Name of Teacher: Miss Radhika M. Patil

Class: B.Sc. Computer Science (Entire)- III **Semester : 6**

Course Title: Computer Network

UNIT I: Data Link Layer and Network Layer

- **Sliding window protocol:**

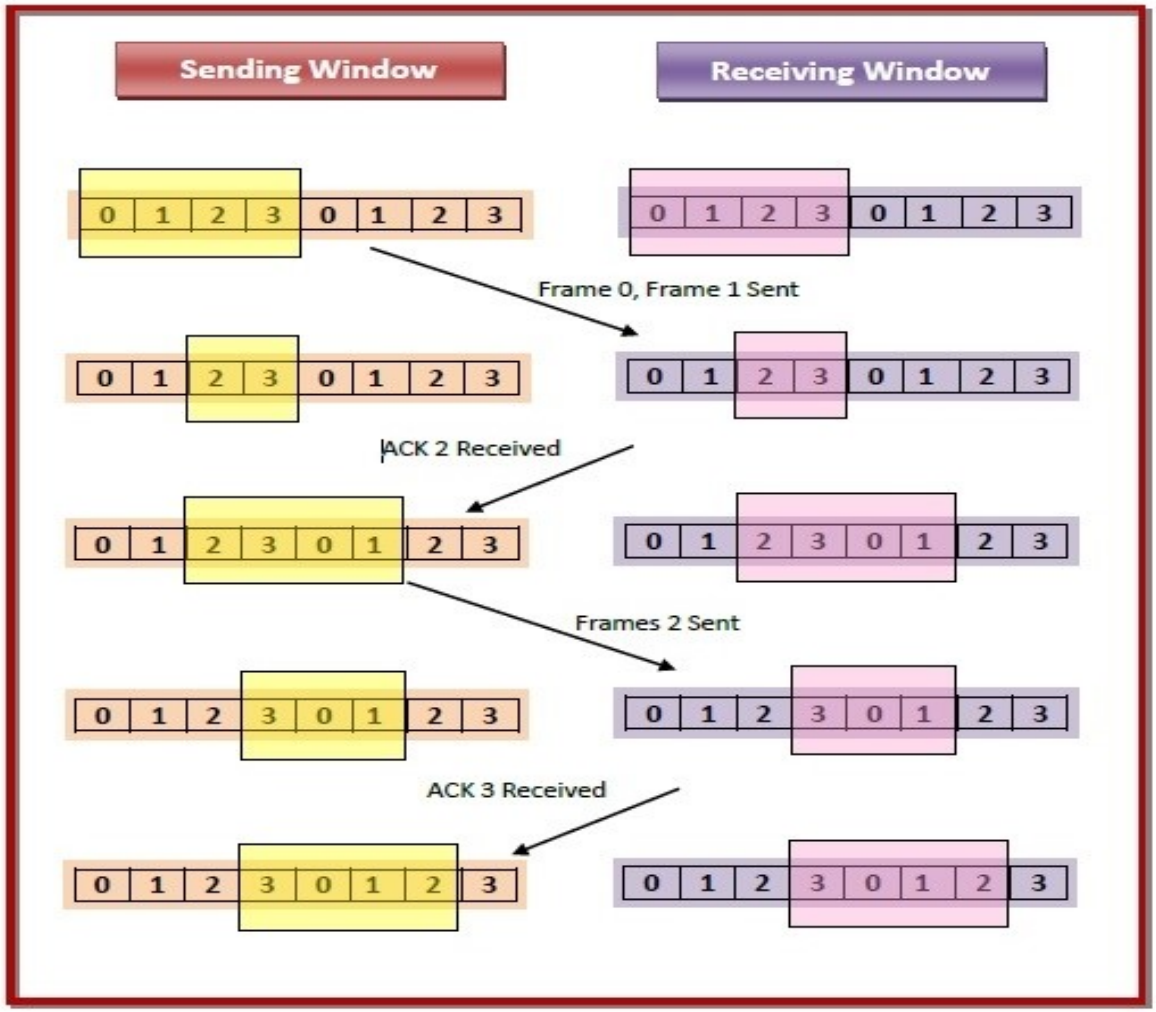
- Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames.
- The sliding window is also used in Transmission Control Protocol.
- In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.
- The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

- **Working Principle**

- In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
- The size of the sending window determines the sequence number of the outbound frames.
- If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1.
- Consequently, the size of the sending window is 2^n-1.
- Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.
- The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on.
- The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.
- The size of the receiving window is the maximum number of frames that the receiver can accept at a time.
- It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example

- Suppose that we have sender window and receiver window each of size 4.
- So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on.
- The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.

