

# UNIT-III

---

## 1. What is subnetting? Discuss. Also state which classes of IP address can be subnetted.

Subnetting

Subnetting is a process of breaking large network in small networks known as subnets. Subnetting happens when we extend default boundary of subnet mask.

IP addresses are broken into the two components:

**Network component :-** Defines network segment of device.

**Host component :-** Defines the specific device on a particular network segment

### IP Classes in decimal notation

Class A addresses range from 1-126

Class B addresses range from 128-191

Class C addresses range from 192-223

Class D addresses range from 224-239

Class E addresses range from 240-254

### classes of IP address can be subnetted:

Class A: 10.0.0.0

Class B: From 172.16.0.0 to 172.31.0.0

Class C: From 192.168.0.0 to 192.168.255.0

No of machines to be connected	Class of network	Network addresses
254 or less	C	192.168.0.0 to 192.168.255.0
255 to 65,534	B	172.16.0.0 to 172.31.0.0
65,535 to 16,777,214	A	10.0.0.0

## 2. What is subnet masking? Discuss.


Subnet mask is a mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, consider the IP address **150.215.017.009**. Assuming this is part of a Class B network, the first two numbers (**150.215**) represent the Class B network address, and the second two numbers (**017.009**) identify a particular host on this network.

### 3. How can we prove that we have 2,147,483,648 addresses in class A

In class A, only 1 bit defines the class. The remaining 31 bits are available for the address. With 31 bits, we can have  $2^{31}$  or 2,147,483,648 addresses.

### 4. What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

```
200.45.34.56 - 11001000 00101101 00100010 00111000
255.255.240.0 - 11111111 11111111 11110000 00000000
11001000 00101101 00100010 00111000 11111111 11111111 11110000 00000000
11001000 00101101 00100000 00000000
```



The subnetwork address is  
(AND operation)

200.45.32.0

### 5. Go-back-n and selective-repeat are two basic approaches to deal with transmission errors.

- Compare the two approaches in terms of storage and bandwidth requirements.
- With the aid of a packet sequence diagram, show the operation of go-back-n when a data-packet/ACK –pack /NAK-packet is corrupted.

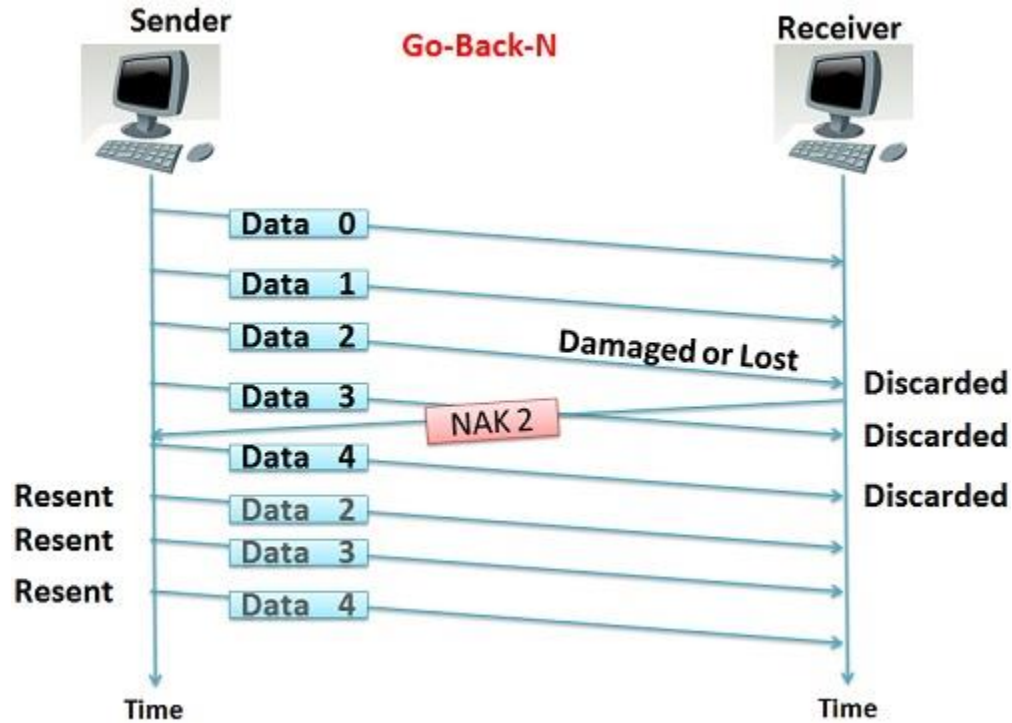
Go-back-n	Selective Repeat
1. Go-back-n requires all retransmission of the succeeding frame along with the lost or damaged frame	1. In the selective repeat, only the specific damaged or lost frame is retransmitted.
2. All subsequent frames including the lost frames will be discarded.	2. The frame that have been lost is the only one that is discarded.
3. The receiver doesn't require any sort of storage and sorting mechanism to store the lost frame in order.	3. The complexity of sorting and storage mechanism, is required by the receiver
4. The sender doesn't require any logic to select the specific frame for retransmission.	4. Extra logic is required for searching and retransmitting the specific frame
5. Receiver doesn't keep any track of the previously received frames	5. Receiver maintain a buffer that keep track of all the previously received frames
6. It is not expensive when compare to selective repeat.	6. It is expensive, but gives better performance.

