AMAS | Page No.
Date 21/08/20

Computer Networks

Network consists of 2 or more computers that are linked in order to share resources, exchange files, or allow electronic communications. The computers on a network may be linked through cables, radio waves, telephone lines, e.g. LAN, WAN, MAN.

Network Topologies

Arrangement of network in space, comprising nodes i.e. computers/devices and connecting lines via sender and receiver is known as network topology.

(i) Mesh Topology :

a. Every device connected to every other devices
b. For N devices, $N*(N-1)$ ports are reqd. to connect.
c. N_{C_2} or $N(N-1)/2$, dedicated lines reqd.

Advantages

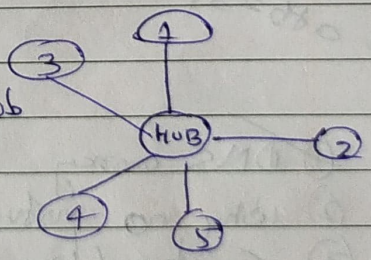
- Robust
- Reliable data due to dedicated channels
- Easy fault diagnosis
- Secured and privacy is maintained.

Disadvantages

- Difficult installation
- Cost of cable is high
- Cost of maintenance is high.

(ii) Star Topology

→ a. Devices are connected to a single hub
b. The hub can be active/passive (having repeaters)



Advantages

- Easy to set up, only N devices, N cables are needed to connect
- Total no.s of ports = N.

Disadvantages

- If hub fails, whole system will crash down.
- High installation cost
- Performance totally relies on single hub.

AMAS | Page No.
Date / /

(iii) Bus topology

a. Every computer and network device is connected to a single cable.

b. Transmits data from one end to another, single direction. No bidirectional data flow.

Advantages

→ For N devices, 1 backbone cable and N drop lines are reqd.

→ Low cost of cables.

Disadvantages.

→ If backbone fails, whole system crashes

→ If network traffic is heavy, collision may increase

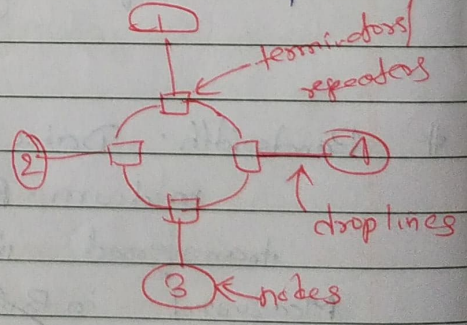
→ Low security

(iv) Ring Topology

a. Forms a ring connecting each devices with exactly 2 of it's neighbours.

b. Repeaters are used for a topology having large no of nodes, to prevent data loss.

c. Transmission is unidirection, but can be made bidirectional by having 2 connections b/w each Network Node, it is called Dual ring topology



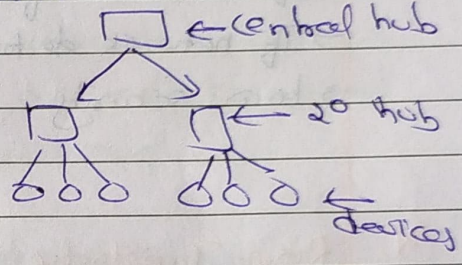
Advantages

1. One of the nodes "Monitor" station takes all responsibilities to perform all operations
2. To transmit, nodes need to hold token. After which it is passed to other nodes.
3. When no node is transmitting, token keeps circulating in ring.
4. Two types of token release techniques
   → Early token release: Release token just after transmitting the data.
   → Delay token release: Release token after receiving Ack from receiver.

Advantages
→ cheap to install and expand.
→ Possibility of collission is minm

Disadvantages
→ Fault detection is not easy
→ Addition & and deletion of nodes can destorb whole topology.
→ less secure

(v) Tree Topology
a. Variation of star topology, hierarchical flow of data
b. Data may flow in either direction
c. Multipoint connection.