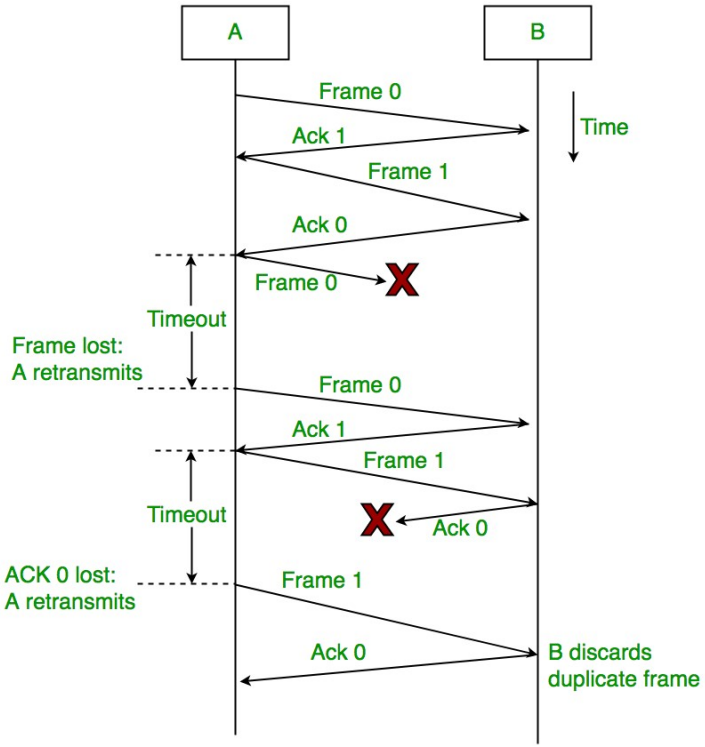


There are Three Sliding Window Protocols:

1. One bit sliding window Protocol
2. Protocol using Go-Back-N
3. Selective Repeat

1. One bit sliding window Protocol is also called as stop and wait ARQ (Automatic Repeat reQuest):

- In one – bit sliding window protocol, the size of the window is 1.
- This protocol provides for full – duplex communications.
- This is because the sender sends one frame and stops until it receives confirmation or ÁCK from the receiver & then sends the next frame.
- This Protocol specifies that frames need to be numbered.
- Frames have one bit sequence number i.e the sequence numbers are based on modulo-2 arithmetic. i.e. Sequence number of frame is either 0 or 1.
- e.g. If a frame 0 (zero) has arrived or received then the receiver sends an ACK frame with ACK 1 i.e. frame 1 is expected next.
- If a frame 1 (zero) has arrived or received then the receiver sends an ACK frame with ACK 0 i.e. frame 0 is expected next.



As shown in fig. 3 things may happen with this protocol:

1. Successful transmission of Frames:

Sender sends the frame to receiver and receiver successfully receives the frame and sends an ACK frame to sender.

2. If frame is lost:

Suppose the sender sends the frame and the frame is lost. The receiver is waiting for the frame for a long time. Since the frame is not received by the receiver, so it does not send any acknowledgment (ACK) to sender. Since the sender does not receive any acknowledgment so it will not send the next frame. This problem occurs due to the lost frame.

