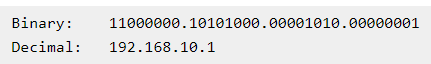
**COMPUTER COMMUNICATION**

## UNIT II

## **IPV4 Addressing**

Internet protocol version 4 in any network is a standard protocol for assigning a logical address (IP address) to hosts. You are currently using the same protocol. This protocol is capable of providing a unique address to the devices available in this world, but will not be available after a few years. Therefore its advanced version IPV6 has been introduced, which you can read in the tutorial of IPV6.

The IP address in IPV4 is 32 bits. It is represented in 4 blocks of 8 bits. The lower IPV4 address is represented in both binary and decimal form.

****

These blocks represent networks and hosts. The starting block represents the network and represents the subsequent hosts that how many blocks will represent the network and how many hosts will represent these are defined by classes of IP address. If you want to know more about the format and classes of the IPV4 address, you can read it in the Addressing tutorial.

## **Address space**

An address space is a range of logical space on any part of a computer or a [peripheral](https://www.computerhope.com/jargon/p/peripher.htm) device where [data](https://www.computerhope.com/jargon/d/data.htm) can be stored. For instance, on a [memory chip](https://www.computerhope.com/jargon/m/memochip.htm), each [byte](https://www.computerhope.com/jargon/b/byte.htm) of data has its own [address](https://www.computerhope.com/jargon/a/address.htm) where it can be stored and then located at a later time. The address can be limited by physical limitations of the device, as well as arbitrary limits that are used to separate certain types of data from one another.

## **Examples of address spaces**

* Memory addresses in a computer's [RAM](https://www.computerhope.com/jargon/r/ram.htm) or [virtual memory](https://www.computerhope.com/jargon/v/virtmemo.htm).
* Addresses on a network, such as [IP addresses](https://www.computerhope.com/jargon/i/ip.htm).
* [Sector](https://www.computerhope.com/jargon/s/sector.htm) addresses on [disk drives](https://www.computerhope.com/jargon/d/diskdriv.htm).
* [File names](https://www.computerhope.com/jargon/f/filename.htm) in a file system [volume](https://www.computerhope.com/jargon/v/volume.htm).

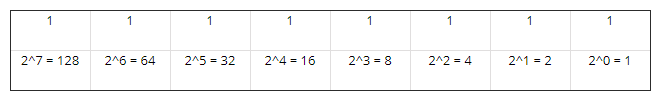
## **Subnet Mask**

A subnet mask is a number that defines a range of [IP addresses](https://pc.net/glossary/definition/ip_address) that can be used in a network. (It is not something you wear on your head to keep subnets out.) Subnet masks are used to designate sub networks, or subnets, which are typically local networks [LANs](https://pc.net/glossary/definition/lan) that are connected to the Internet. Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a [router](https://pc.net/glossary/definition/router). Therefore, sub networks can be used to partition multiple networks and limit the traffic between them.

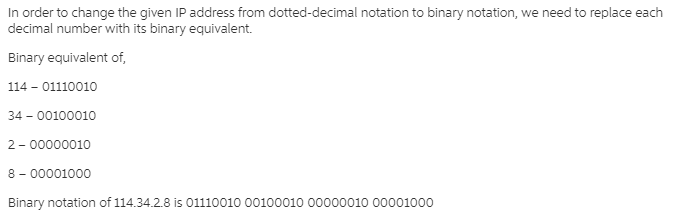
A subnet mask hides, or "masks," the [network](https://pc.net/glossary/definition/network) part of a system's IP address and leaves only the host part as the machine identifier. A common subnet mask for a Class C IP address is 255.255.255.0. Each section of the subnet mask can contain a number from 0 to 255, just like an IP address. Therefore, in the example above, the first three sections are full, meaning the IP addresses of computers within the subnet mask must be identical in the first three sections. The last section of each computer's IP address can be anything from 0 to 255. For example, the IP addresses 10.0.1.201 and 10.0.1.202 would be in the same subnet, while 10.0.2.201 would not. Therefore, a subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

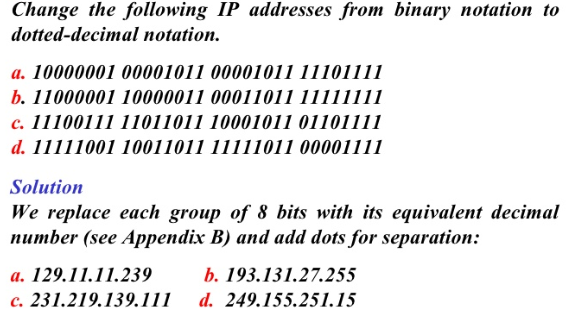
If your system is connected to a network, you can typically view the network's subnet mask number in the Network [control panel](https://pc.net/glossary/definition/controlpanel) (Windows) or System Preference (Mac OS X). Most home networks use the default subnet mask of 255.255.255.0. However, some office networks may use a different subnet mask such as 255.255.255.128, which can be used to split a network into two subnets. Large networks with several thousand machines may use a subnet mask of 255.255.0.0. This is the default subnet mask used by Class B networks. The largest Class A networks use a default subnet mask of 255.0.0.0.

