Unit-1 : Introduction to Computer Networ

- Ankit Pangeni DATE

Computer Network.

A computer network is a set (group) of interconnected computers and other computing hardware devices which are linked together through communication channels

The main purpose of computer network is to exchang resources and services among wide range of users.

Uses of computer Network.

* Business application
  - → Resource sharing ex: printer sharin
  - → Server-Client model
  - → Communication medium & E-comme rce
* Home applications
  - → Access to remote information
  - → Person-to-person communicatio
  - → Interactive entertainment
  - → Electronic commerce: B2C, B2B, P2P
* Used by mobile users for various communication as well as entertainment purposes like email, video meetings, Netflix, youtube, etc.

Benefits / Advantage

i) It offers convenient resource sharing
ii) It is highly flexible and it is inexpensive
iii) It increases the storage capacity

DATE

iv) It makes file sharing easier
v) It enhances communication.

Disadvantages

i) Comes with the risk of security issues
ii) Encourages people to become dependant on computers
iii) High chance of computer viruses and malware.
iv) If the main server of the network is down, the entire system becomes useless.
v) Requires an efficient handler.

Network Topologies

Network topologies refer to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with each other.

It describes how the data is transferred between these nodes. The nodes may be computers, hardware devices, and so on. It is divided into five categories.

1) Bus Topology
2) Star Topology
3) Ring Topology
4) Tree Topology
5) Mesh Topology
6) Hybrid Topology

DATE

* Bus topology

Here, all devices share single communication line or cable. All the devices/nodes are connected sequentially to the same transmission line. This is the simplest, low-cost topology where a failure of a device doesnot affect the other devices, but the failure of shared communication line can make all other devices stop functioning

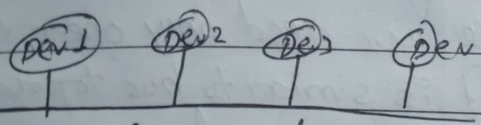
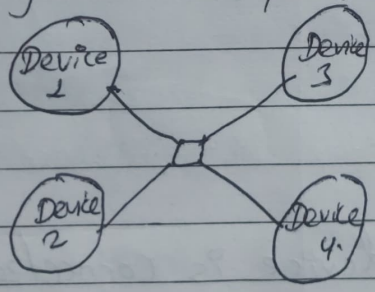


fig: Bus topology.

* Star Topology.

All devices in a star topology are connected to a central device, known as a hub device, using a point-to-point connection. Failure of an individual node or cable does not necessarily create downtime in the network but the failure of central device can. It is the most popular and widely used topology.



Advantages:

i) Fast performance.
ii) Hub can be upgraded easily
iii) Easy to setup, modify and troubleshoot

Disadvantages:

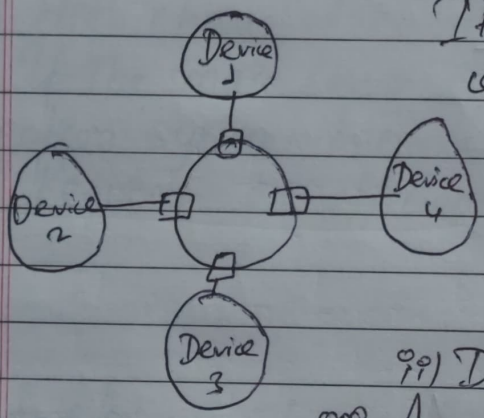
i) Cost of installation is high
ii) If hub fails, whole network is stopped.
iii) Performance depends upon hub its capacity.

DATE

* Ring Topology.

In this, each nodes/devices connects to exactly two other devices, creating a circular ring like network structure. The data travels through all intermediate nodes in a specific direction. When two non adjacent devices need to communicate, the data travels through all intermediate devices. To connect a new node, we need only one extra cable.

It is similar to bus topology, but with a closed loop.