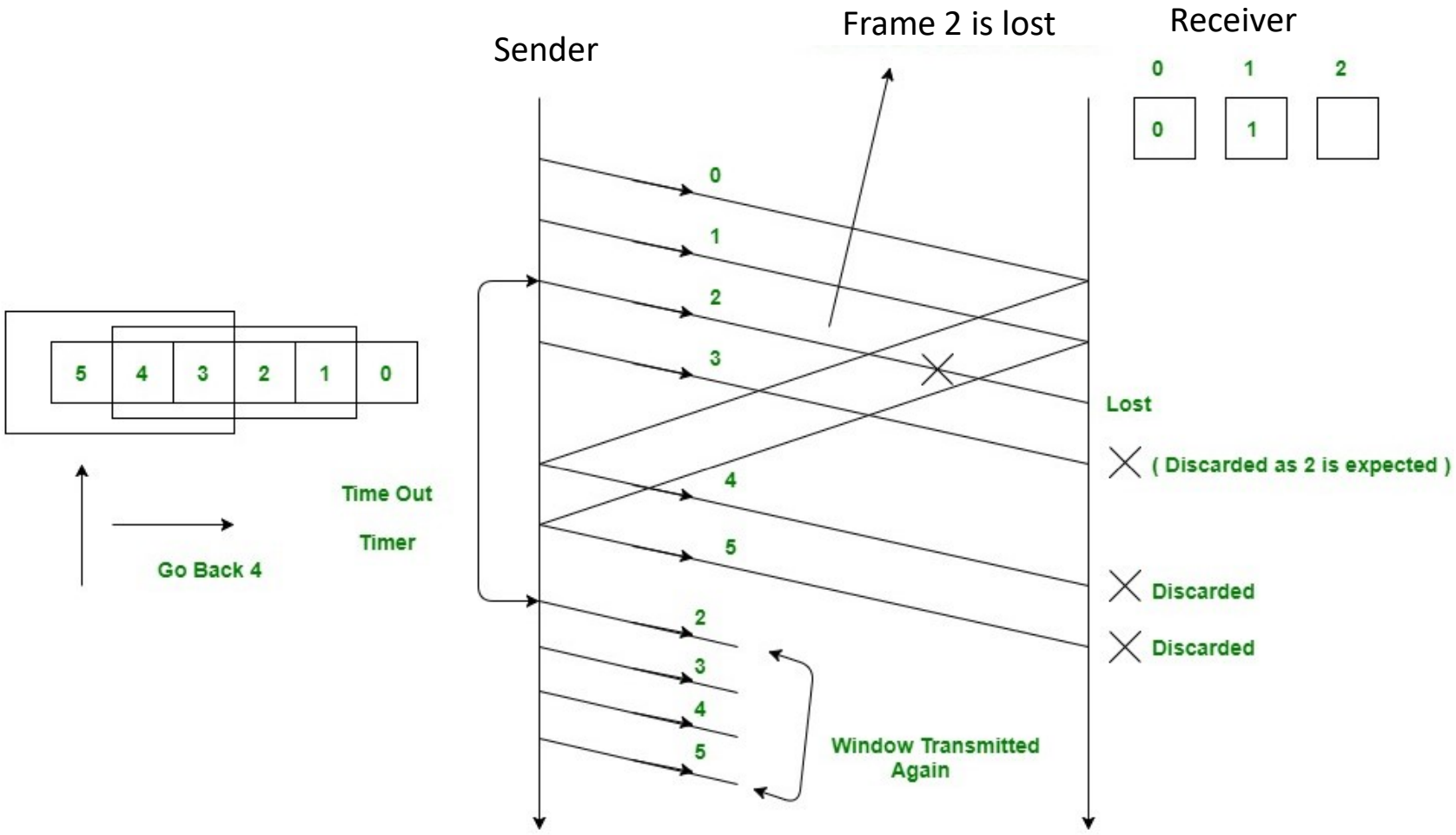
In this case sender starts a timer as soon as it sends the frame to the receiver , if ACK is not received within specified time interval then after timeout sender resends the same frame to the receiver.

3. If Acknowledgment is lost:

Suppose the sender sends the frame and it has also been received by the receiver. On receiving the frame, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next frame as the next frame cannot be sent until the acknowledgment of the previous frame is received. In this case after timeout sender resends the same frame. Note that the frame here is duplicate frame. The receiver discards the duplicate frame.