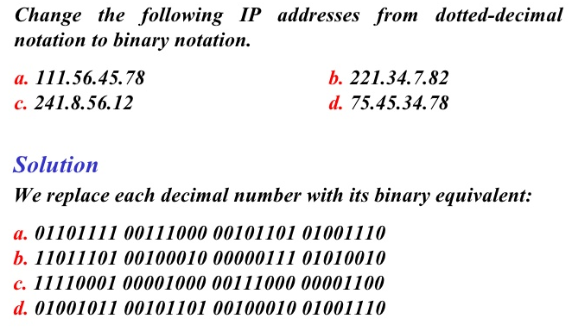


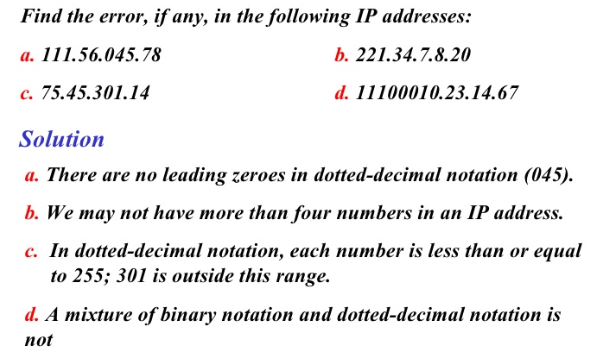


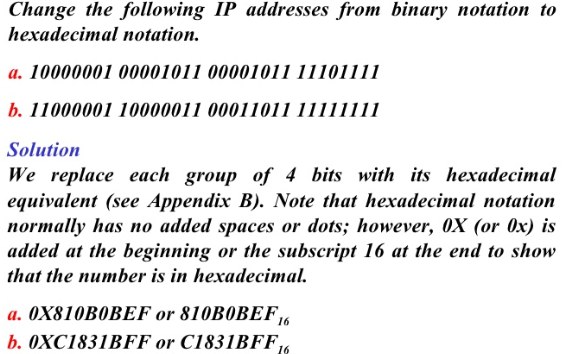
64+32+16+2=114











## Addressing modes in IPv4

## IPv4 provides support to three different types of addressing modes.

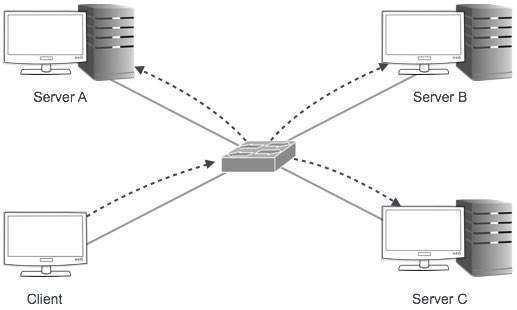
## **Unicast Addressing Mode:**

## In this mode, data will be sent only to one intended host and the Destination Address field will consist of 32- bit IP address of the destination host. Here the client will send data to the targeted server:

## 

## **Broadcast Addressing Mode:**

## In this mode, the packet will be addressed to all the hosts in a network segment. The Destination Address field consists of a special broadcast address, i.e. 255.255.255.255. When a host sees this packet on the network, it will be bound to process it. Here the client sends a packet, which is entertained by all the Servers:



## **Multicast Addressing Mode:**

## This mode is a combination of the earlier two modes, i.e. the packet sent will be neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address consists of a special address which starts with 224.x.x.x and can be entertained by more than one host.

## Here a server will send packets that are entertained by more than one server. Every network will have one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

## **Special IP Addresses**

## There are actually certain numbers of IP addresses that are reserved for a specific reason or purpose. Not all IP addresses can be used for hosts; in fact, there are some IP addresses that are assigned by the Internet Assigned Numbers Authority (IANA) for special purposes.

### **#1. IP: 0.0.0.0**

This IP has special meaning on the computer networks. A computer usually shows this exclusive IP when your computer is disengaged with a TCP/IP network. With this exceptional IP, Your computer will not be able to reach or converse with any other computers over IP.

Sometimes, TCP/IP software applications also use **0.0.0.0**as a programming procedure in order to observe the traffic over the network from any legitimate IP address.

When connected, the nodes don’t employ this address, but rather, the information running over IP usually embrace 0.0.0.0 within the header when the origin of information is unidentified.

### **#2. IP 240.0.0.0**

This IP comes under IPv4’s class E network (240.0.0.0/4) and carries around 268 million addresses. The IP addresses in this class are set aside for the purpose of future and experimental use.

Since IPv6 has been insisting that they have been running out of address space, IPv4 still makes a solid claim to being “Reserved for future use”. In future when IPv6 is widely implemented IPv4 will be utilized.

### **#3. IP: 127.0.0.1**

IP **127.0.0.1**is computers’ loopback address, this inimitable purpose address is reticent for use on each computer. Network utilities may use this address in order to access any local computer’s TCP/IP network resources.

Each message passed to loopback IP address such as 127.0.0.1 is not reached outside to the local area network (LAN) but rather, they are reached through the design re-routed by your computer’s self-network adapter. Normally each of the IP address that comes in between 127.0.0.1 – 127.255.255.255 is kept for private users.