b) With the aid of a packet sequence diagram, show the operation of go-back-n when a data-packet/ACK-pack /NAK-packet is corrupted.

### Definition of Go-Back-N

Go-Back-N protocol is a sliding window protocol. It is a mechanism to detect and control the error in datalink layer. During transmission of frames between sender and receiver, if a frame is damaged, lost, or an acknowledgement is lost then the action performed by sender and receiver is

explained in the following content.



#### *Damaged Frame*

If a receiver receives a damaged frame or if an error occurs while receiving a frame then, the receiver sends the NAK ( negative acknowledgement) for that frame along with that frame number, that it expects to be retransmitted. After sending NAK, the receiver discards all the frames that it receives, after a damaged frame. The receiver does not send any ACK (acknowledgement) for the discarded frames. After the sender receives the NAK for the damaged frame, it retransmits all the frames onwards the frame number referred by NAK.

#### *Lost frame*

The receiver checks the number on each frame, it receives. If a frame number is skipped in a sequence, then the receiver easily detects the loss of a frame as the newly received frame is received out of sequence. The receiver sends the NAK for the lost frame and then the receiver discards all the frames received after a lost frame. The receiver does not send any ACK (acknowledgement) for that discarded frames. After the sender receives the NAK for the lost frame, it retransmits the lost frame referred by NAK and also retransmits all the frames which it has sent after the lost frame.

#### *Lost Acknowledgement*

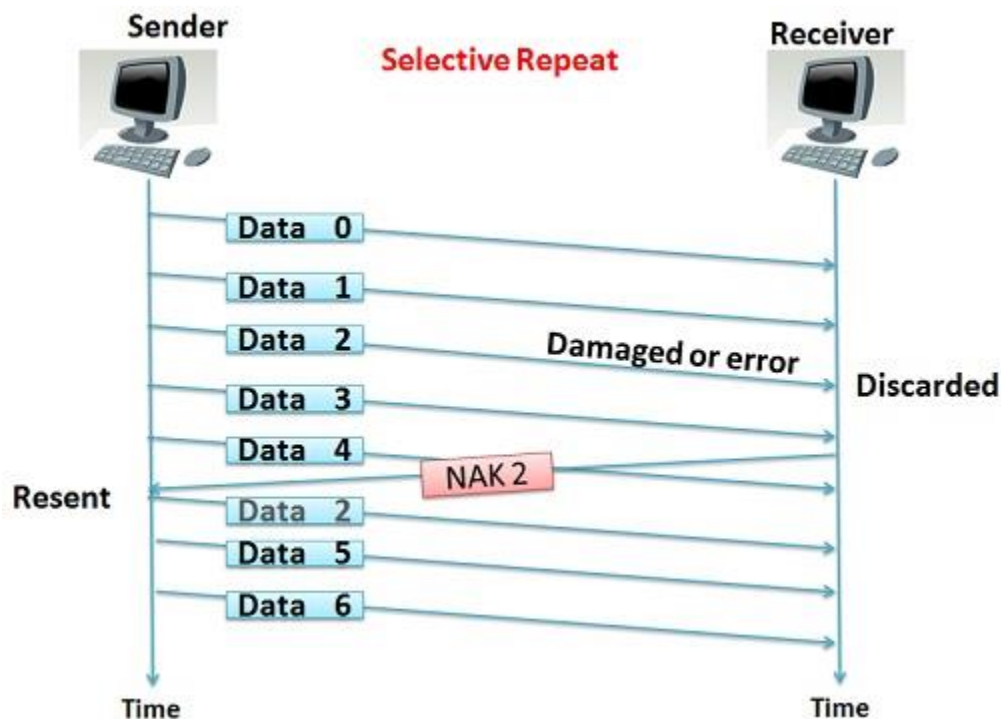
If the sender does not receive any ACK or if the ACK is lost or damaged in between the transmission. The sender waits for the time to run out and as the time run outs, the sender retransmits all the frames for which it has not received the ACK. The sender identifies the loss of ACK with the help of a timer.

