Unit - III Network Layer & Transport Layer

(#) Network Layer

- The network layer is the 5th layer from the top and 3rd layer from the bottom of the OSI Model
- It is one of the most important layer which plays a key role in data transmission.
- The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination

(#) Function of Network Layer

(1) Assigning logical address

Network layer is responsible for assigning logical address to devices which are either sending or receiving data packets. The data packets sent or received consist the IP address of both senders and receiver's device

(2) Routing

Routing is the process of identifying the best path to transmit the packet, Network layer not only just sends packets from sender to receiver, but also determine the best route to send them.

③ Host - to - Host delivery

Host - to - Host delivery also known as Forwarding is the process in which the network layer transmits or forward the data packet via routers after determining the best route.

④ Logical Subnetting

Network layer also allows a bigger network to be divided into smaller network known as logical subnetting. It help IP address to be used more effeciently.

⑤ Error Handling

Network layer also check for error and handles them. Network layer uses various error detection technique like CRC, Checksum etc.

⑥ Network Address Translation (NAT)

Network address translation (NAT) means that it converts any private IP address into a public IP address which is required to communicate between the sender and the receiver.

Advantages

→ Easy to transmit data over network because it breaks down the data into packets.

→ Router is the important component of network layer because it reduces network congestion.

→ Used to send data packets across the network nodes

Disadvantages

→ There is no flow control mechanism provided by network layer.

→ Important data may be lost in this process.

→ Indirect control cannot be implemented at the network layer.

Networking and Internetworking Devices

- Network devices are component used to connect computer or other electronic devices together so that they can share files or resources like printer. Ex - LAN

- An Internetwork is a collection of individual network, connected by intermediate networking devices, that function as a single large network.

Devices :-

① Access Point

A wireless access point (WAP) is a networking device that allows connecting the device with the wired network. A WAP is used to create wireless local area network (WLAN) It is commonly used in large offices and building which have expanded businesses

- It is easier and simpler to understand and implement the device

Advantages
→ More user access
→ Broader transmission Range
→ flexible networking

Disadvantage
→ High cost
→ Poor stability
→ Limited range

② Modem

Modem stands for modulator / demodulator. The modem is defined as a networking device that is used to connect device connected in a network to the internet.

- Modem is used to convert digital signal into analog signal of different frequencies and transmit these signal to a modem at the receiving location

Advantage
→ It helps to connect LAN to the internet
→ Perform both modulation & demodulation process simultaneously

Disadvantage
→ Modem slows down when connected to Hub
→ limited number of network device connected to internet

Types of Modem

- DSL Modem
  Uses regular phone lines to connect to internet
- Cable Modem
  Sends data through TV cables, providing faster internet
- Wireless Modem
  Connect device to the internet using wi-fi
- Cellular Modem
  Connect to internet using mobile data from cellular network

③ Firewall

A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization.

- Based on defined set of security rules

  ↳ Accept - allow the traffic
  ↳ Reject - block the traffic but reply with "unreachable error"
  ↳ Drop - block the traffic with no reply.

④ Repeater

A repeater operates at the physical layer. Its main function is to amplify the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.

Features

- Repeater regenerate signal without modyfying it.
- Repeaters can be used in analog signal and digital signal.
- Repeaters can extend the range of network.
- Repeaters reduces error and loss of data
- Repeaters used in various wireless technologies such as wi-fi and wired technologies such as ethernet.

Advantage

→ Better performance of network
→ Cost effective
→ Extend the network
→ Enhanced signal

Disadvantage

→ Network traffic
→ Network segmentation
→ Limited number of repeaters

⑤ HUB

HUB is a networking device plays a vital role in data transmission and broadcasting. A hub is a hardware device used at physical layer to connect multiple device in a network.

- Hub are widely used to connect LANs.

Types of HUB

→ Active Hub

They have a power supply for regenerating and amplyfying the signal. It regenerates the signals then send it to other ports.

→ Passive Hub

Passive hub are simply used to connect signals from different network cables as they do not have any computerised element. This do not have any regeneration signal.