2. Protocol using Go-Back-N:

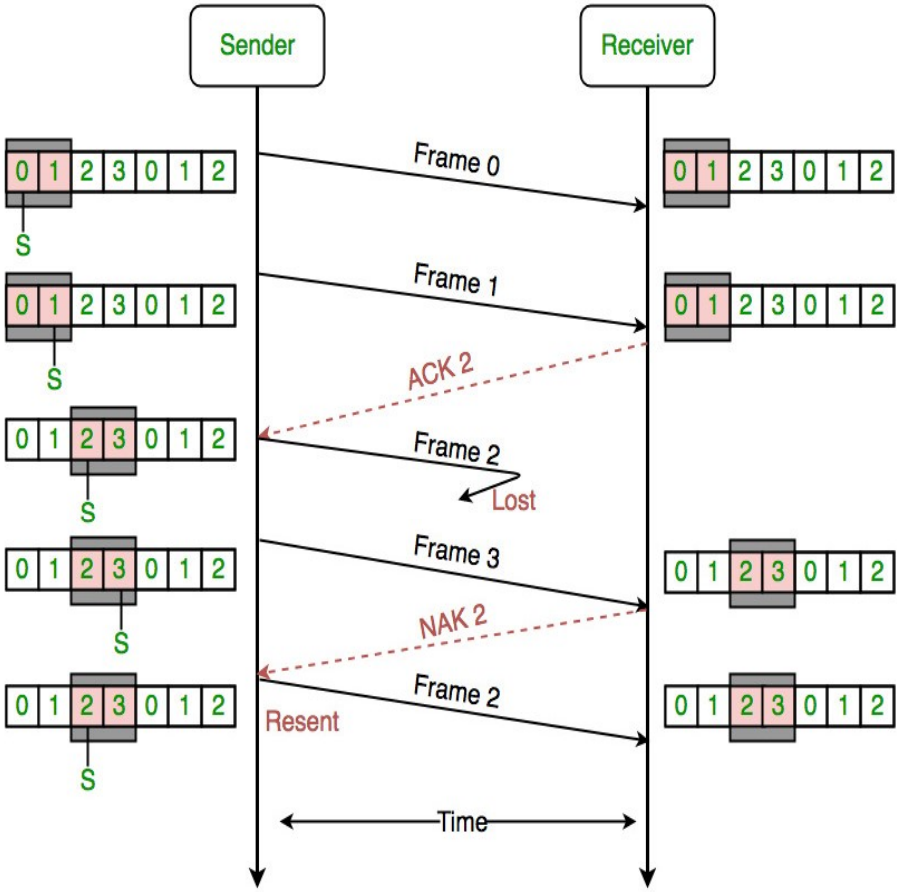
- It is the special case of sliding window protocol
- In Go-Back-N **sender's window size is N** and **receiver's window size is 1.**
- Sender can send N frames to the receiver before getting an acknowledgment.
- The receiver process keeps the track of frames that it expects to receive and send that number with every ACK it sends .
- The receiver accepts only those frames which are in order.
- e.g. After receiving frame 0 and frame 1 the next frame that receiver expects is frame 2.
- The receiver will discard any frame which does not have the exact sequence number it expects (i.e. a duplicate frame or out of order frame) and will resend the ACK for last corrected in order frame .
- Once the sender sends all the frames in its window it will detect that all of the frames since the first lost frame are outstanding and will go back to the sequence number of last acknowledged frame it received from the receiver.
- Go- Back –N is more efficient than stop and wait protocol
- This method also results in sending frames multiple times if any frame was lost or ACK was lost then that frame and all following frames in window will be resent.


Sender
Frame 2 is lost
Receiver
0
1
2
0
1
5
4
3
2
1
0
Time Out
Timer
Go Back 4
0
1
2
3
Lost
(Discarded as 2 is expected)
4
5
Discarded
Discarded
2
3
4
5
Window Transmitted
Again

- In above fig. after receiving frame 0 and frame 1 successfully , the receiver sends an ACK to sender.
- After that the receiver expects next frame i.e. frame 2.But suppose frame 2 is lost or damaged.
- In this case Go-Back-N protocol discards N frames (Here N=4) **including lost frame** .
- This is because in Go-Back-N protocol receiver accepts only those frames which are in order and discards the frames which are out of order.
- Frame 3 is received at receiver successfully, but frame 3 is received then receiver knows that frame 2 is lost or corrupted.
- After that frame 4 and frame 5 are received successfully but receiver discards all these frames to maintain the sequence or order of frames.
- In this case sender retransmits the N (in this example N=4) frames to the receiver before timeout of lost frame expires.
- Frames should be received in the order as they were sent.
- This method is called Go-Back-N because we are going back N frame from last frame to the corrupted frame and resends the N frames to the receiver.