The ACK number, like NAK (negative acknowledgement) number, shows the number of the frame, that receiver expects to be the next in sequence. The window size of the receiver is 1 as the data link layer only require the frame which it has to send next to the network layer. The sender window size is equal to 'w'. If the error rate is high, a lot of bandwidth is lost wasted.

#### Definition of Selective Repeat

Selective repeat is also the sliding window protocol which detects or corrects the error occurred in datalink layer. The selective repeat protocol retransmits only that frame which is damaged or lost. In selective repeat protocol, the retransmitted framed is received out of sequence. The selective repeat protocol can perform following actions

- The receiver is capable of sorting the frame in a proper sequence, as it receives the retransmitted frame whose sequence is out of order of the receiving frame.
- The sender must be capable of searching the frame for which the NAK has been received.
- The receiver must contain the buffer to store all the previously received frame on hold till the retransmitted frame is sorted and placed in a proper sequence.
- The ACK number, like NAK number, refers to the frame which is lost or damaged.
- It requires the less window size as compared to go-back-n protocol.



**6. Define fragmentation and explain why the IPV4 and IPV6 protocol need to fragment some packets.**

**IP fragmentation** is an Internet Protocol (**IP**) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.

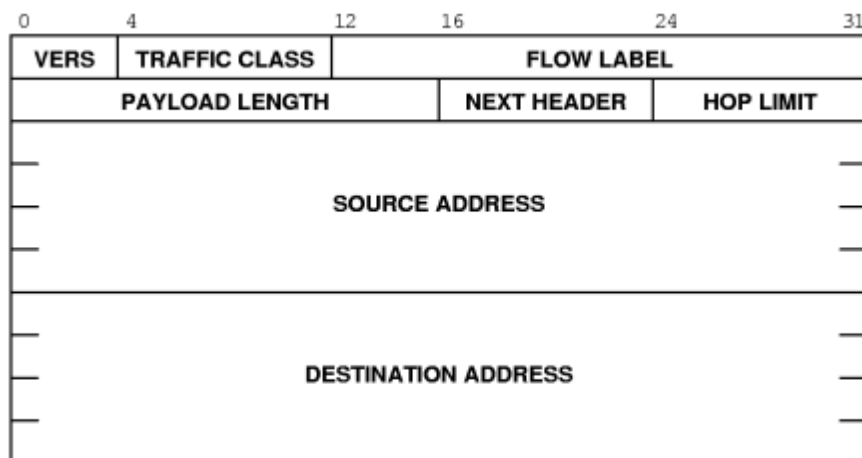
**IPV4:**

The router divides the packet into fragments. The max size of each fragment is the MTU minus the IP header size (20 bytes minimum; 60 bytes maximum). The router puts each fragment into its own packet, each fragment packet having following changes:

- The *total length* field is the fragment size.
- The *more fragments* (MF) flag is set for all fragments except the last one, which is set to 0.
- The *fragment offset* field is set, based on the offset of the fragment in the original data payload. This is measured in units of eight-byte blocks.
- The *header checksum* field is recomputed.