If you need to find “[my live IP address](https://whatismyip.live/)” one of the easiest ways is by using a website such as “What is my IP”.

### **#4. IP 10.0.0.1**

It is often times referred to as a “default gateway address” since it normally presents the local part of a router’s link with the Internet. **This IP address**is a default for a number of network routers such as Cisco’s routers. A network server can use IP 10.0.0.1 as well.

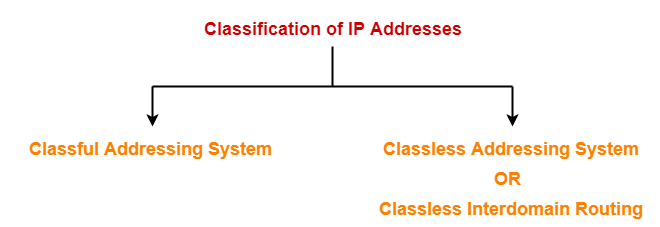
[Business networks than](http://opsblog.org/) households normally use it. The 10.x.x.x, as well as the 192.168.x.x ranges, are private IP addresses.

### **#5.** **IP 224.0.0.0**

The IP address in the range of 224.0.0.0 – 224.0.0.255 is kept for particular “well-known” multicast addresses. These IP addresses are allocated by IANA and chosen for multicasting barely on the local network.

A Multicast address is used in order to process datagram or frame anticipation to be used as a multicast to a chosen network. In addition, the range for multitasking address starts from 224.0.0.0 and ends to 239.255.255.255.

These are the following five IP address allotted by the Internet Assigned Numbers Authority (IANA) for special purposes.



**Classless Addressing-**

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a ‘/’ symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

* Classless Addressing is an improved IP Addressing system.
* It makes the allocation of IP Addresses more efficient.
* It replaces the older classful addressing system based on classes.
* It is also known as Classless Inter Domain Routing (CIDR).

**CIDR**

Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices. The IP addresses allow particular information packets to be sent to specific computers. Shortly after the introduction of CIDR, technicians found it difficult to track and label IP addresses, so a notation system was developed to make the process more efficient and standardized. That system is known as CIDR notation.

CIDR IP addresses consist of two groups of numbers, which are also referred to as groups of bits. The most important of these groups is the network address, and it is used to identify a network or a sub-network (subnet). The lesser of the bit groups is the host identifier. The host identifier is used to determine which host or device on the network should receive incoming information packets. In contrast to classful routing, which categorizes addresses into one of three blocks, CIDR allows for blocks of IP addresses to be allocated to Internet service providers. The blocks are then split up and assigned to the provider’s customers. Until recently, IP addresses used the IPv4 CIDR standard, but because IPv4 addresses are nearly exhausted, a new standard known as IPv6 has been developed and will soon be implemented.

# **Classful Addressing**

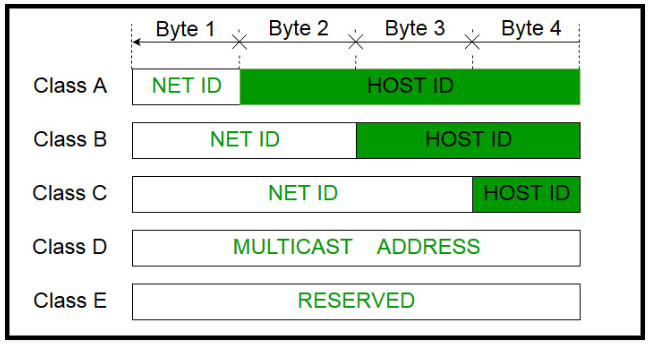
The 32 bit IP address is divided into five sub-classes. These are:

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

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.  
IPv4 address is divided into two parts:

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

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



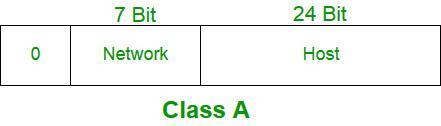
**Class A:**

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

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

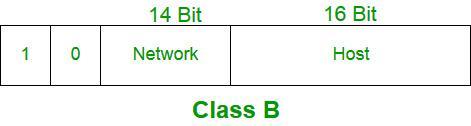
The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

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

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_4.jpg)

**Class B:**

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

* The network ID is 16 bits long.
* The host ID is 16 bits long.
* The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:
* 2^14 = 16384 network address
* 2^16 – 2 = 65534 host address
* IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.  
  [](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_5.jpg)

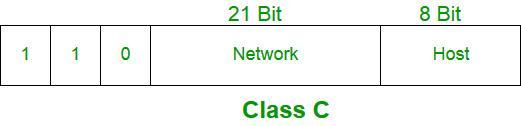
**Class C:**

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

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

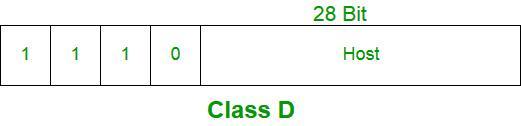
The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

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

IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_6.jpg)