→ Intelligent Hub

The intelligent hub comprises a special moni-toring unit named a Management Information base (MIB). This is the s/w that helps in analysing and troubleshooting network problem.

Advantage

- It is less expensive
- Does not impact network performance
- It support different network media

Disadvantage

- It cannot find shortest path of network
- No mechanism for traffic detection.
- No mechanism for data filteration.

⑥ Bridge

A Bridges is a network device that connect and filter traffic between two or more network segment. It operates at data link layer of OSI Model.

- Bridges connect two network in well organized manner.
- Bridges are used to extend LAN.

Types

→ Transparent Bridge

Automatically connect and filter traffic between network segment

→ Source Routing Bridge

Used in network where the sender defines the data path

→ Translational Bridge

Connect different types of network

→ Wireless Bridge

Connect two network wirelessly over long distance

Advantage

- Traffic segmentation
- filtering
- Security

Disadvantage

- Slower speed
- Cost effective
- Require configuration

⑦ Switch

Switches in computer network are device that connect multiple devices within a network. These are small devices that can receive data from multiple input port and send it to specific output port.

- In switch two important things to know are its "poles" and "throws". A pole where electrical contact is made and throw is how many different contact each pole can connect to. The numbers of poles and throws tells us how the switch works.

Types
- → Mechanical switch
- → Electronic switch
- → Managed switch
- → Unmanaged switch
- → Layer 2 switch
- → Layer 3 switch

Advantages
- Control over network traffic
- Simple to install and operate

Disadvantage
- Limited security and performance

⑧ Gateway

- It is a device that is the center point for two or more networks to communicate with each other.
- Commonly used in businesses and large organization
- A gateway connect to multiple devices.
- Gateway is expensive.

⑨ NIC (Network Interface Card)

- NIC is a network adapter that is used to connect the computer to the network.
- It is installed in the computer to establish LAN. It has a unique id that is written on the chip and it has connector to connect the cable to it.

Types

→ Wired NICs

This types of NICs uses cables to connect to a network. It support high-speed data up to 1 Gbps

→ Wirless NICs

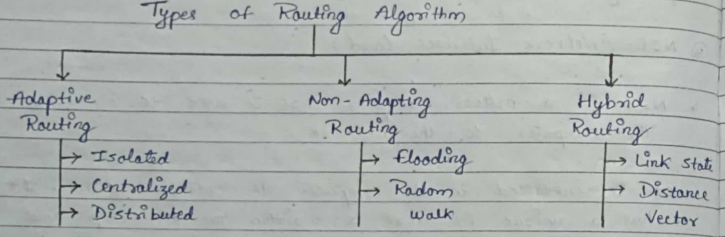
This types of NICs uses radio signal to connect to a network. Commonly used for wi-fi connection.

Routing Algorithm

Routing is the process of establishing the routes that data packets must follow to reach the destination.

In this process, a routing table is created which contain information regarding routes that data packets follow.

Classification of Routing Algorithm



① Adaptive Routing Algorithm

Adaptive algorithm is also known as dynamic routing, these are the algorithm that change their routing decision whenever network topology or traffic load change. The changes in routing decision are reflected in topology as well as traffic of network.

- These are classified as follows :-

→ Isolated

In this method each, node make its routing decision using the information it has without seeking information from other nodes

→ Centralized

In this method, a centralized node has entire information about the network and makes all the routing decision. The advantage of this is only one node is required to keep the information of the entire network

→ Distributed

In this method, the node receives information from its neighbours and then takes the decision about routing the packets It is also known as decentralized algorithm

② Non-Adaptive Algorithm

Non-adaptive algorithm is also known as static routing, these are the algorithm that do not change their routing decision once they have been selected.

- These are classified as follows :-

→ flooding

This adapts the technique in which every incoming packets is sent on every outgoing line except from which it arrived.

→ Random Walk

In this method, packets are sent host by host or node by node to one of its neighbours randomly. This is highly robust method that is usually implemented.

③ Hybrid Algorithm

As the name suggest, these algorithm are a combination of both adaptive and non-adaptive algorithm. In this approach, the network is divided into several region and each region uses different algorithm.