3. Selective Repeat ARQ

- Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- The Go-back-N ARQ protocol works well if it has fewer errors.
- But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again.
- So, we use the Selective Repeat ARQ protocol.
- In this protocol, the **size of the sender window is always equal to the size of the receiver window**.
- The **size of the sliding window is always greater than 1**.
- If the receiver receives a corrupted frame, it does not directly discard it.
- It sends a **negative acknowledgment** to the sender.
- The sender sends that frame again as soon as on the receiving negative acknowledgment.
- There is no waiting for any time-out to send that frame.
- The design of the Selective Repeat ARQ protocol is shown below.



- As shown in this fig. after receiving the frames 0 and frame 1 Receiver send an ACK with sequence of next frame i.e. frame 2.
- Sender sends frame 2 and frame 3, but frame 2 is lost and frame 3 is received successfully.
- On receiving frame 3, receiver knows that frame 2 is lost and it sends negative ACK with sequence number of lost frame to the sender instead of discarding the out of frame (in this case frame 3).
- After that sender retransmits the frame 2 to the receiver.

- **Network Layer:**

➢ **Functions of Network Layer:**

1. Addressing:

Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.

2. Packeting:

This is performed by Internet Protocol. The network layer converts the packets from its upper layer.

3. Routing:

It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.

4. Inter-networking:

It works to deliver a logical connection across multiple devices.

- **Network Layer Design Issues**

1. Store-and-Forward Packet Switching
2. Services Provided to the Transport Layer
3. Implementation of Connectionless Service
4. Implementation of Connection-Oriented Service
5. Comparison of Virtual-Circuit and Datagram Subnets

1. Store-and-Forward Packet Switching

Here, the elements are the carrier's equipment (the connection between routers through transmission lines) and the customer's equipment.

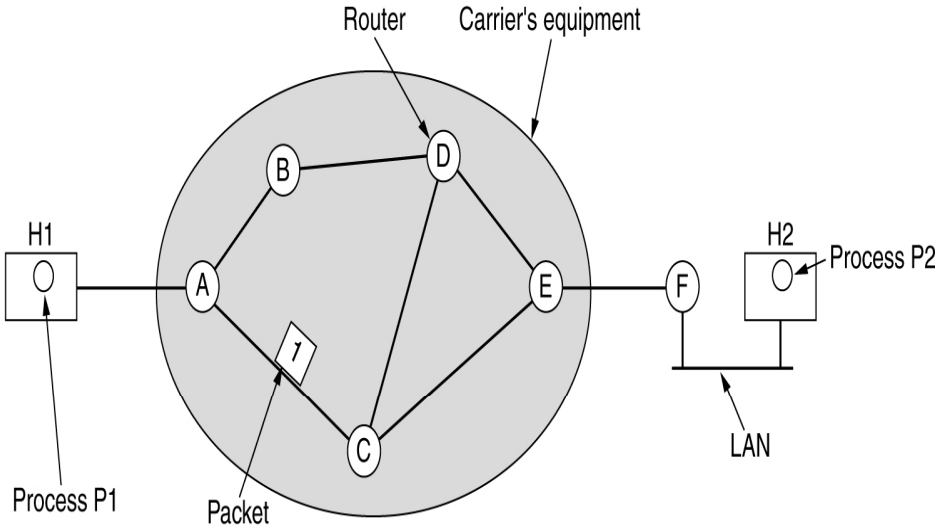


Fig. Store-and-forward packet switching

- H1 has a direct connection with carrier router 'A', while H2 is connected to carrier router 'F' on a LAN connection.
- One of the carrier router 'F', is pointed outside the carrier's equipment as it does not come under the carrier, whereas considered as protocols, software, and construction.
- This switching network performs as Transmission of data happens when the host (H1) with a packet transfers it to the nearby router through LAN (or) point-to-point connection to the carrier.
- The carrier stores the packet until it completely arrives.
- Then after, the packet is transmitted over the path until H2 is reached.

2. Services Provided to the Transport Layer:

- Through the network/transport layer interface, the network layer delivers its services to the transport layer. One might come across the question of what type of services does the network layer provides?
- Here, two groupings are possible based on the offered services.

