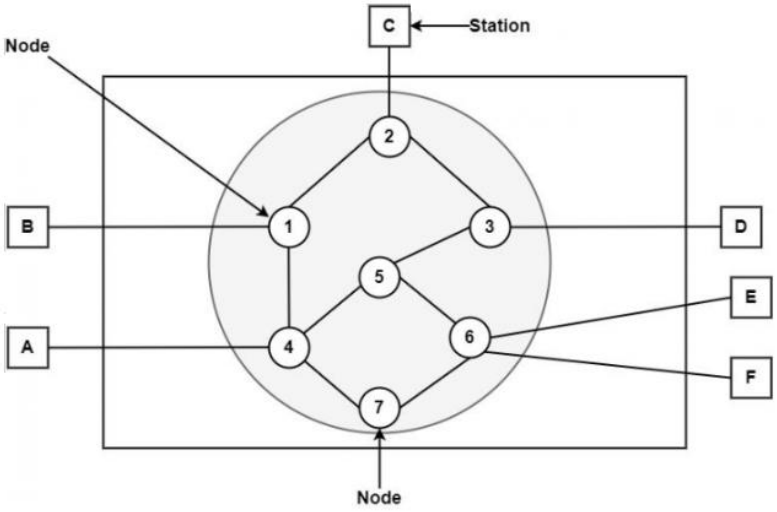
UNIT - III

3.1 CIRCUIT SWITCHING

It is a dedicated connection path between the sending and receiving devices. The dedicated route is a connected series of connections between the switching nodes.

A traditional mobile network, where a dedicated route is established between the caller and the called party for the span of a mobile call, is termed as circuit switching.



3.1.1 PHASES

It has three phases, **Circuit Establishment, Data Transfer** and **Circuit Disconnect**

i. Circuit Establishment

A circuit switching network is necessary to establish an end-to-end link before any signal is transmitted. For example, if the communication is between A and D, then the path from A to node 4 to node 5 to node 3 and D must be established first.

ii. Data Transfer

Once a circuit is established between the two stations, it is exclusively used by the two parties. The information can be transferred from A to D through the network. The data can be analog or digital, relying on the features of the network.

iii. Circuit Disconnect

After the transfer of complete data, the connection is terminated either by the sender or receiver.

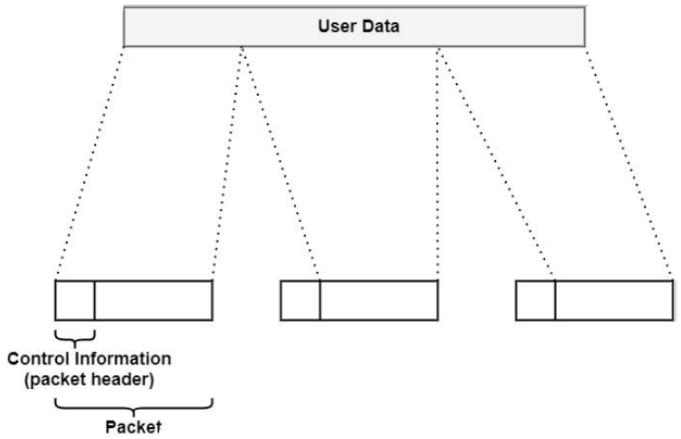
Advantages

- During the circuit is settled, data is communicated with no delay.
- The approach is feasible for high infinite communication, because a dedicated endless communication route is settled.
- The approach is easy and does not require specific facilities.

Disadvantages

- The time needed to settle a physical connection between the two stations is considerable.
- The network resources are not adequately utilised, because the physical connection is a dedicated one.
- It is an uneconomical method.

3.2 PACKET SWITCHING merges the benefit of the message and circuit switching. Long messages are divided into smaller units known as packets.



A question appears as to how the network will manage this flow of packets as it tries to path them through the network and transfer them to the planned designation. In a packet-switched network, data is transmitted in discrete units of potentially variable length of blocks known as packets. The maximum length of packets depends on the network. In this, longer size messages are broken into multiple packets. Each packet contains the data with a header. The header includes the control information like priority, source and destination addresses etc.