Advantages
→ Allows more devices to be attached to a single central hub
→ Allows networks to get isolated and prioritize from different computers.

Disadvantages
→ If the central hub fails, entire system fails.
→ Cost of cabling is high

Bandwidth: Data carrying capacity of network/transmission medium. Refers to potential of data that is transferred in a specific period of time.
Measured in ~~Bits~~ Hz.

Throughput: Practical measure of the amount of data actually transmitted through a channel.
Measured in bps. Depends upon latency.

Performance of Network is the measure of quality of service of a network as perceived by the user. Following characteristics determines it

(1) Bandwidth : capacity

Bandwidth means "capacity" and "speed" means transfer rate.

Bandwidth in Hz : It refers to the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.

Bandwidth in BPS: No. of bits a channel, a link, or rather a network can transmit

(2) Throughput: ~~No of messages~~

(3) Latency (Delay): Total time taken for a complete message to arrive at the destination starting with the time the first bit of the message is sent out from the sender till the time when the last bit is delivered at the destination

Latency → High latency networks (leads to battle neck)
→ Low latency networks

Measured in ms (also known as ping rate)

Latency = Propogation time + Queuing time + Transmission time + Processing Delay

(4) Bandwidth - Delay product

(5) Jitter: Variation in packet delay

Different packets of data faces different delays and receives application is time sensitive.

Nodes: Any network device that can recognize, process, and transmit information to any other network node. It is a connection point that can recieve, send, create or store data.

AMAS | Page No.
Date / /

Links : connecting wires/wireless medium b/w two nodes in a network that makes data transmission possible.

Routers : Analyses data inside the packet to determine the best way for the information to reach destination. It forwards data packets until it reaches their destination node. (Works between networks)

Switches : connects devices and manages node-to-node communication within a network; to ensure data packets reach their ultimate destination
Circuit Switching, Packet Switching, Message Switching.

Ports : Identifies a specific connection between network devices. Each of them is identified by a no.
[Eg IP address is address of a hotel, room numbers are the port nos.]
Computers uses port no. to determine which application, service, or process should receive specific messages

Layers of OSI model : (Open System Interconnections)
There are 7 layers in it, performing specific functionalities. They work collaboratively to transmit the data from one person to another

(1) Application layer
(2) Presentation layer → Software layers
(3) Session layer
(4) Transport layer → Heart of OSI.
(5) Network layer
(6) Data link layer → Hardware layers
(7) Physical layer

Sender ↓
↑ Receiver

AMAS | Page No.
Date / /

Date : 23/08/21

1. Physical layer

Functions

1. Bit synchronization using a clock
2. Bit rate control : Defines transmission rate
3. Specifies physical topology.
4. Transmission mode.

Hub, Repeaters, Modem are physical layer devices

2. Data link layer

a. Responsible for node to node delivery
b. After receiving package from Network layer, it divides it into frames depending upon frame size (in NIC).
c. Encapsulates Sender's and receiver's MAC address in the header.

Functions

1. Framing
2. Physical addressing
3. Error control
4. Flow control : Data rate must be constant in both sides
5. Decides access control.

Switch & Bridges are used here

3. ~~Transport layer~~

4. Network layer

a. Transmission of data from 1 host to other in different networks.

Functions

1. Routing : Using network layer protocols (IP)
2. Logical Addressing : IP addresses distinguishes each device uniquely and universally.

Routers used here.

AMAS | Page No.
Date

4. Transport Layer

Data referred to as Segments

Responsible for end-to-end delivery of the message.

At sender's side:

Recieves data from upper layers → Performs Segmentation → Implements flow & error control → Adds src and dest PORT NO in the header → forwards data to Network layer.

At receiver's side:

Reads PORT NO from header → Forwards data to the respective application → Also performs sequencing and reassembling of the segmented data.

Functions: (1) Segmentation and reassembly
(2) Service Point Addressing

Services provided

1. Connection oriented
   a. Connection establishment b. Transmission
   c. Termination/disconnection

   Recieving packet sends ack back to sender, hence reliable.