For example, for an MTU of 1,500 bytes and a header size of 20 bytes, the fragment offsets would be multiples of  $(1500-20)/8 = 185$

**IPV6:**



A packet containing a fragment of an original (larger) packet consists of two parts: the unfragmentable part of the original packet (which is the same for all fragments), and a piece of the fragmentable part of the original packet, identified by a Fragment Offset. The Fragment Offset of the first ("leftmost") fragment is 0.

The unfragmentable part of a packet consists of the fixed header and some of the extension headers of the original packet (if present): all extension headers up to and including

the *Routing* extension header, or else the *Hop-by-Hop* extension header. If neither extension headers are present, the unfragmentable part is just the fixed header.

The *Next Header* value of the last (extension) header of the unfragmentable part is set to 44 to indicate that a *Fragment* extension header follows. After the *Fragment* extension header a fragment of the rest of the original packet follows.

The first fragment(s) hold the rest of the extension headers (if present). After that the rest of the payload follows. Each fragment is a multiple of 8 octets in length, except the last fragment.

Each *Fragment* extension header has its *M* flag set to 1 (indicating more fragments follow), except the last, whose flag is set to 0.

**7. An organization has a class-C network with one of the IP addresses as 210.26.26.250. If the company wishes to form subnets for its 4 departments, say A, B, C, and D having equal number of addresses in the given order, then what are the values of the following:**

- a. The subnet mask
- b. Range of addresses in department C.
- c. The no. of addresses in each department.

a)  $210.26.26.250$   
 $11010010.11001011.11100101.11110110$   
 $11111111.11111111.11111111.00000000$   
 $11010010.11001011.11100101.00000000$   
 $210.26.26.0$  → starting address

Since this is a class C IP address we have to mask 24-bits (∵ 3 octets are network)

b) Range of address in dept of IT  
 Since we have 4 department we need two bits to address them (00, 01, 10, 11)

00	01
CSE	ECE
11	10
Mech	IT

	Starting Addr	Ending Addr
CSE	$210.26.26.0$	$210.26.26.63$
ECE	$210.26.26.64$	$210.26.26.127$
IT	$210.26.26.128$	$210.26.26.191$
Mech	$210.26.26.192$	$210.26.26.255$

Range of Address for IT  
 $210.26.26.128 - 210.26.26.191$

c) The no. of addresses in each dept (0-255)  
 Total No = 256  
 we have 4 depts  
 so no. of address in each dept =  $\frac{256}{4} = 64$

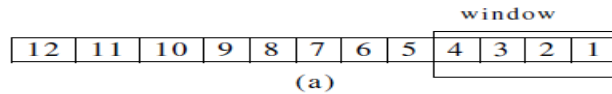
**8. Write short notes:**

**(i) Sliding Window Protocol.**

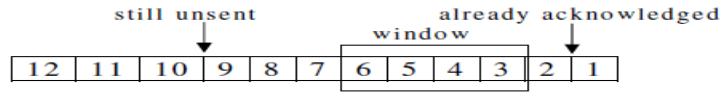
**Answer:**

To obtain high throughput rates, protocols use a flow control technique known as sliding window. The sender and receiver are programmed to use a fixed window size, which is the maximum amount of data that can be sent before an acknowledge arrives. For example, the sender and receiver might agree on a window size of four packets.

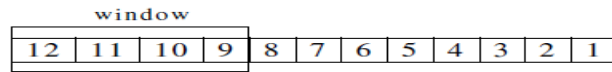




(a)



(b)



(c)

A 4-packet window sliding through outgoing data.

(a) When transmission begins (b) after two packets has been acknowledged, and (c) after eight packets have been acknowledged.

### 1. Write about Piggybacking Protocol?

#### Answer:

In some protocols data frames flow in only one direction although control information such as ACK and NAK frames can travel in the other direction. In real life, data frames are normally flowing in both directions, from node A to node B and from node B to node A. This means that the control information also needs to flow in both directions. A technique called piggybacking is used to improve the efficiency of the bidirectional protocols.

When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.