3.2.1 METHODS

It has two methods, **i). Datagram Packet switching** **ii). Virtual Circuit Switching**

i). Datagram Packet Switching

A packet-switching technology in which a packet is called a datagram. It is treated as a separate entity. Each packet includes data about the destination, and the switch helps this data to forward the packet to the right destination. It is also known as connectionless switching.

ii). Virtual Circuit Switching

Virtual Circuit Switching is also referred to as connection-oriented switching. A fixed, consistent direction through the transmitter's network is settled in the virtual circuit method. The packets are transmitted earlier. This direction remains constant for the session period.

Advantages

- Storage requirement at intermediate nodes is minimal because the packets are of small & fixed size.
- Transmission is high-speed.
- This method is quick enough for interactive/real-time software.
- Line adaptability is superior.
- When traffic becomes heavy, the packet is accepted, but the delivery delay increases.

Disadvantages

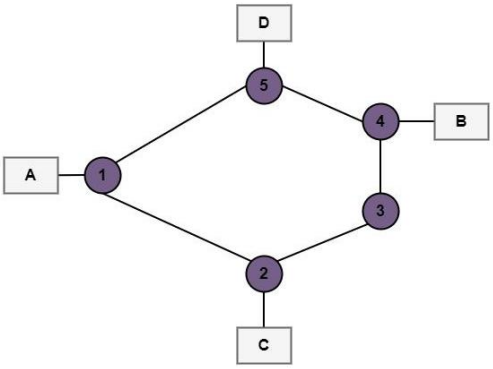
- The packet switching method can suffer from congestion when nodes accept more packets than the outgoing links can transmit.
- Processing and control procedures are more complex.
- Transmission overhead is increased, because each packet requires an address and control header.

3.3 MESSAGE SWITCHING

The sending device joins the destination location to the communication and develops it to the network. The message is then generated by the web from one node to the other node, because it arrives at the predetermined destination.

Each switching hub gets a message, stores it momentarily and afterward, sends it to the following hub, as shown in the diagram below.

An example of message switching is emails, PC documents, telegrams and transaction queries and responses. A full exchange can include various messages.



If a message is transmitted from station A to station B, it can take either path 1-2-3-4 or 1-5-4 depending on the free output path's availability at that particular moment.

Advantages

- There is no physical link between the source and the destination hub.

- This method facilitates communication medium very efficiently, because the channels are used when messages are sent.

Disadvantages

- As the message length is unlimited, and each node must have sufficient storage to store the messages.
- This method is very low for interactive real-time applications.
- Processing and control procedures are more complex.
- Transmission overhead is increased, because each message requires an address and control header.
- A message is delayed at each node.

3.4 Difference between Circuit Switching, Message Switching & Packet Switching

Basics	Circuit Switching	Message Switching	Packet Switching
Connection Creation	Connection is created between the source and destination by establishing a dedicated path between source and destination.	Links are created independently one by one between the nodes on the way.	Links are created independently one by one between the nodes on the way.
Queuing	No queue is formed.	Queue is formed.	Queue is formed.
Message and Packets	There is one big entire data stream called a message.	There is one big entire data stream called a message.	The big message is divided into a small number of packets.
Routing	One single dedicated path exists between the source and destination.	Messages follow the independent route to reach a destination.	Packets follow the independent path to hold the destination.

Basics	Circuit Switching	Message Switching	Packet Switching
Addressing and sequencing	Messages need not be addressed as there is one dedicated path.	Messages are addressed as independent routes are established.	Packets are addressed, and sequencing is done as all the packets follow the independent route.
Propagation Delay	No	Yes	Yes
Transmission Capacity	Low	Maximum	Maximum
Sequence Order	Message arrives in Sequence.	Message arrives in Sequence.	Packets do not appear in sequence at the destination.
Use Bandwidth	Wastage	Bandwidth is used to its maximum extent.	Bandwidth is used to its maximum extent.

To send the data from one device to another device there should be a connection. The connection can be established to **transfer data between the devices** can be done in two ways and they are as follows

- Connection Oriented Service
- Connectionless Services

3.5 CONNECTION ORIENTED SERVICE (Data Transfer)

Connection oriented is **TCP** protocol. In connection-oriented services, the devices at both the endpoints use a protocol to establish an end-to-end connection before sending any data. We have to establish a connection before starting the communication in connection oriented service. Whenever the connection is established we can send the message and after that we can release the connection. Connection oriented service is more reliable than connectionless service. In connection oriented service we can also send the message if there is an error at the receiver's end.