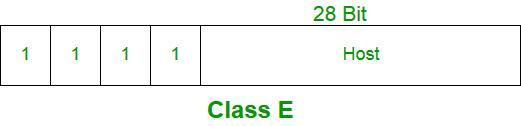
**Class D:**

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

Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_7.jpg)

**Class E:**

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

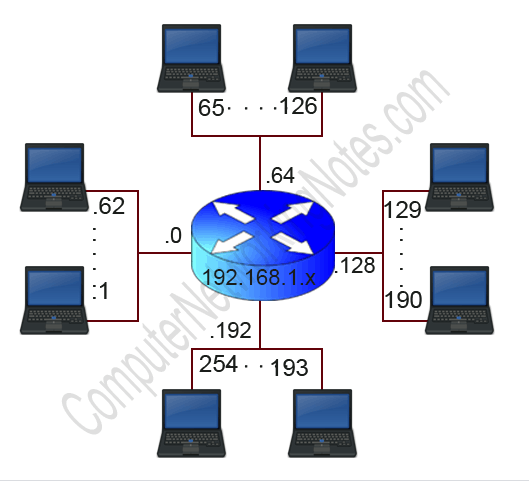
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_8.jpg)

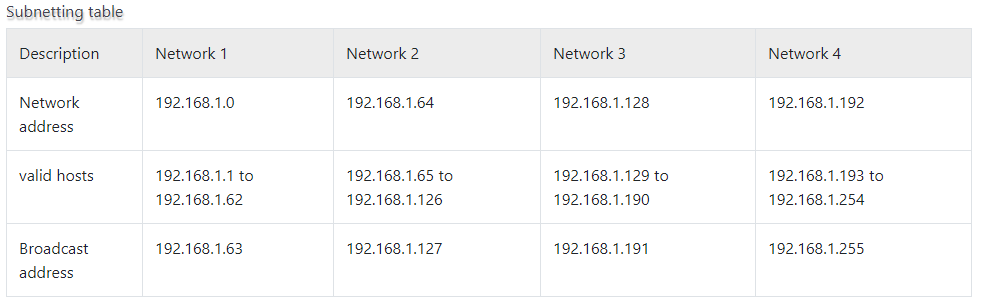
## **Subnetting**

Computer networks also follow the same concept. In computer networking, Subnetting is used to divide a large IP network in smaller IP networks known as subnets.

A default class A, B and C network provides 16777214, 65534, 254 hosts respectively. Having so many hosts in a single network always creates several issues such as broadcast, collision, congestion, etc.

Let’s take a simple example. In a company there are four departments; sales, production, development and management. In each department there are 50 users. Company used a private class C IP network. Without any Subnetting, all computers will work in a single large network.



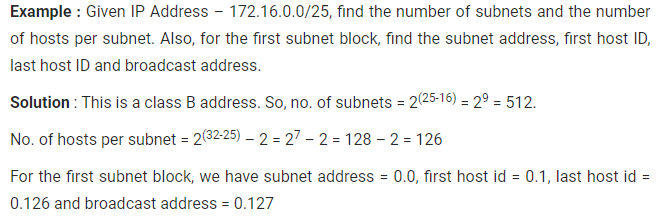


##### **Advantage of Subnetting**

* Subnetting allows us to break a single large network in smaller networks. Small networks are easy to manage.
* Subnetting reduces network traffic by allowing only the broadcast traffic which is relevant to the subnet.
* By reducing unnecessary traffic, Subnetting improves overall performance of the network.
* By blocking a subnet’ traffic in subnet, Subnetting increases security of the network.
* Subnetting reduces the requirement of IP range.

##### **Disadvantage of Subnetting**

* Different subnets need an intermediate device known as router to communicate with each other.
* Since each subnet uses its own network address and broadcast address, more subnets mean more wastage of IP addresses.
* Subnetting ads complexity in network. An experienced network administrator is required to manage the subnetted network.
* That’s all for this introductory part. In next parts we will learn the Subnetting components and terminology in detail. If you have any suggestion or comment about this tutorial, please mail me. If you like this tutorial, please don’t forget to share it with friends through your favorite social channel.



172.16.0.0 / 25

Class B

* + 1. Subnet = 2(25 -16) = 512
    2. No of host per subnet = 2(32-25)

= (0 t0 127)

Network address = 172.16.0.0

Broadcast address = 172.16.0.127

Host address = 172.16.0.1 to 172.16.0.126

## **Subnet Mask**

## The 32-bit IP address consists of information about the host and its network and it is very essential to differentiate both. For this, routers will make use of Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, result will be the Network address. For example, assume that the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then:

## 

**PROBLEM:1**

An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

**Solution:**

**/ 24 =**

**8 BITS = 28**

**= 256 ( 0 to 255)**

The first address is 14.24.74.0/24;

the last address is 14.24.74.255/24.

To satisfy the third requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one.

1. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2.

We allocate 128 addresses. ( 0 to 127)

The subnet mask for this subnet can be found as n1 =32−log2128

=32−log2.27

=25.

The first address in this block is 14.24.74.0/25;

the last address is 14.24.74.127/25.

1. The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either.

We allocate 64 addresses. (128 to 191)

The subnet mask for this subnet can be found as

n2 = 32 − log2 64

n2 = 32 − log2 .26

= 26.