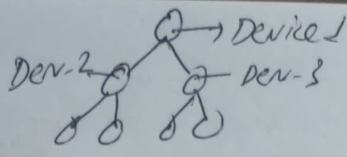
Advantages

i) Cheap to install or expand
ii) Data transfer can be done at high speed
iii) As data flows in one direction, it reduces chance of packet collisions

Disadvantages: i) Troubleshooting is difficult
ii) Failure of one device disturbs whole network
iii) If more number of devices are on network, the data transfer rate may be slow.

* Tree Topology

A root node/device is connected to two or more sub-level nodes, which themselves are connected to sublevel nodes. Physically, this is similar to star and bus topology; the network



DATE

transmission line may have a bus topology, while lowlevel nodes connect using star topology.

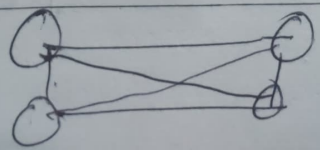
Advantages	Disadvantages
i) It is an extension of bus and star topologies	i) If root node goes down, the entire network suffers.
ii) Expansion of nodes is possible and easy	ii) Heavily cabled
iii) Easily managed and maintained.	iii) It is costly and maintenance is difficult in case of large no. of nodes.

* Mesh Topology.

In this type, ~~the~~ a node/device is connected to one or multiple devices. It has devices in point-to-point connection with every other devices or may be to few devices only. There are two forms.

i) Full Mesh Topology : ~~Every~~ Each device has a point-to-point connection to every other device in the network. Thus, for every new devices, $n(n-1)/2$ connections are required. It provides most reliable network structure among all other topologies.

ii) Partiaw Mesh : Not all hosts/devices/nodes have point-to-point connections to every other host. It exists where we need to provide reliability to some hosts out of all.



classmate

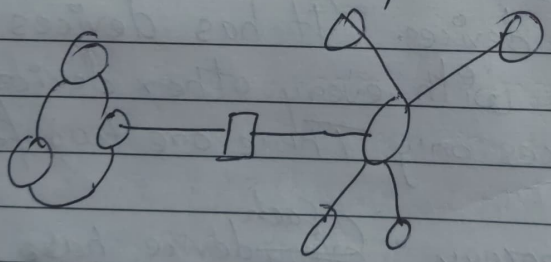
PAGE

DATE

Advantages	Disadvantages
i) Each connection can carry its own data load.	i) Installation and configuration is difficult
ii) Fault is diagonised easily	ii) Bulk wiring is required
iii) Provides security and privacy.	iii) Cable costing is more

* Hybrid topology

It is a network structure whose design contains more than one topology. It inherits merits and demerits of all incorporating topologies



Advantages	Disadvantages
i) Reliable & troubleshooting is easy.	i) Complex in design
ii) Effective & Scalable as size can be increased easily	ii) More costly
iii) Flexible.	iii) Bulk wiring is required.

PAGE

DATE

Network Types

i) Personal Area Network (PAN)

It is the smallest and most basic type of network. A PAN is made up of a wireless modem, one or two phones, printers, tablets, etc. and revolves around one person in one building. These type of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.
Example: Wirelessly accessing bluetooth devices, headphones, printers, mobiles from a PC.

~~ii) Local Area Network (LAN)~~ Advantages:

a) No extra space required
ii) Connect many devices at a time
iii) Cost effective, easy to use, reliable, portable & secure

Disadvantages:

a) Less distance range & slow data transfer
b) Interfere with radio signals.
c) Health problem (uses microwave signals)

ii) Local Area Network (LAN)

LAN is a computer network which spans over a small geographical area such as home, building, office. It can be a simple network where computers are placed relatively close using different topologies like Ring, Buss, Tree to share files &

DATE

network among each other. LAN are also widely used to share resources like printers, shared hard-drive etc. LAN are mostly private networks and relatively faster than typical WAN.