2. Connectionless

   Reciever doesn't ack but is a faster communication Service.

Operated by Operating System. Part of the OS and communicates with the application through system calls.

Heart of OSI model.

5. Session layer

Functions:

1. Session establishment, maintenance and termination
2. Synchronization
3. Dialog control : Allows two systems to communicate in half/full duplex

6. Presentation layer (Translation layer)

1. Translation (e.g ASCII to EBCDIC)
2. Encryption/decryption is done here.
3. Data Compression

7. Application layer

a. Produces the data which is to transferred over the network.

b. User interface.

Functions:

1. Network virtual terminal
2. FTAM → File transfer access and management.
3. Mail services
4. Directory services

OSI model has not been implemented, it is a reference model because of it's later invention.

Currently we use TCP/IP model.

TCP/IP (DoD)

Concise version of OSI model

Layers

1. Application layer/process (Upper layers)
2. Transport layer (Host-to-host) (transport)
3. Internet layer (Network layer)
4. Network Access layer (DLL + Physical)
   /Link layer

AMAS | Page No.
Date / /

Differences

OSI	TCP/IP
1. Uses both session & presentation layer in different layers.	1. In ~~physical~~ application layer itself.
2. OSI developed model	2. Developed protocols more than models.
3. Transport layer provides assurance of packet delivery	3. Doesn't provide.
4. Connectionless and connection oriented both	4. Only connection less service
5. Protocols are easy to replace with the change in technology	6. Protocols are not easily replaceable.

1. Network Access layers
→ Combination of DLL and Physical layer in OSI model
→ Responsible for physical addressing, and protocols how allows for physical transmission of data.

2. Internet Layer.
Protocols
→ IP: Responsible for delivering packets from source host to destination host by looking at IP addresses in headers.
→ ICMP (Internet Control Message protocol) : Responsible for providing hosts with network problems.
→ ARP (Address Resolution protocol) → Finds physical address using logical addr.

AMAS | Page No.
Date / /

3. Host-to-Host layer (Transport)
→ shields the upper layer application from the complexities of data.

Protocols
TCP → Reliable and error free communications
→ Has ack feature, controls flow of data
→ Does segmentation and reassembly
→ Has overhead due to lots of features. High cost

UDP: It is connection less transport and hence faster. low cost transportation.

4. Application/Process layer
→ Responsible for node to node communications
→ Controls user-interface specifications
Protocols: HTTP/S, FTP, SMTP, NTP, DNS, etc.

1. HTTP/HTTPS: Used by WWW to manage communications b/w web browsers and servers
HTTPS is HTTP-Secure: Combination of HTTP and (Secure Socket Layer). Efficient in case browsers needs to fill out forms, sign in, carry out bank transactions.

2. SSH: (Secure Shell): It can maintain encrypted connection. Sets up a secure connection over TCP/IP connection

3. NTP (Network Time protocol): Used to synchronize our clocks with standard time

AMAS | Page No.
Date / /

Repeaters: Used in physical layer to amplify the signal if it becomes too weak while travelling large distances. 2 port devices

Hub: It is basically a multiport repeater
Not intelligent, cannot filter data, eg. hub in star topology.

Bridge: Operates in DLL
→ A repeater with data filtering intelligence based on MAC address of src and destination.
→ 2 port device.

Switch: Multiport bridge. Can perform error checking DLL device.

Routers: Network layer device,
Routes data packets based on IP addresses.
Connects LANs and WANs together

Gateway: Passage to connect two networks together that may work upon different network models.
→ Also known as protocol converters
→ Can operate at any network layer
→ More complex than switches & routers.