Stages for Connection-oriented Transmission

i) **Connection is established**

ii) **Information is sent**

iii) **Connection is released**

i). Connection Establishment

Before transmitting data in connection oriented, the sending device has to determine the availability of the other device to exchange data and a connection has to be established by which data can be sent.

Generally the Connection establishment requires the following **three steps** −

- First sender computer requests the connection by sending a connection request packet to the intended receiver.
- After that, the receiver computer returns a confirmation packet to the requesting computer.
- Finally, the sender computer returns a packet acknowledging the confirmation.

ii). Data transfer

The sender starts sending data packets to the receiver after the connection is established.

iii). Connection Termination

When all the data gets transferred, the connection has to be terminated. This connection termination requires a **three-way** handshake.

- First, the sender computer requests disconnection by sending a disconnection request packet.
- After that, the receiver computer confirms the disconnection request.
- Finally, the sender computer returns a packet acknowledging the confirmation.

3.6 CONNECTION LESS SERVICES

Connectionless service is **UDP** (User Datagram Protocol) protocol.

- In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it is prepared to accept the message. Authentication is not needed in this.
- It allows the transfer of information among subscribers without the need for end-to-end connection establishment procedures.

- Connection-less service is sometimes known as “unreliable” network service. Connectionless protocols are usually described as stateless because the endpoints have no protocol-defined way of remembering where they are in a “conversation” of message exchange.
- It is a data transmission service provided by the network and transport layer protocols.
- Connectionless service is based on the postal service.

Example − postal service, where the letter has source and destination address and each one of the letter routed through different paths to reach the destination. In connectionless service, each packet of the same message **may follow a different route** to get delivered to the destination. In connectionless service, packets are routed **based on the destination address** on the packet.

3.7 DIFFERENCES

Connection Oriented Services	Connectionless Services−
It can generate an end to end connection between the senders to the receiver before sending the data over the same or multiple networks.	It can transfer the data packets between senders to the receiver without creating any connection.
It generates a virtual path between the sender and the receiver.	It does not make any virtual connection or path between the sender and the receiver.
It needed a higher bandwidth to transmit the data packets.	It requires low bandwidth to share the data packets.
There is no congestion as it supports an end-to-end connection between sender and receiver during data transmission.	There can be congestion due to not providing an end-to-end connection between the source and receiver to transmit data packets.
It is a more dependable connection service because it assures data packets transfer from one end to the other end with a connection.	It is not a dependent connection service because it does not ensure the share of data packets from one end to another for supporting a connection.

3.8 ROUTING ALGORITHM

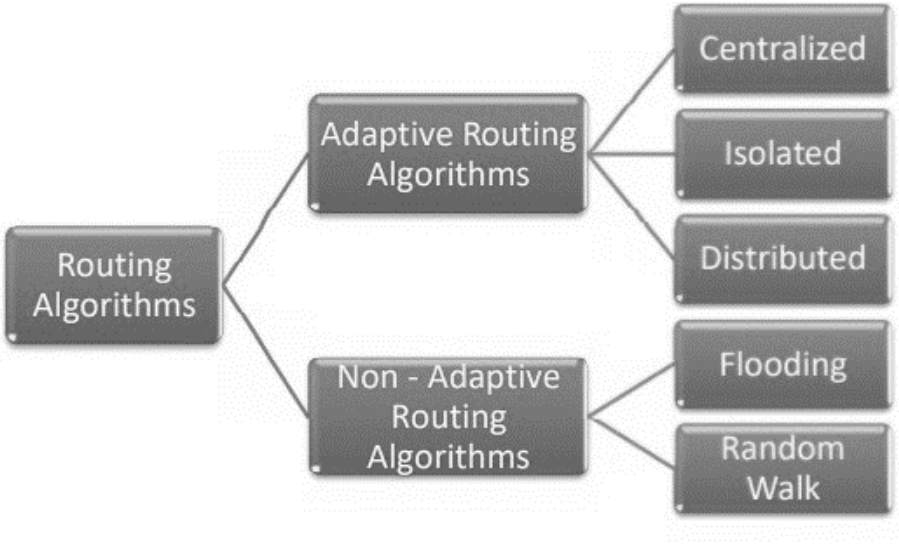
- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.

- 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.