Advantages	Disadvantages
i) Resource Sharing	i) High setup cost
ii) Easy & cheap communication	ii) Covers limited area only
iii) Centralized data and more secure	iii) Privacy violations.
iv) Internet Sharing.	iv) LAN Maintenance job.

iii) Campus Area Network (CAN)

A CAN is a computer network made up of an interconnection of local area networks within a limited geographical area. These type of networks are typically seen in universities, large K-12 schools, districts or small busines. They can be spread across several buildings that are fairly close to each other so users can share resources.

iv) Metropolitan Area Network (MAN)

It is made up of interconnection of LANs in a town or a geographical area or region as large as a ~~city~~ or a small neighbourhood. It is larger than CAN and within a metropolitan area

DATE

Smaller than WAN. They are used to establish connection between buildings of a town, or Universities, distribution of wireless routers across a city, cable TV, fiber connections, and so on. It also connects traffic lights & parking meters wirelessly as a metropolitan area network. Generally covers towns and cities up to 50 km in range.

Advantages	Disadvantages
i) Extremely efficient and provides faster communication due to use of fiber optic cables	i) More cables required.
ii) Provides good backbone for large networks & provides greater access to WANs	ii) Difficult to make the system secure from hackers and spying.

v) Wide Area Network (WAN).

It spans over a large geographical area such as a state, region or a country. They are typically used to connect two or more LANs or MANs which are located very ~~fast~~ far from each other. Communication medium used by WAN are PSTN or satellite links. Examples of WAN are Internet, ISPs, mobile broadbands, telecom companies etc.

Advantages	Disadvantages
i) Covers a large geog. area.	i) Needs a good firewall
ii) Very fast.	ii) Very expensive & complicated
iii) Easily share softwares & large files	iii) Maintenance is difficult.

CLASSMATE

DATE

Networking Types

i) Peer-to-Peer Network (P2P)

A P2P network is a group of computers each of which acts as a node for sharing files and resources within a group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it. Example: Torrent.

Advantages:-

a) As a peer joins the network, it adds resources to the existing network, adding more members to the system, so it increases the capacity or resources of the system itself. As a result, throughput increases

b) Very robust as there is no single point of failure. If one peer is lost, it doesn't affect the network.

Disadvantages:

a) P2P networks have high bandwidth consumption rates.

b) Lack of security as no checking of authentication happens.

ii) Multi-point Architectures:

It means the channel is shared among multiple devices or nodes. In this architecture,

DATE

There is one transmitter and many receivers. Link is provided all the times for sharing the connection among nodes. It does not provide security and privacy because communication channel is shared.

(iii) Client-server Network

It is a networking model in which the server host delivers and manages most of the resources and services to be consumed by the client. This type of architecture has one or more client computers connected to a central server over a internet connection.

It is a producer-consumer networking model where server acts as a producer and consumer is client. A server computer can manage several clients simultaneously, whereas one client can be connected to several services at a time, each providing a different set of services.

Advantages	Disadvantages
i) Centralized backup is possible.	i) Requires specialized servers with large memory and secondary storage.
ii) Security is better.	ii) Cost is high
iii) Use of dedicated server improves performance & overall speed of whole system	iii) Requires dedicated network administrator

classmate

PAGE

DATE

Difference between Peer-to-peer & Client-server

Peer-to-peer	Client server
i) Clients and server are not distinguished; each node acts as both.	i) Clients and server are specified.
ii) Each node can request as well as provide services	ii) Client requests for service and server responds with servi
iii) It focuses on connectivity	iii) It focuses on sharing of information.
iv) Each peer has its own data.	iv) The data is stored in a centralized server.
v) They are less expensive to implement	v) More expensive to implement
vi) Peer-to-peer suffers if the number of peer increases in the system.	vi) Client-server is more stable and scalable.

classmate

PAGE

DATE

Overview of Protocols and Standards

* Network Protocols

In information technology, a protocol is a special set of rules that determine how data is transmitted between different devices in same network. Essentially, it allows connected devices to communicate with each other, regardless of any difference in their internal processes, structure or design.

Some examples of network protocols are Hyper-text transfer protocol (HTTP), File Transfer Protocol (FTP), Transmission Control Protocol / Internet Protocol (TCP/IP). ~~etc~~, Secure sockets layer (SSL), etc.

→ In simple language, protocol is a set of rules that governs the communication.

Network protocols are also similar to natural human languages in that they have three basic components: Syntax, Semantics and timing.