NIC: Network adapter used to connect computer to the network.
Has unique id written on it's chip.
It is a layer 2 device (both in physical & DLL)

AMAS | Page No.
Date / /

Date: 23/08/21

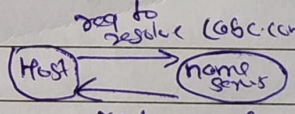
PING (Packet internet Groper)
→ Used to check network connectivity between host and server using IP address of the server
→ Sends a data packet with the msg "PING" to the server and gets response in some time (latency) which is recorded to analyze the network.
→ Uses ICMP to send ICMP echo to server which sends back ICMP reply message to the host.

DNS (Domain Name System) : A distributed database which is used to translate domain name to IP address.
→ Implemented in a hierarchy of name servers, an application layer protocol.

Types of Domains
1. Generic : .com, .edu, .org
2. Country domain : .us, .in, .uk

DNS Record : consists of domain name, IP address, details of validity.

Name Server : Implementation of resolution mechanism



Hierarchy of name Servers
(1) Root name Servers (2) Top level name Servers
(3) Authoritarian name Servers.

In order to reach cse.dtu.in, we have to ask root DNS server, then it will point out to the top level domain (.in) server and then to authoritative domain name server (dtu.in), which will actually contain the IP address of (cse.dtu.in). So, authoritative domain server will return the associated IP address.

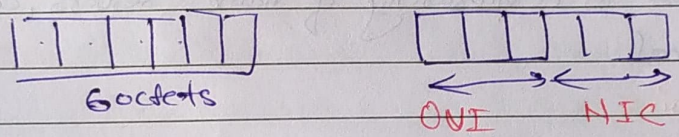
.edu

AMAS | Page No.
Date / /

DNS Forwarder : In DNS, forwarder is a DNS server that is used to forward DNS queries for external DNS names to DNS servers outside the network. It does it to DNS queries that it cannot resolve locally, meaning DNS queries that it has no personal knowledge of.

MAC address (Media Access Control address)

→ 48 bit hardware no. embedded into the NIC during time of manufacturing
→ used by MAC sublayer of DLL.
→ Address is world wide unique



OUI : organisationally unique identifier
NIC : Network interface Controllers specific

Format of MAC address:
48 bits = (48/4) = 12 digit hexadecimal no.
1st 6 digit represents manufacturer (OUI)
↳ e.g. Cisco, Google, Inc, HP, etc.

The rightmost 6 digits represent NIC, which is assigned by manufacturer.

Three formats:
(1) Hyphen-Hexadecimal notation (CC-DD-01-CD-EF-01)
(2) Colon-Hexadecimal (: : : : : :)
(3) Period Separated hexadecimal (CCD.D01.CDE.F01)

AMAS | Page No.
Date / /

IP address : An unique address that identifies all devices across the network.

→ Helps distinguishing btw different routers, computers, and websites.

IPv4 structure

A set of four numbers '.' separated

each Ranges from 0-255, so, IP addr ranges from 0.0.0.0 to 255.255.255.255

[x1.x2.x3.x4]

1. First 3 denotes Network Id : Specifies the specific network where device is located.

Suppose When the device has 192.168.1.32 as the IP addr. 192.168.1 refers to network. It is mandatory to fill the last digit with non-zero value, so the device's network Id is 192.168.1.0.

2. Last one denotes host Id : It is not taken from the network Id, denotes a specific device.

So, for above example 32 will be unique host Id on the 192.168.1.0 network.

Types : Public, Private, Fixed, Dynamic

Public : encrypted by various servers / devices

→ It is the one accessed over the internet by various mailservers, web server to communicate.

→ They will order this public IP address.

Private IP addr : Our router needs a way to identify these no.s of devices that has access to internet. So, router generates unique private IP addresses for each device.

DNS

DNS

fo

n

pe

MAC

→ 4

→

→

O

N

For

48

AMAS | Page No.
Date / /

Difference b/w IPV4 and IPV6

IPV6 is the new version(6), which is better than IPV4 in terms of complexity and efficiency.