• These are classified as follows :-

→ Link - State

In this method, each router creates a detailed and complete map of the network which is shared with all other router.

→ Distance Vector

In this method, each router maintains a table that contains information about the distance and direction to every other node in the network.

* Routing Protocol

① Routing Information Protocol (RIP)

One of the earliest protocols developed is the inner gateway protocol or RIP. we can use it with LANs that are linked computer in a short range or WANs which are telecon network that cover a big range

② Interior gatway protocol (IGRP)

IGRP was developed by the multinational technology corporation cisco. function better on larger network. IGRP requires comparison across indicator such as load, reliability and network capacity.

③ Exterior Gateway Protocol (EGP)

Exterior gateway protocol are helpful for transferring data or information between several gateway host.

④ Enhanced Interior gateway routing protocol (EIGRP)

These routers can use the tables of other routers to obtain information and store it for later use. It stops routers for miscommunicating with each other.

⑤ Open shortest path first

OSPF is a inner gateway, link state and classless protocol that makes use of shortest path first (SPF) algorithm to guarantee effective data transfer.

Congestion control

It refers to the method used to prevent network overload and ensure smooth data flow. when too much data is sent through the network at once, it can cause delays and data loss.

Congestion control technique help manage the traffic, so all users can enjoy a stable and efficient network connection

Techniques

- Congestion control techniques can be broadly classified into two categories :-

① Open loop Congestion Control

Open loop congestion control are applied to prevent congestion before it happens. The congestion control is handled either by source or the destination

- Policies adopted by open loop congestion control -

→ Retransmission Policy

It is the policy in which retransmission of packets are taken care of. If the sender feel that a sent packet is lost or corrupted, the packet needs to be transmitted.

→ Window Policy

The type of window at the sender's side may also effect the congestion. several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side.

→ Discarding Policy

A good discarding policy adopted by the router is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages also maintain the quality of message

→ Acknowledgement Policy

The acknowledgement policy imposed by the receiver may also affect congestion.

→ Admission Policy

In admission policy a mechanism should be used to prevent congestion

② Closed loop Congestion Control

Closed loop congestion control technique are used to treat congestion after it happens.

- Several techniques are used by different protocols :-

→ Backpressure

Backpressure is a technique in which a congested node stops receiving packets from upstream nodes. Backpressure is node-to-node congestion control technique that propagates in the opposite direction of data flow.

→ Choke Packet technique

A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resource and the utilization at each of its output lines

→ Implicit Signaling

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network.

→ Explicit Signaling

In explicit signaling, if a node experience congestion it can explicitly send a packet to the source or destination to inform about congestion.

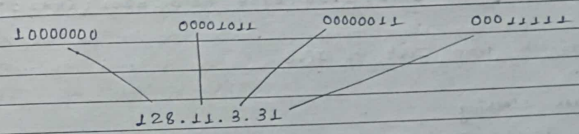
IPv4

- IPv4, or Internet Protocol version 4 is the original addressing system of the internet introduced in 1983. It uses 32 bit address scheme which theoritically allows for over 4 billion unique addresses

- IPv4 address are typically displayed in decimal format, divided into four octets separated by dots.
  Ex - 192.168.1.1 is a common IPv4 address you might find in a home network

→ IPv4 Address format

IPv4 address format is a 32-bit address that comprises binary digit separated by a dot (.).



IPv6

- IPv6 stands for Internet Protocol version 6. IPv6 is the new version of Internet Protocol which is way better than IPv4 in terms of complexity and efficiency.
- IPv6 was designed by Internet Engineering Task Force (IETF) in december 1998. IPV6 is written as a group of 8 hexadecimal number separated by colon (:). It can be written as 128 bits of 0s and 1s.

→ IPv6 Address format

- IPv6 address format is a 128-bit IP address, which is written in a group of 8 hexadecimal number separated by colon (:).

ABCD : EF01 : 2345 : 6789 : ABCD : B201 : 5482 : DC23

To switch from IPv4 to IPv6

→ Dual stacking

Devices can use both IPv4 and IPv6 at the same time

→ Tunneling

This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users.