→ Syntax: Refers to the structure and format of the information data. In other words, the order in which pieces of information will be packaged by the sender & opened up by the receiver.

→ Semantics: Determine what individual pieces of information within a network protocol mean. How is a particular pattern to be interpreted? and what action is to be taken based on that interpretation?

DATE

→ Timing: It governs/refers to two characteristics when data should be sent and how fast it should be sent. Ex: if sender produces data at 100 Mbps but receiver can process data only at 1 Mbps, transmission will overload and data will be lost.

* Standards.

Network Standards define the rules for data communications that are needed for interoperability of networking technologies and processes.

They are the guidelines that explain to all IT stakeholders - from device manufacturers to software programmers and network administrators - how a particular protocol should operate. As long as everyone follows a common standard, the protocol guarantees that two devices can communicate, even if they were built by different companies or running in different OS. Ex: ~~International Standards Organization~~ (ISO), HTTP, etc

Data communication standards falls in two (types) categories:

→ De facto (by fact): These are the standards that are followed without any ~~guidelines~~ formal plan or approval by any organization. i.e. based on facts only. Ex: HTTP

classmate

PAGE

DATE

→ De jure (by law): These standards are the ones which have been adopted through regulation (legislation) by any officially recognized standards organization. Most of the communication (network) standards that are used today are de jure standards.

* Standards Organizations:-

→ International Standards Organization (ISO)
Created in 1947, the ISO is an entirely voluntary organization dedicated to worldwide agreement on international standards. Its main concern is in the field of technology, which have resulted in creation of Open Systems Interconnection (OSI) model.

→ International Telecommunication Union (ITU)
Created in early 1970s, a no. of countries were defining national standards for telecommunications. Later, it was made international on 1993 & since then it is devoted to research & establishment of standards for telecommunication.

→ American National Standards Institute (ANSI)
Despite its name, it is a completely private, nonprofit corporation not affiliated with US federal government. It serves as national coordinating institution for voluntary standardization in the United States.

→ Institute of Electronics & Electrical Engineers (IEEE)
→ Electronic Industries Association (EIA)
→ World wide web consumption (W3C)

CLASSMATE PAGE

DATE

Network Models.

A network model refers to a design or architecture to accomplish communication between different systems. They are also referred to as network stacks or protocol suites: Eg: OSI, TCP/IP, Net-BIOS, etc.

A network model contains layers. Each layer represents specific functionality. A layer is normally a collection of protocols.

IMP.

OSI Reference Model.

OSI stands for Open Systems Interconnection. It has been developed by ISO - 'International Standard Organization' in the year 1984. It is a 7 layer architecture with each layer having specific functionality. All these 7 layers work collaboratively to transmit data from one system to another across the globe.

It is not a protocol, but a model for understanding and designing a network architecture that is most efficient and robust. Using OSI model, we can design a network system that allows communication between all types of computer systems.

DATE

Software layers

7.	Application Layer	o Provides a user interface. ie. Human-computer interaction
6.	Presentation Layer	o Presents data and handles the encryption of data.
5.	Session Layer	o Maintains connections and is responsible for controlling ports & sessions
4	Transport Layer	o Transmits data using transmission protocols including TCP and UDP.
3	Network Layer	o Determines which physical path the data will take.
2	Data Link Layer	o Defines the format of data on network (bit, byte, frame) o Provides access to media using MAC address
1	Physical Layer	o Moves bits between physical devices. o Specifies voltage, wire speed.

Heart of OSI

Hardware layers

* Physical Layer

It is the lowest layer of OSI reference model. It is responsible for the actual physical connection between the devices. It is responsible for transmitting individual bits from one device to another. When receiving data, this layer will get the signal received & convert it into 0's & 1's & send to data link layer which will put the frame back together.

Ex: Hub, repeater, modem, cables.