The first address in this block is 14.24.74.128/26;

the last address is 14.24.74.191/26.

1. The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2 either.

We allocate 16 addresses.

The subnet mask for this subnet can be found as n3 = 32 − log216

n3 = 32 − log2. 24 = 28

The first address in this block is 14.24.74.192/28;

the last address is 14.24.74.207/28

If we add all addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve.

The first address in this range is 14.24.74.208.

The last address is 14.24.74.255. We don’t know about the prefix length yet.

**PROBLEM:2**

Find the Network, broadcast address and host address of the given IP address: **192.168.1.0/27**

**Solution:**

**192.168.1.0/27**

Class C - SUBNET MASK: 255.255.255.0

255 255 255 0

11111111 11111111 11111111 00000000

* **Prefix length: 27 ( NET ID is 27)**

**32 -27 = 5**

(i) Total no of network in this IP address = 2^n

= 2^3=**8 Networks**

(ii) No of host in each network: 256 (0 to 255)

= 256/8=**32 Host**

11100000

| | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 | | --- | --- | --- | --- | --- | --- | --- | --- | | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |  |  |  |  |  |  |  |  | | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| **128+64+32=224**  255.255.255.224=Subnet Mask  255 255 255 224  11111111 11111111 11111111 11100000 |  |  |  |  |  |  |  |
| **8 NUMBER OF NETWORK AND**  **32 NUMBER OF HOST ASSIGNED TO EACH NETWORK** | | |  |  |  |  |  |

| NETWORK | IP | NETWORK ID | HOST ID | BROADCAST ID |
| --- | --- | --- | --- | --- |
| NETWORK 1 | 192.168.1.0 | 192.168.1.0 | 192.168.1.1 | 192.168.1.31 |
| 192.168.1.31 | 192.168.1.30 |
| NETWORK 2 | 192.168.1.32 | 192.168.1.32 | 192.168.1.33 | 192.168.1.63 |
| 192.168.1.63 | 192.168.1.62 |
| NETWORK 3 | 192.168.1.64 | 192.168.1.64 | 192.168.1.65 | 192.168.1.95 |
| 192.168.1.95 | 192.168.1.94 |
| NETWORK 4 | 192.168.1.96 | 192.168.1.96 | 192.168.1.97 | 192.168.1.127 |
| 192.168.1.127 | 192.168.1.126 |
| NETWORK 5 | 192.168.1.128 | 192.168.1.128 | 192.168.1.129 | 192.168.1.159 |
| 192.168.1.159 | 192.168.1.158 |
| NETWORK 6 | 192.168.1.160 | 192.168.1.160 | 192.168.1.161 | 192.168.1.191 |
| 192.168.1.191 | 192.168.1.190 |
| NETWORK 7 | 192.168.1.192 | 192.168.1.192 | 192.168.1.193 | 192.168.1.223 |
| 192.168.1.223 | 192.168.1.222 |
| NETWORK 8 | 192.168.1.224 | 192.168.1.224 | 192.168.1.225 | 192.168.1.255 |
| 192.168.1.255 | 192.168.1.254 |

# **Supernetting**

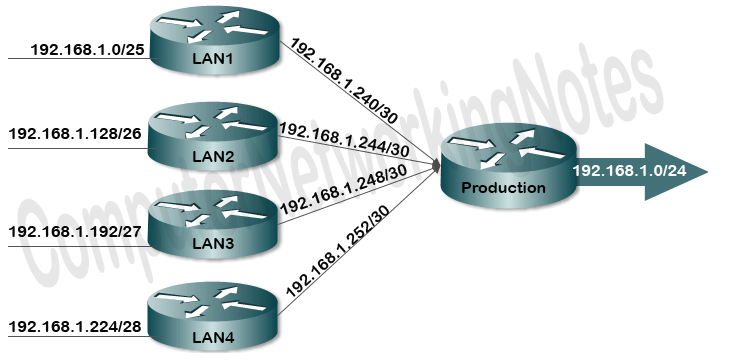
# Supernetting is the process of summarizing a bunch of contiguous Subnetted networks back in a single large network. I'm

# Supernetting is also known as route summarization and route aggregation.

Supernetting is mainly done for optimizing the routing tables. A routing table is the summary of all known networks.

Routers share routing tables to find the new path and locate the best path for destination.

Without Supernetting, router will share all routes from routing tables as they are. With Supernetting, it will summarize them before sharing. Route summarization reduces the size of routing updates dramatically.



### **Advantage of Supernetting**

Supernetting provides following advantages.

* It reduces the size of routing updates.
* It provides a better overview of network.
* It decreases the use of resources such as Memory and CPU.
* It decreases the required time in rebuilding the routing tables.

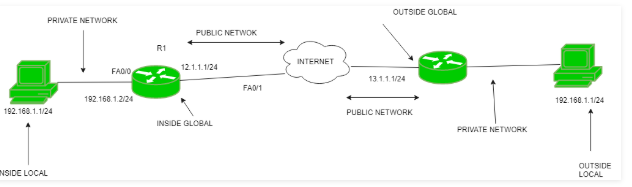
# **Network Address Translation (NAT)**

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

**Network Address Translation (NAT) working**

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

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



**Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.

**Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

**Outside local address –** This is the actual IP address of the destination host in the local network after translation.