1. <u>Connectionless</u> **:** Here, routing and insertion of packets into subnet is accomplished individually. No additional setup is necessary

2. <u>Connection-Oriented</u> **:** Subnet must offer reliable service and all the packets are transmitted over a single route.

3. Implementation of Connectionless Service

- In this scenario, packets are termed as datagrams and the corresponding subnet is termed as datagram subnet.
- Routing in datagram subnet is as follows:

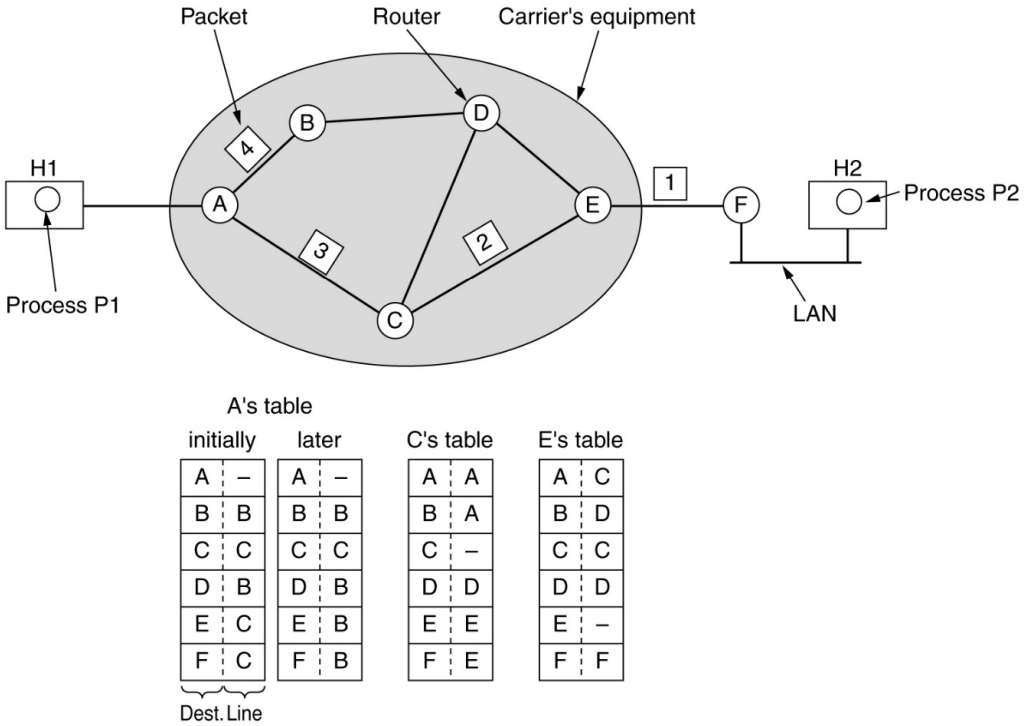


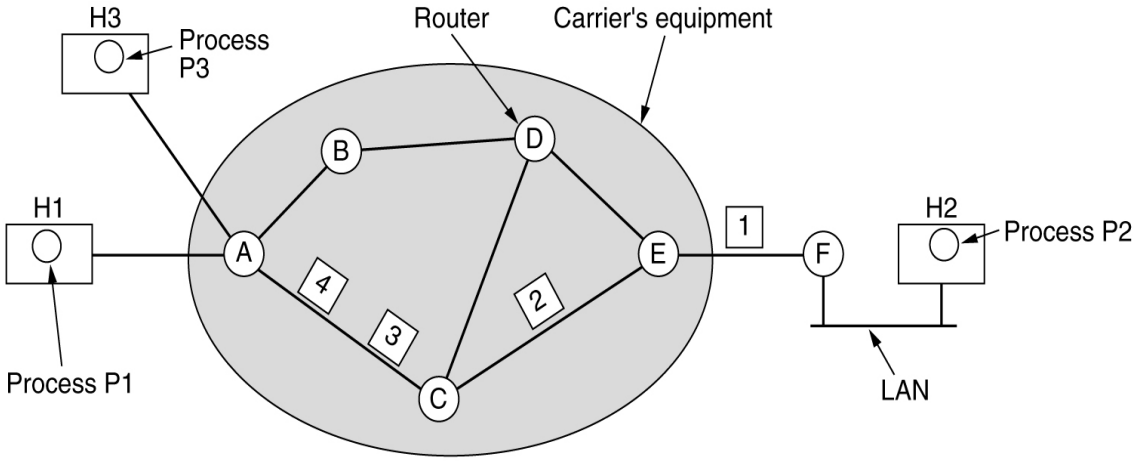
Fig. Routing within a diagram subnet

- Each router is provided with a routing table where it decides the destination points.
- No connection setup
- Message is broken into packets called datagram
- Each packet is individually routed
- Routers decides line based on routing table
- Packets may follow different paths
- Packet may not be guaranteed to arrive in order