MAC → Media Access Control

DATE

Responsibilities / functions:

i) Bit synchronization
⇒ sender & receiver must be synchronized at bit level. Their clocks must be synchronized.

ii) Bit rate control
⇒ defines transimission rate ie. no of bits sent per sec

iii) Bit representation
⇒ consists of bits (1's & 0's) which is encoded into electrical signals before transmission.

iv) Physical topology
⇒ Specifies which network topology is used to arrange nodes/devices

v) Transimission mode.
⇒ defines way in which data flows: simplex, half-duplex and full-duplex.

∀ Data Link Layer:

It is responsible for node to node delivery of message. It makes sure that the data transfer is error free. The main function of this layer is to define the format of data on the network. (i.e. bits, bytes, frames). It provides access to media using MAC. address. It makes physical layer appear error free to the upper layer (network layer)

DATE

Responsibilities/functions

i) Framing ⇒ divides the bits received into data units called frames.

ii) Physical addressing ⇒ After creating frames. DLL adds physical address (MAC) of sender & receiver in the header of each frame.

iii) Error control ⇒ detects & retransmits damaged or lost frames

iv) Flow control ⇒ data transmission rate must be equal on both sides, else data will be lost.

v) Access control ⇒ If two or more devices are connected to the same link, it determines which one has control over the link. at any given time.

* Network Layer.

This layer determines which physical path the data will take. It is responsible for the delivery of packets from source to destination across multiple networks and links

Responsibilities/functions

i) Logical Addressing
⇒ provides IP address to deliver packets from source to destination across the networks

ii) Routing:
⇒ determines which route is suitable from source to destination. Shortest path (route) is considered.

PAGE

classmate

DATE

* Transport Layer.

This layer is the heart of OSI reference model. It is responsible for overall transmission of data using transmission protocols like TCP and UDP. It make sure that the whole messages arrive in order, overseeing both error & flow control at source-destination level. The data in the transport layer is called as segments.

Responsibilities / function

i) Service-point addressing => delivers the packet from a specific process at a host to correct destination

ii) Segmentation & Re-assembly => A message is divided into segments before transmission & it is again assembled at the receiving end.

iii) Connection control => it can either be connection oriented or connectionless transport.

iv) Flow control & Error control => flow control is performed at end to end whereas error control is performed at process to process rather than across a single link.

* Session Layer.

This layer maintains the connections and is responsible for controlling ports & sessions. It establishes, maintains & synchronizes the interaction among communicating systems.

classmate

PAGE

DATE

Responsibilities / Functions.

i) Dialog control → This session allows two systems to communicate either in half or full duplex.

ii) Synchronization → allows a process to add checkpoints or synchronization points to a stream of data

* Presentation Layer

This layer presents the data and handles the encryption of the data. It is concerned with the syntax and semantics of the information exchanged between two systems.

Responsibilities / functions:

i) Translation → Ex: ASCII to EBCDIC.

ii) Encryption / Decryption → Data encryption translates the data to another form. The encrypted data is called cipher text & decrypted is plain text. A key value is used for enc & dec.

iii) Compression → Reduces the no. of bits that need to be transmitted on the network.

* Application Layer.

This layer provides the user interface ie. Human-computer interaction & supports for services such as emails, remote file access & transfer, share DBMS, etc.
Ex: Applications, browsers, Skype, Messenger, etc.

Functions / services provided:

i) Network virtual terminal ⇒ allows user to log on to a remote host

ii) FTAM (File transfer & Management) ⇒ access files in a remote host

iii) Mail services ⇒ basis for email forwarding & storage

iv) Directory services ⇒ provides distributed data sources.

DATE

TCP/IP Model

The OSI model was designed to describe functions of communication systems. But TCP/IP was developed and designed By Department of Defence (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control protocol/Internet protocol. It contains following four layers:-

1) Application Layer
2) Transport layer
3) Internet Layer
4) Network Access Layer

OSI model specifies which functions belong to each of its layers whereas the layers of TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the need of the system.

* Network Access layer

It is the lowest layer of TCP/IP protocol hierarchy. It defines how to use the network to transmit an IP diagram.
It does not define any specific protocol but supports all the standard & proprietary protocols.