Difference between IPv4 and IPv6

★ IPv4

- IPv4 has a 32-bit address length
- It can generate 4.29×10^9 address space
- Address representation of IPv4 is in decimal
- In IPv4 checksum field is available
- In IPv4 Encryption and authentication not provided
- IPv4 consist of 4 field separated by dot (.)
- IPv4's IP address are divided into five different class.

★ IPv6

- IPv6 has a 128-bit address length
- It can generate 3.4×10^{38} address space
- Address representation of IPv6 is in hexadecimal.
- In IPv6 checksum field is not available
- In IPv6 Encryption and authentication are provided
- IPv6 consist of 8 field separated by colons (:)
- IPv6 does not have any classes of IP address

Transport layer

- The transport layer or layer 4 of the OSI model, control network traffic between host and end system to guarantee full data flows.
- The transport layer is positioned between network layer and session layer.
- Two services are offered by the transport layer. Both Connectionless and connection-oriented services are available.

function of transport layer

→ To enable efficient network transmission, the transport layer split the total amount of data into smaller unit known as segment.

→ In situation when organised data transfer is required, the transport layer create a connection between source and the destination.

→ Most crucial roles of transport layer is flow regulation. In order to prevent data overload, it regulate data transfer rate.

→ Both error detection and correction are handled by the transport layer. Checksum are one of these technique for error detection.

Flow Control & Buffering

- The transport layer provide a flow control mechanism between the adjacent layer of TCP/IP model. TCP also prevent data loss due to a fast sender and slow receiver by imposing some flow control technique.
- Transport layer manages end to end flow. If the receiver is not able cope with the flow of data then data flow should be control from sender side.
- Buffer are allocated at sender and receiver side. If the network service is reliable, so every send TDPU sent will be delivered to receiver and will be buffered and process at receiver, so we need to keep buffer at sender.

  But if network services is unreliable and receiver may not able to handle every incoming TDPU then sender also keep a buffer.

TCP / UDP Protocol

- TCP (Transmission Control Protocol) is one of the main protocol of Internet protocol suite. It lies between the Application and network layer which are used in providing reliable delivery services.

Feature
→ TCP keeps track of the segment being transmitted.
→ TCP implement an error control mechanism for reliable data transfer.
→ TCP takes into account the level of congestion in network.

Application

① World Wide Web
When you browse website, TCP ensure reliable data transfer between your browser and web server.

② Email
TCP is used for sending and receiving emails.

③ File transfer protocol (FTP)
FTP relies on TCP to transfer larger files securely.

④ Streaming Media
Services like Netflix, Youtube, and spotify use TCP to stream videos and music.

- UDP (user datagram protocol) is part of Internet protocol suite referred to as UDP/IP suite. UDP helps to establish low latency and loss-tolerating connection establish over the network. UDP enables process to process communication.

Feature
→ UDP is used for some routing update protocol like (RIP).
→ It is suitable protocol for multicasting.
→ Used for simple request-response communication.

Application

① Real-Time Multimedia Streaming
UDP is ideal for streaming audio and video content.

② Online Gaming
Many online games rely on UDP for fast communication between players.

③ Multicasting
UDP supports packet switching, making it suitable for multicasting scenario.

④ Network monitering
Tools that monitor network performance often use UDP for lightweight

Difference between TCP and UDP

* TCP (Transmission Control Protocol)

- TCP is a connection-oriented protocol. Connection Orientation means that the communicating device should establish a connection before transmitting data and should close connection after transmitting the data.
- TCP gurantees the delivery of data to the destination.
- TCP provide extensive error-checking mechanism.
- TCP is slower than UDP
- TCP doesn't support Broadcasting.
- TCP connection is byte stream.
- TCP is used by HTTP, HTTPs, FTP, SMTP etc.

* UDP (User Datagram Protocol)

- UDP is a datagram-oriented protocol. This is because there is no overhead for opening a connection, mainting a connection or terminating a connection.
- The delivery of data to destination cannot be gurantee in UDP.
- UDP has only basic error-checking checksum.
- UDP is faster, simpler and more efficient.
- UDP support Broadcasting.
- UDP connection is a message stream.
- UDP is used by DNS, DHCP, RIP etc.