dept 1	210.25.23.0	/26	62	210.25.23.1 to 210.25.23.62	210.25.23.63
Dept 2	210.25.23.64	/26	62	210.25.23.65 to 210.25.23.126	210.25.23.127
Dept 3	210.25.23.128	/26	62	210.25.23.129 to 210.25.23.190	210.25.23.191
Dept 4	210.25.23.192	/26	62	210.25.23.193 to 210.25.23.254	210.25.23.255



**Q2. Suppose you are network administrator with provided network 172.16.0.0/24. You need to manage the entire n/w by dividing into subnetworks so that each of the Development, Sales, Reception, HR and Production. How would you do so?**

Ans: Provided network: 172.16.0.0/24. Here, /24 indicates 256 hosts are contained in the given network.

There are five departments to address the networks with. So, we divide the given network into 8 networks.  $256/8 = 32$

Each of the 8 subnetworks will contain 32 hosts each. The divided networks will be:

172.16.0.0 to 172.16.0.31	(172.16.0.0/27)
172.16.0.32 to 172.16.0.63	(172.16.0.32/27)
172.16.0.64 to 172.16.0.95	(172.16.0.64/27)
172.16.0.96 to 172.16.0.127	(172.16.0.96/27)
172.16.0.128 to 172.16.0.159	(172.16.0.128/27)
172.16.0.160 to 172.16.0.191	(172.16.0.160/27)
172.16.0.192 to 172.16.0.223	(172.16.0.192/27)
172.16.0.224 to 172.16.0.255	(172.16.0.224/27)

Now, we can assign 5 of the above 8 subnetworks to the departments of our requirement.

The result will be as follows:

The result will be as follows:

Network Name	Network ID	Subnet mask	No. of usable hosts	Usable Host ID Range	Broadcast address
Development	172.16.0.0	/27	30	172.16.0.1 to 172.16.0.30	172.16.0.31
Sales	172.16.0.32	/27	30	172.16.0.33 to 172.16.0.62	172.16.0.63
Reception	172.16.0.64	/27	30	172.16.0.65 to 172.16.0.94	172.16.0.95
HR	172.16.0.96	/27	30	172.16.0.97 to 172.16.0.126	172.16.0.127
Production	172.16.0.128	/27	30	172.16.0.129 to 172.16.0.158	172.16.0.159
Unused	172.16.0.160 to 172.16.0.191			(172.16.0.160/27)	
Unused	172.16.0.192 to 172.16.0.223			(172.16.0.192/27)	
Unused	172.16.0.224 to 172.16.0.255			(172.16.0.224/27)	

End of chapter 4