DATE

* Internet Layer

It supports the internet working protocol (IP) and also four other supporting protocols: ARP, RARP, ICMP and IGMP. It corresponds to the functions of Networ layer of OSI Model.

a) Internetworking Protocol (IP): It is unreliable & connectionless protocol & transmission mechanism used by TCP/IP protocols
b) Address Resowtion Protocol (ARP): Used to associate a logical address with a physical address
c) Reverse Address Resowtion Protocol (RARP): Allows host to discover its IP address when it knows only its physical address.
d) Internet Control Message Protocol (ICMP): It is a mechanism used by hosts & gateways to send query & error reporting notifications of datagram problems back to the sender
e) Internet Group Message Protocol (IGMP): Used to facilitate the simultaneous transmission of a message to a group of receipents

* Transport Layer

- The traditional UDP and TCP are transport level protocols that are responsible for delivery of a message from a process to another process. The protocols in this layer

a) User Datagram Protocol (UDP) : Simple process to process protocol that add's only port addresses, checksum error control & length information to the data from the upper layer.

PAGE

classmate

b) Transmission Control Protocol (TCP): It provides full transport layer services to applications.

c) Stream Control Transmission Protocol (SCTP): Combines best features of UDP & TCP & provides support for newer applications such as voice over internet

* Application Layer:

This layer is equivalent to the combined session, presentation and application layers of the OSI model. Lists of protocols defined in this layers are:

- Hypertext transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Routing Information Protocol (RIP)
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Telnet

DATE

TCP/IP Comparison with OSI

OSI	TCP/IP
i) Stands for Open systems Interconnection & is a reference model.	i) Stands for Transmission Control protocol & is an implementation of OSI model.
ii) It has 7 layers namely:-	ii) It has 4 layers namely:
iii) It has separate session and presentation layer.	iii) It combines the session & presentation layer in the application layer.
iv) Supports connectionless and connection oriented communication in the network layer.	iv) Supports only connectionless communication in the network layer.
v) It has vertical approach	v) It has horizontal approad.
vi) It has strict boundaries for the protocols.	vi) Protocols are not strictly defined.
vii) OSI uses the network layer to define routing standards & protocols.	vii) TCP IP uses only the internet layer.
viii) OSI is less reliable.	viii) TCP IP is more reliable.

PAGE

classmate

14P

DATE

* Connection less and Connection Oriented Network Service

Both connection-less and connection oriented service are used for the connection establishment between two or more than two devices. Those type of services are offered by the network layer.

Connection less Service :

→ Connection less system is related to postal system
→ It does not include any connection establishment and termination.
→ This service does not give the guarantee of reliability.
→ Here, packets do not follow the same path to reach the destination so they are not received in order they sent.
→ It transfers data without any authentication.
→ No handshaking is used as there is no any virtual connection between sender & the receiver.
→ User Datagram protocol (UDP), Internet Protocol (IP) and Internet Protocol (IP) are some examples.
→ Requires low bandwidth to transfer the data packets.

Connection Oriented Service.

→ This Service is based on the telephone system.
→ It creates end to end connection between the senders to the receiver before transmitting data packets over network and there is connection termination after data is transferred.
→ The data packets follow the same path to reach the dest. So...
→ Handshaking method is used to establish the connection.
→ Requires more bandwidth to transfer data packet so it is preferred by long & steady communication.
→ TCP is an example of connection oriented. Service

DATE
PAGE

DATE

* Basic Concepts of Internet & ISPs

Internet

→ Internet is a vast network that connects computers all over the world. Through the internet, people can share information and communicate from anywhere with an internet connection

→ Internet is most often used for three main purposes: communication, buying & selling (e-commerce) & searching of information

→ It is a self-publishing medium which means no one is in charge of the content found on it. Anyone can publish anything on the internet, whether the information is true or not.

ISPs

→ Internet Service provider (ISP) is the company that provides internet connections and services to individuals and organizations. & also email, website services

→ They use fiber optics, satellite, copper wire and other forms to provide the internet access to its customers

→ To connect to an ISP, we need a modem and an active account. The ISP verifies our account and assigns an IP address to our modem.

→ Once we have IP address, we are connected to internet.