Types of Routing Algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm



Adaptive Routing Algorithms

Adaptive routing algorithms, also known as dynamic routing algorithms, makes routing decisions dynamically depending on the network conditions. It constructs the routing table depending upon the network traffic and topology. They try to compute the optimized route depending upon the hop count, transit time and distance.

The three popular types of adaptive routing algorithms are −

- **Centralized algorithm** − It finds the least-cost path between source and destination nodes by using global knowledge about the network. So, it is also known as global routing algorithm.

- **Isolated algorithm** − This algorithm procures the routing information by using local information instead of gathering information from other nodes.
- **Distributed algorithm** − This is a decentralized algorithm that computes the least-cost path between source and destination iteratively in a distributed manner.

Non – Adaptive Routing Algorithms

Non-adaptive Routing algorithms, also known as static routing algorithms, construct a static routing table to determine the path through which packets are to be sent. The static routing table is constructed based upon the routing information stored in the routers when the network is booted up.

The two types of non – adaptive routing algorithms are −

- **Flooding** − In flooding, when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled, controlled or selective flooding.
- **Random walks** − This is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbours randomly.

3.9 CONGESTION CONTROL ALGORITHM

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

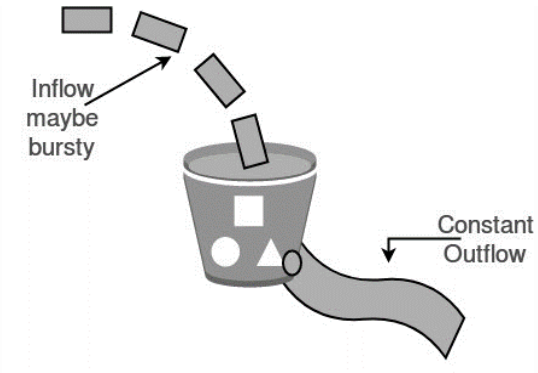
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Types of Congestion Control Algorithms

1. Leaky Bucket Algorithm **2. Token bucket Algorithm**

1. Leaky Bucket Algorithm

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Steps of leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

2. Token bucket Algorithm

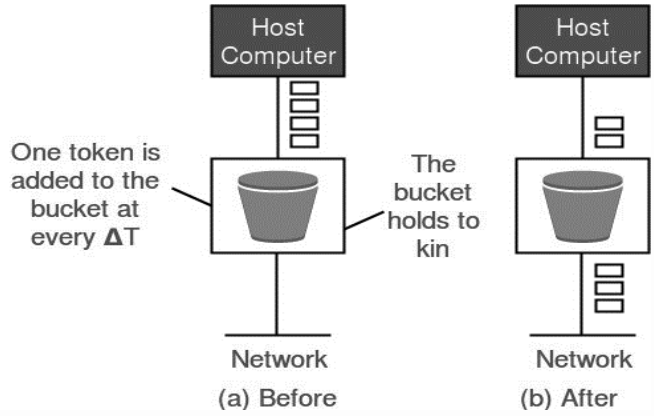
The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm:

1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.



Ways in which token bucket is superior to leaky bucket:

The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: $M * s = C + \rho * s$

where S – is time taken

M – Maximum output rate

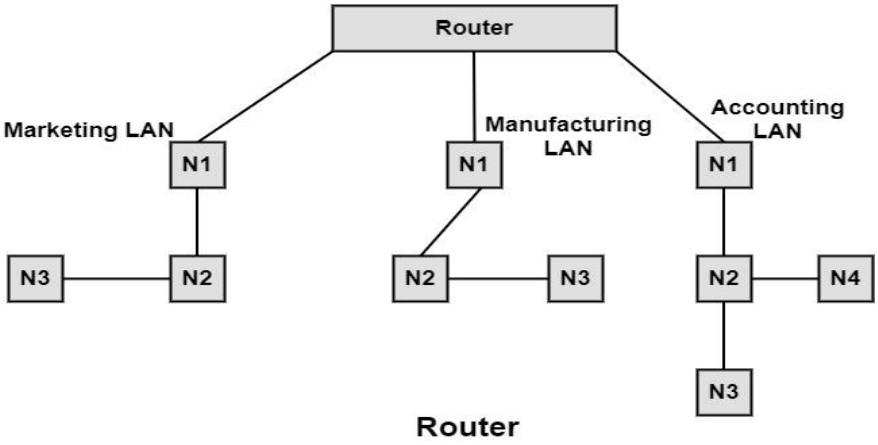
ρ – Token arrival rate

C – Capacity of the token bucket in byte

Let's understand with an example,

3.10 ROUTERS IN INTERNETWORKING

Router is a particular type of device used to connect two or more subnets that cannot be similar. These devices support connectedness between two LANs or two WANs over the large geographical range. The routers evaluate the best route from a sender to a receiver.