**Outside global address –** This is the outside host as seen form the outside network. It is the IP address of the outside destination host before translation.

**Network Address Translation (NAT) Types**

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.  
     
   Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.
2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.  
     
   Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool.
3. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

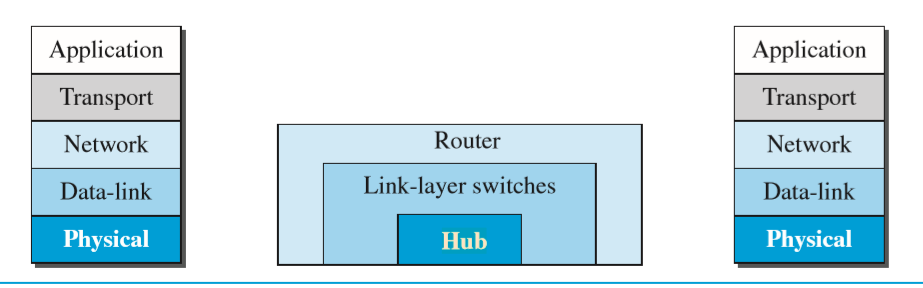
**Advantages of NAT –**

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

**Disadvantage of NAT –**

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

**CONNECTING DEVICES**

****

Hosts and networks do not normally operate in isolation. We use connecting devices to connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model.

We discuss three kinds of connecting devices:

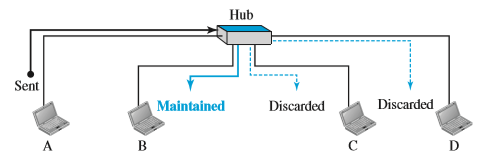
hubs,

link-layer switches,

and routers.

Hubs today operate in the first layer of the Internet model. Link-layer switches operate in the first two layers. Routers operate in the first three layers

**Hubs**

****

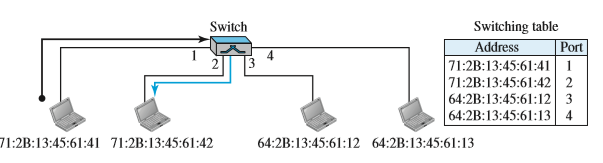
A **hub** is a device that operates only in the physical layer.

Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern. The repeater then sends the refreshed signal. In the past, when Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable.

Today, however, Ethernet LANs use star topology. In a star topology, a repeater is a multiport device, often called a hub, that can be used to serve as the connecting point and at the same time function as a repeater.

Figure shows that when a packet from station A to station B arrives at the hub, the signal representing the frame is regenerated to remove any possible corrupting noise, but the hub forwards the packet from all outgoing ports except the one from which the signal was received. In other words, the frame is broadcast. All stations in the LAN receive the frame, but only station B keeps it. The rest of the stations discard it. Figure shows the role of a repeater or a hub in a switched LAN. The figure definitely shows that a hub does not have a filtering capability; it does not have the intelligence to find from which port the frame should be sent out.

**Switch**

****

A link-layer switch (or switch) operates in both the physical and the data-link layers. As a physical-layer device, it regenerates the signal it receives.

As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

Like hubs, switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive.

Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device.

It does this by learning the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives.

By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard, half-duplex, connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.

**Advantages of Switches**

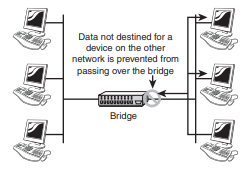
**Collision Elimination**

A link-layer switch eliminates the collision. This means increasing the average bandwidth available to a host in the network. In a switched LAN, there is no need for carrier sensing and collision detection; each host can transmit at any time.

**Connecting Heterogenous Devices**

A link-layer switch can connect devices that use different protocols at the physical layer (data rates) and different transmission media. As long as the format of the frame at the data-link layer does not change, a switch can receive a frame from a device that uses twisted-pair cable and sends data at 10 Mbps and deliver the frame to another device that uses fiber-optic cable and can receive data at 100 Mbps.

**Bridges**

****

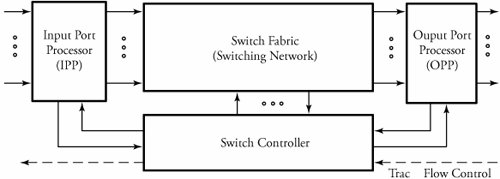
Bridges are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if ONLINEthey can verify that it is on the interface from which it came When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually, a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network. Such devices are called learning bridges because of this functionality.

**Types of Bridges**

➤ Transparent bridge—Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address. ➤ Source route bridge—Used in Token Ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet. ➤ Translational bridge—Used to convert one networking data format to another; for example, from Token Ring to Ethernet and vice versa.