→ We can use a router to connect multiple devices.

→ ISPs act as hubs on the internet since they are often connected directly to the internet backbone.

→ Some examples of ISPs in Nepal are Worldlink, Vianet, Nepal telecom, Classic tech, etc.

PAGE

classmate

DATE

→ List of various ISPs according to geographical region.

1) International Service Providers
2) National " "
3) Regional " "
4) Local service providers

* Backbone Network:-

A backbone or core network is a part of a computer network which interconnects networks providing a path for the exchange of information between LANs or subnetworks.
It is a network containing a high capacity connection infrastructure to different part of the network.

Types of Backbone network:

1. Bus Backbone (Distributed Backbone)

→ Uses Bus topology for the backbone.
→ In the figure below, the Bus backbone structure is used as a distribution backbone for connecting different buildings in an organization
→ Each building may have either a single LAN or another backbone which comes in star backbone.
→ The structure is bridge based backbone with four LANs

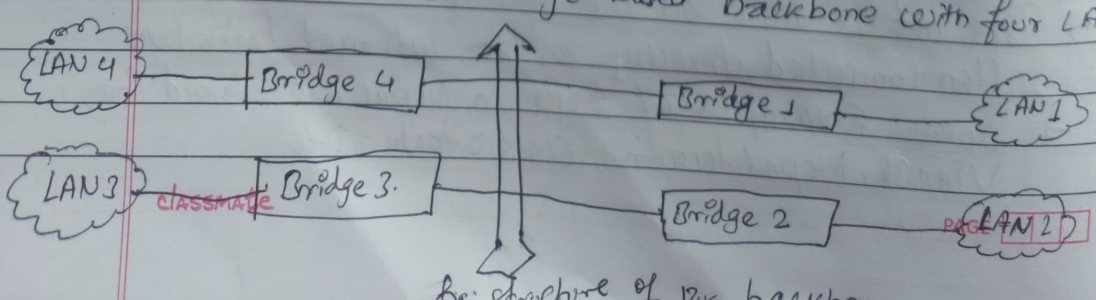


Fig: structure of Bus backbone

DATE

2. Star backbone.

→ Uses star topology for the backbone

→ In the figure below, the switch does the job of backbone & connect the LANs.

→ This type of backbone are basically used as distribution backbone inside a building

→ The backbone network which is just a switch, can be installed in the basement or the 1st floor, & separate cables can run from the switch to each LAN.

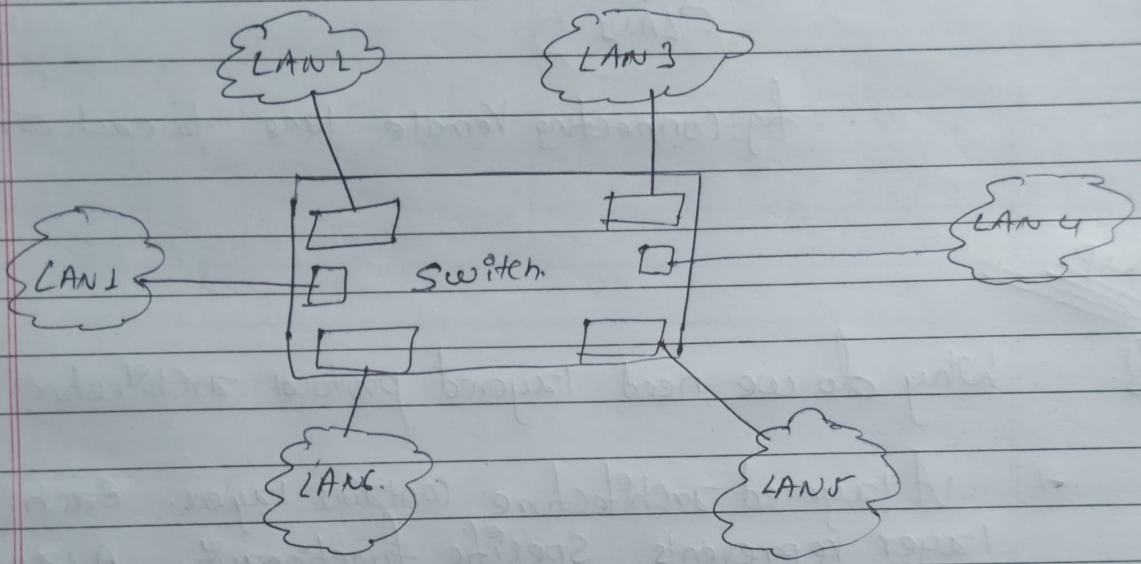


fig: Structure of star backbone.