4. Implementation of Connection-Oriented Service

- Path from source to destination must be established before any data can be sent
- Connection is called a VC (Virtual Circuit)
- E.g. physical circuit in phone system
- Avoid choosing new route for each packet
- Same route used for all packets in connection
- Each packet has ID for which VC it belongs to

Example:



A's table

In		Out	
H1	1	C	1
H3	1	C	2

C's table

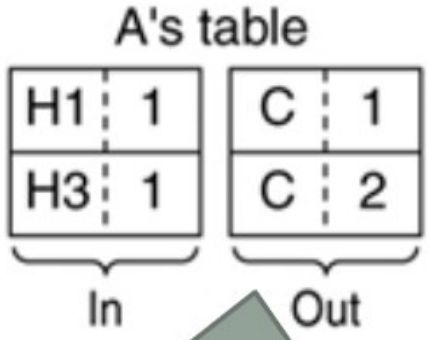
A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

- H1 has established connection 1 with H2
- First entry in each routing table
- H3 later establishes connection with H2
- 'A' can easily know connection 1 packets of H1 from connection 1 packets of H3
- C can not do this
- Thus, A assigns different connection ID to outgoing traffic for second connection
- To avoid conflicts, routers need ability to replace connection IDs in outgoing packets
- This is called label switching.

If packet with ID 1 comes from H1
Send it to router C, give it ID 1



If packet with ID 1 comes from H3
Send it to router C, give it ID 2
Why ID 2?

5. Comparison of Datagram subnet and Virtual Circuit Subnet

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

- **Routing**

- Routing is a process of selecting path along which the data/packet can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets.
- The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery.
- The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

- **Routing Metrics**

- Routing metrics are used for determining the best route to the destination.
- The factors used by the protocols to determine the shortest path, these factors are known as a metric.

The most common metric values are given below:

1. Hop count:

- Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination.
- If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.

2. Delay:

- It is a time taken by the router to process, queue and transmit a datagram to an interface.
- The protocols use this metric to determine the delay values for all the links along the path end-to-end.
- The path having the lowest delay value will be considered as the best path.

3. Bandwidth:

- The capacity of the link is known as a bandwidth of the link.
- The bandwidth is measured in terms of bits per second.
- The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb.
- The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.

4. Load:

- Load refers to the degree to which the network resource such as a router or network link is busy.
- A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second.
- If the traffic increases, then the load value will also be increased.
- The load value changes with respect to the change in the traffic.

5. Reliability:

- Reliability is a metric factor may be composed of a fixed value.
- It depends on the network links, and its value is measured dynamically.
- Some networks go down more often than others.
- After network failure, some network links repaired more easily than other network links.

- **Types of Routing**

Routing can be classified into three categories:

1. Static Routing
2. Default Routing
3. Dynamic Routing

1. Static Routing

- Static Routing is also known as Non adaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

- **Advantages Of Static Routing**

Following are the advantages of Static Routing:

1. **No Overhead:** It has no overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
2. **Bandwidth:** It has not bandwidth usage between the routers.
3. **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

- **Disadvantages of Static Routing:**

Following are the disadvantages of Static Routing:

1. For a large network, it becomes a very difficult task to add each route manually to the routing table.
2. The system administrator should have a good knowledge of a topology as he has to add each route manually.

2. Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not.
- A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hop device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

3. Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- If any route goes down, then the automatic adjustment will be made to reach the destination.
- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

- **Advantages of Dynamic Routing:**

1. It is easier to configure.
2. It is more effective in selecting the best route in response to the changes in the condition or topology.

- **Disadvantages of Dynamic Routing:**

1. It is more expensive in terms of CPU and bandwidth usage.
2. It is less secure as compared to default and static routing.

THANK YOU…