IPV4	IPV6
1. Has 32-bit length = ~~4 octal nos~~ = 4×8 = 32 bits.	1. Has 128 bit length 8 hexadecimal digits of 16 size (bits) = 8×16 = 128.
2. Address representation in decimal	2. In hexadecimal format
3 Encryption and auth not provided	3. Provided
4. Header of 20-60 bytes.	4. Header of 40 bytes

16×8 = 128

128 ⇒ DDDD:BBBB:CCCC:EEEE:AAAA:- - -

4bits×4 = 16

saved with a probability of (1/2)

Date : 21/08/21

What happens when we hit on URL in the browser and press ENTER

1. Suppose we typed maps.google.com in our browser and hit enter.

2. Browser checks for corresponding IP address of the website in the four caches one by one, to find the DNS record.

[DNS (Domain name System) is a database that maintains URL vs IP addresses of each website on internet.

Finding the DNS record in 4 caches

1. → It checks in browser cache of client. which is their for a fixed duration, if prev. visited

2. → If not found, it checks in the OS cache (through a system call "gethostname")

3. → Then it checks in the router cache

4. Fourth, it checks in the ISP cache

Caches are essential for network traffic regulation and data transfer rate improvements.

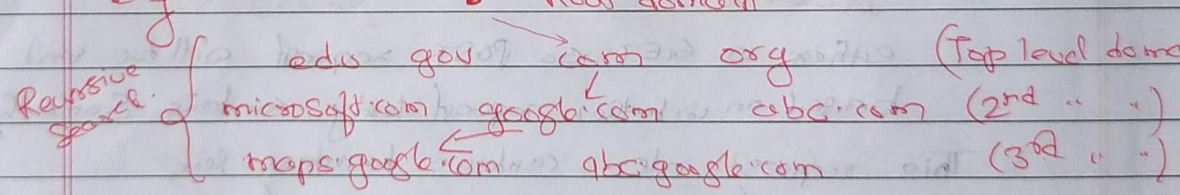
3. If not found in ISP's cache, DNS server initiates a query to find the IP address

⇒ DNS server does recursive search until it finds the IP address.

So, ISP's DNS server is called DNS recursor, who is responsible to find the proper IP address.

Other DNS servers which takes participation in this recursive search are called name servers.

e.g



For maps.google.com, DNS recursor will contact root name Server, which will redirect it to .com domain name server. .com NS will redirect it to google.com which in turn searches for the correct IP addr. corresponding to the ~~domain~~ URL and return it to our DNS recursor, which will be send back to our browser.

The request travel to the destination in the fastest possible way using routing tables.

Now that correct IP addr is found

4. Browser initiates a TCP connection with the server
   Internet protocols (like TCP) are used to build the connection.
   Connections are established using a process called TCP/IP three-way handshaking.
   1. Client machine send SYN packet to the server asking if it is open for new connections.
   2. If open server responds with a SYN/ACK packet to the client.
   3. Client will finally send an Ack after recieving SYN/Ack from the Server.

   TCP connection is established for data transmission.

5. Browser send an HTTP request to the destined webserver.
   either a GET or POST request will be sent based on whether request body contains something.
   This request also contains headers like accept, user-agent, connection (to be kept alive or not) and some cookies related to that domain.

6. Server receives Client's request and sends back a response.
   → Webservers (like Apache) receives client requests and passes it to a request handler to generate a response. Request handler is a program written in backend languages. It may also update data on Server. And assembles a response in some particular format for JSON/HTML/XML.

7. Server sends out an HTTP request

Response contains the web page, status code, compression type, cookies to set, privacy info etc.

Status codes (5 types)

1. 1xx → Denotes an informational message only
2. 2xx → Any kind of success
3. 3xx → Redirection to another URL
4. 4xx → Error on client's side
5. 5xx → Error on server side

8. Browser displays the HTML content in the client's screen

It is done in phases.

i. First the bare bone HTML skeleton
ii. Then it checks for HTML tags and sends out GET requests CSS/images etc.
iii. Static files are cached by browsers, so that next time it takes less time to load.

Also, we can see maps.google.com in our screen.