* Connecting remote LANs (interconnection of remote control)

Connecting remote LANs is one of the common application for a back bone network. This type of backbone network is useful when a company has several offices with LANs & needs to connect them.

→ The network connection are done through bridge called remote bridge which acts as connecting devices to connect LANs as point to point network link, such as leased telephone lines or ADSL lines. The following figure shows a backbone connecting remote LANs:

PAGE

classmate

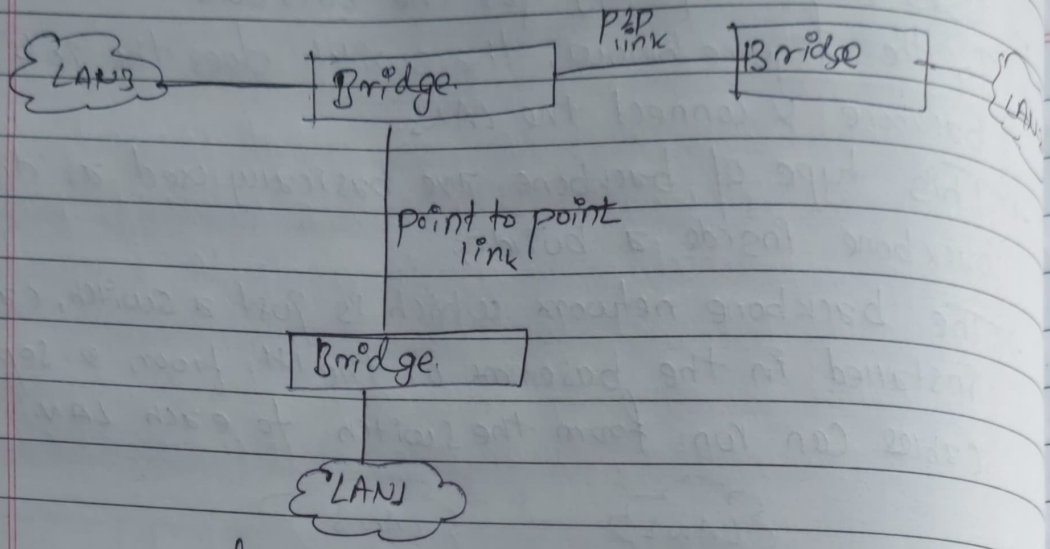


fig: Connecting remote lans to each other

TMP

Q. Why do we need layered protocol architecture?

→ A layered architecture contains layers. Each layer represents specific functionality. A layer is normally a collection of protocols. A layered architecture provides a clean-cut interface so that minimum information is shared among different layers.

Its main goal is to split the design into tiny parts. Each lower layer contributes its services to the top layer resulting in a complete collection of services for managing communication & running applications.

It provides more flexibility to modify & develop network services. Some ex: OSI, TCP/IP etc.

DATE

Questions asked from this Chapter

(2076 - 5 marks)

Q. Explain LAN with example. How is it different from PAN?

Q. Define network topology. Explain ring topology with its merits & demerits (2076 - 5 marks)

Q. What is protocol? Why do we need layered protocol architecture? Explain each layer of OSI. (2071 - 10 marks) (2074 - 10 marks) (2069 - 10 marks) (2073) (2070)

Q. Explain each layer of TCP/IP model in detail. Compare it with OSI model. (2076 - 10 marks) (2070 - 10 marks)

Q. What do you mean by Internet Protocol Stack? (2068 & 69)

Q. Explain Client Server System? How is it different from peer to peer system? (2071)

PAGE