**INTERNAL STRUCTURE OF ROUTERS**

Link: <https://flylib.com/books/en/2.959.1.25/1/>



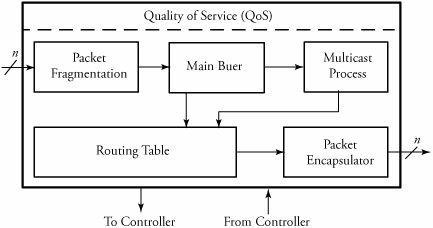
##### *Overview of a typical router*

Routers are the building blocks of wide area networks. Figure 3.10 shows an abstract model of a router as a layer 3 switch. Packets arrive at n input ports and are routed out from n output ports. The system consists of four main parts : input port processors , output port processors , switch fabric (switching network), and switch controller .

Input Port Processor (IPP)

Input and output port processors , as interfaces to switch fabric, are commercially implemented together in router line cards , which contain some of the task of the physical and data link layers . The functionality of the data link layer is implemented as a separate chip in IPP, which also provides a buffer to match the speed between the input and the switch fabric. Switch performance is limited by processing capability, storage elements, and bus bandwidth. The processing capability dictates the maximum rate of the switch. Owing to the speed mismatch between the rate at which a packet arrives on the switch and the processing speed of the switch fabric, input packet rate dictates the amount of required buffering storage. The bus bandwidth determines the time taken for a packet to be transferred between the input and output ports.

An input port processor (IPP) typically consists of several main modules, as shown in Figure 3.11. These modules are packet fragmentation , main buffer , multicast process , routing table , packet encapsulator , and a comprehensive QoS .



##### *Overview of a typical IPP in routers*

##### *Packet Fragmentation*

The packet fragmentation unit , converts packets to smaller sizes. Large packets cause different issues at the network and link layers. One obvious application of packet fragmentation occurs in typical LANs, in which large packets must be fragmented into smaller frames . Another example occurs when large packets must be buffered at the input port interface of a router, as buffer slots are usually only 512 bytes long. One solution to this problem is to partition packets into smaller fragments and then reassemble them at the output port processor (OPP) after processing them in the switching system. Figure 3.12 shows simple packet fragmentation at the input buffer side of a switch. It is always desirable to find the optimum packet size that minimizes the delay.

##### *Routing Table*

The routing table is a look-up table containing all available destination addresses and the corresponding switch output port. An external algorithm fills this routing lookup table. Thus, the purpose of the routing table is to look up an entry corresponding to the destination address of the incoming packet and to provide the output network port. As soon as a routing decision is made, all the information should be saved on the routing table. When a packet enters an IPP, the destination port of the switch should be chosen , based on the destination address of the incoming packet. This destination port needs to be appended to the incoming packet as part of the switch header.

The look-up table management strategy takes advantage of first in, first out (FIFO) queues' speed and memory robustness. To increase memory performance, queue sizes are fixed to reduce control logic. Since network packets can be of various lengths, a memory device is needed to store packet payloads while a fixed-length header travels through the system. Since packets can arrive and leave the network in different order, a memory monitor is necessary to keep track of which locations in memory are free for use. Borrowing a concept from operating systems principles, a free-memory list serves as a memory manager implemented by a stack of pointers. When a packet carrying a destination address arrives from a given link i , its destination address is used to identify the corresponding output port j .

Figure 3.13 shows an example of routing tables at routers between hosts A and B. Assume that host B's address is requested by a packet with destination address 182.15.0.0/22 arriving at router 1. The routing table of this router stores the best-possible path for each destination. Assume that for a given time, this destination is found in entry row 5. The routing table then indicates that port 2 of the router is the right output to go. The table makes the routing decision, based on the estimated cost of the link, which is also stated in the corresponding entry. The cost of each link, as described in Chapter 7, is a measure of the load on each link. When the packet arrives at router 2, this switch performs the same procedure

##### *Multicast Process*

A multicast process is necessary for copying packets when multiple copies of a packet are expected to be made on a switching node. Using a memory module for storage, copying is done efficiently . The copying function can easily be achieved by appending a counter field to memory locations to signify the needed number of copies of that location. The memory module is used to store packets and then duplicate multicast packets by holding memory until all instances of the multicast packet have exited IPP. Writing to memory takes two passes for a multicast packet and only one pass for a unicast packet. In order to keep track of how many copies a multicast packet needs, the packet counter in the memory module must be augmented after the multicast packet has been written to memory. Each entry in the memory module consists of a valid bit, a counter value, and memory data. The multicast techniques and protocols are described in a greater detail in Chapter 15.

##### *Packet Encapsulation*

Packet encapsulation instantiates the routing table module, performs the routing table lookups, and inserts the switch output port number into the network header. The serial-to-parallel multiplexing unit converts an incoming serial byte stream into a fully parallel data stream. This unit also processes the incoming IP header to determine whether the packet is unicast or multicast and extracts the type-of-service field. Once the full packet is received, it is stored into memory. The packet encapsulation unit formats the incoming packet with a header before forwarding the packet to the crossbar

##### *Congestion Controller*

The congestion controller module shields the switching node from any disorders in the traffic flow. Congestion can be controlled in several ways. Sending a reverse-warning packet to the upstream node to avoid exceeding traffic is one common technology installed in the structure of advanced switching systems. Realistically, spacing between incoming packets is irregular. This irregularity may cause congestion in many cases. Congestion control is explained in Chapters 7, 8, and 12.