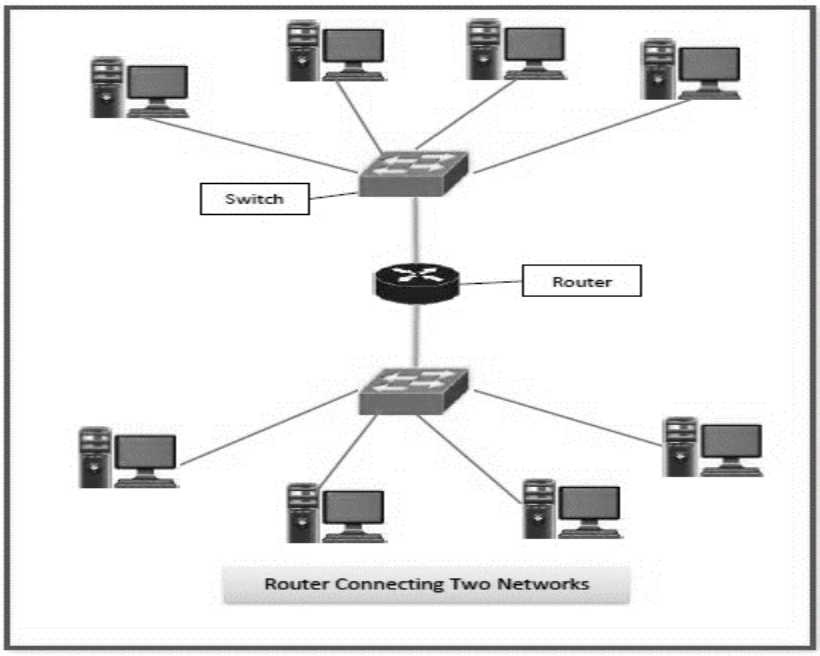


Router

For this, they perform in a routing protocol to create the network topology, and the data thus gathered is used to evaluate routes. They operate at the OSI model's network layer and accommodate all the sub networks differences up to this layer to provide a uniform network service to the nodes transport layer entities.

Routers are generally a mixture of hardware and software. The hardware includes physical interfaces to various networks, while the software consists of operating system and routing protocol. They use both logical and physical transmitting to link two or more logically separated networks. The figure shows three types of LANs connected by a single router.

For this, each network to be connected is allocated a logical address, and then these logical segments are combined by the router in a large network. They use the store and forward technique to transmit the message, i.e., receive messages, check their destination and send the needed LAN message.



Types of Routers

Central Router

Central router is a router that acts as the backbone of a network. It connects many LANs.

Local Router

The local router has limitations to operate within the limits of its LAN driver's cable length limitations.

Remote Router

A remote router uses modems or remote connections to connect the LANs beyond its device driver limitations.

Internal Router

Internal router is a part of the network file server, and it routes the data accordingly.

External Router

The external router is located in a workstation on the network.

Peripheral Router

The peripheral router link single LANs to a central router or sometimes to another peripheral router.

Features of Routers

- Routers are multiport tools with huge speed backbones.
- It is used to provide penetrating and encapsulation like bridges.

- Routers continuously monitor the network's condition to adapt to changes in the network's condition dynamically.
- They generally support some method of redundancy so that they are less prone to catastrophic failure.

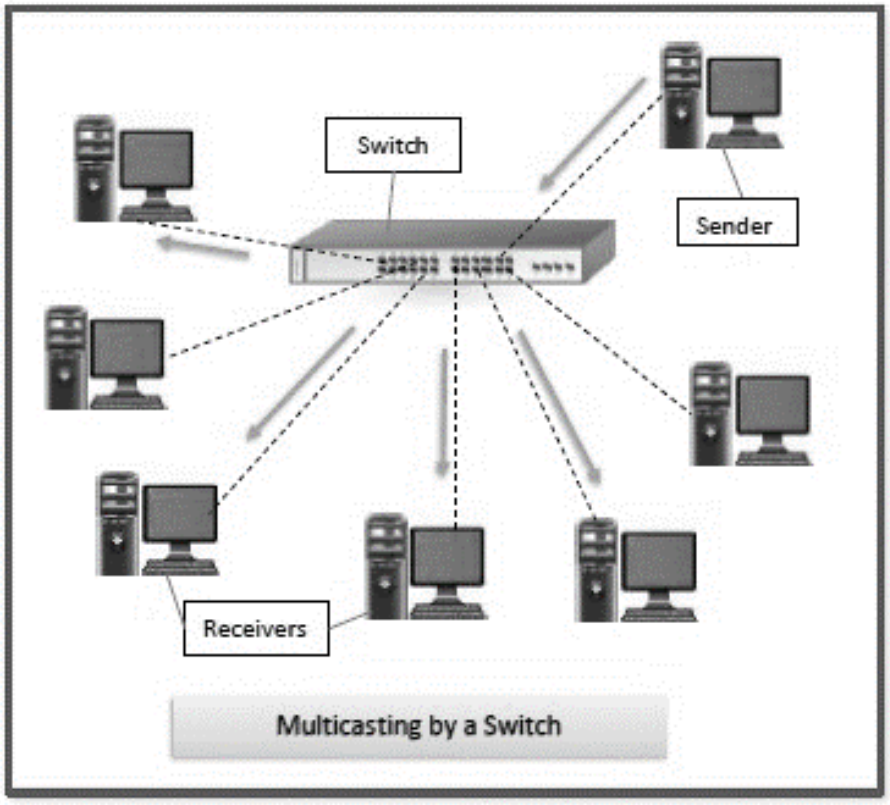
Types of Routers

- **Wireless Router** − They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers** − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers** − They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers** − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
- **Brouters** − Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

3.11 SWITCHES IN NETWORKING

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

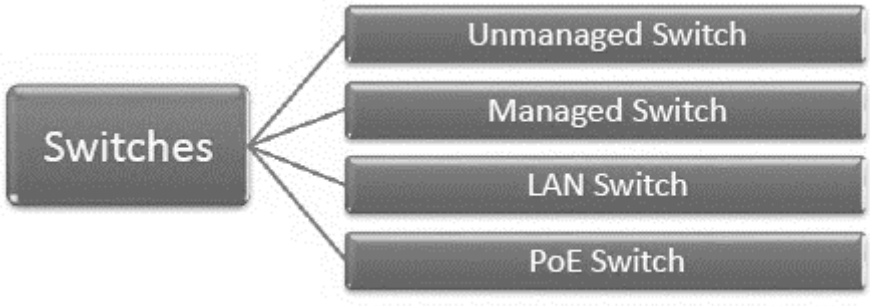
A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.



Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types of Switches



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

3.12 INTRODUCTION OF FIREWALLS

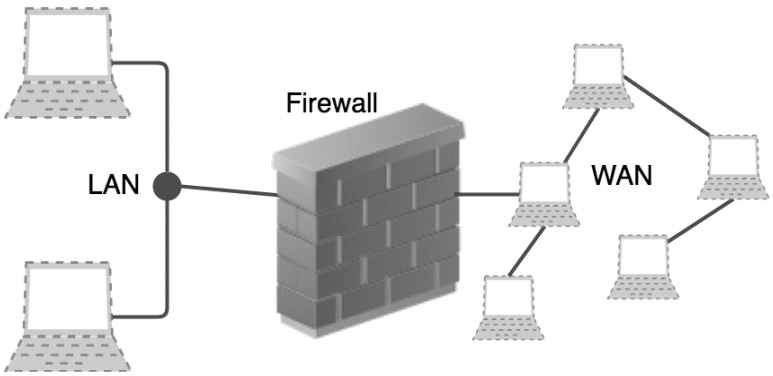
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept: allow the traffic

Reject: block the traffic but reply with an "unreachable error"

Drop: block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.

But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall

maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).

Generation of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).

   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only it can allow or deny the packets based on unique packet headers.

   Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.

2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

2. **Second Generation- Stateful Inspection Firewall:** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. **Third Generation- Application Layer Firewall:** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

~~~~ The End - Unit-III ~~~~~