#### 3.4.2. Switch Fabric

In the switch fabric of a router, packets are routed from input ports to the desired output ports. A packet can also be multicast to more than one output. Finally, in the output port processors, packets are buffered and resequenced in order to avoid packet misordering. In addition, a number of other important processes and functions taken place in each of the mentioned blocks.

abstract model of a virtual-circuit switching router, another example of switching systems. This model can work for ATM technology: Cells (packets) arrive at n input ports and are routed out from n output ports. When a cell carrying VCI b arrives from a given link i , the cell's VCI is used to index a virtual-circuit translation table (VXT) in the corresponding input port processor to identify the output link address j and a new VCI c . In the switching network, cells are routed to the desired outputs. As shown in Figure 3.14, a cell can also be multicast to more than one output. Finally, in output port processors, cells are buffered; in some switch architectures, cells are resequenced in order to avoid misordering.

#### 3.4.3. Switch Controller

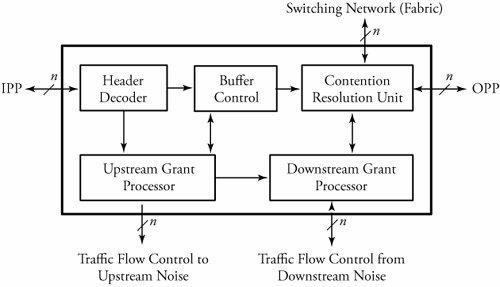
The controller part of a switching system makes decisions leading to the transmission of packets to the requested output(s). The details of the controller are illustrated in Figure 3.15. The controller receives packets from an IPP, but only the headers of packets are processed in the controller. In the controller, the header decoder first converts the control information of an arriving packet into an initial requested output vector. This bit vector carries the information pertaining to the replication of a packet so that any bit of 1 represents a request for one of the corresponding switch outputs.

The initial request vector ultimately gets routed to the buffer control unit, which generates a priority value for each packet to enable it for arbitration. This information, along with the request vector, enters an array of arbitration elements in the contention resolution unit . Each packet in one column of an arbitration array contends with other packets on a shared bus to access the switch output associated with that column. After a packet wins the contention, its identity (buffer index number) is transmitted out to an OPP. This identity and the buffer-control bit explained earlier are also transferred to the switching fabric (network), signaling them to release the packet. This mechanism ensures that a losing packet in the competition remains in the buffer. The buffer-control unit then raises the priority of the losing packet by 1 so that it can contribute in the next round of contention with a higher chance of winning. This process is repeated until eventually, the packet wins.

The identities of winning packets are transmitted to the switch fabric if traffic flow control signals from downstream neighboring nodes are active. The upstream grant processor in turn generates a corresponding set of traffic flow control signals, which are sent to the upstream neighboring nodes. This signal is an indication that the switch is prepared to receive a packet on the upstream node. This way, network congestion comes under control.

#### 3.4.4. Output Port Processors (OPP)

Implementing output port processors in switches includes parallel-to-serial multiplexing, main buffer, local packet resequencer, global packet resequencer, error checker, and packet reassembler, as shown in Figure 3.16. Similar to IPP, OPP also contributes to congestion control. Parallel-to-serial multiplexing converts the parallel-packet format into serial packet format.



##### *Overview of a switching system controller*

##### *Main Buffer*

The buffer unit serves as the OPP central shift register. The purpose of this buffer is to control the rate of the outgoing packets, which impacts the quality of service. After collecting signals serially from the switch fabric, the buffer forwards packets to resequencers. The queue runs on a clock driven by the link interface between the switch and an external link. This buffer must have features that support real-time and non-real -time data.

##### *Reassembler and Resequencer*

The output port processor receives a stream of packet fragments and has to identify and sort out all the related ones. The OPP reassembles them into a single packet, based on the information obtained from the fragment field of headers. For this process, the OPP must be able to handle the arrival of individual fragments at any time and in any order. Fragments may arrive out of order for many reasons. Misordered packets can occur because individual fragments, composed of a fairly large number of interconnections with different delay times, are independently routed through the switch fabric.

A packet reassembler buffer is used to combine fragments of IP packets. This unit resequences receiving packet fragments before transmitting them to external circuits, updates the total-length field of the IP header, and decapsulates all the local headers. The resequencer's internal buffer stores misordered fragments until a complete sequence is obtained. The in-sequence fragments are reassembled and transmitted to the external circuit. A global packet resequencer uses this same procedure to enforce another reordering , this time on sequences, not fragments, of packets that belong to a single user .

##### *Error Checker and CRC*

When a user sends a packet or a frame, a cyclic redundancy check (CRC) field is appended to the packet. The CRC is generated from an algorithm and is based on the data being carried in the packet. The CRC algorithms divide the message by another fixed-binary number in a polynomial form, producing a checksum as the remainder. The message receiver can perform the same division and compare the remainder with the received checksum. The error checker applies a series of error-checking processes on packets to ensure that no errors are on the packets and creates a stream of bits of a given length, called frames. A frame produces a checksum bit , called frame check sequence, which is attached to the data when transmitted.