CHAPTER ONE: INTRODUCTION

Network - A group of computers connected together in a way that allows information to be exchanged between the computers.

Node - Anything that is connected to the network. While a node is typically a computer, it can also be devices such as:

- Mainframes, minicomputers, supercomputers
- Workstations
- Printers, disk servers, robots
- X-terminals
- Gateways, switches, routers, bridges
- Cellular phone, Pager.
- Refrigerator, Television, Video Tape Recorder

Segment - Any portion of a network that is separated, by a switch, bridge or router, from other parts of the network.

Backbone - The main cabling of a network that all of the segments connect to. Typically, the backbone is capable of carrying more information than the individual segments. For example, each segment may have a transfer rate of 10 Mbps (megabits per second: 1 million bits a second), while the backbone may operate at 100 Mbps.

Topology - The way that each node is physically connected to the network.

1.1 Network Topologies

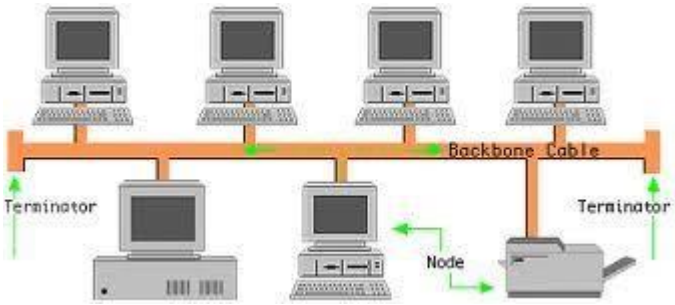
A network topology can be physical or logical.

Physical Topology is the actual layout of a network and its connections. Logical Topology is the way in which data accesses the medium and transmits packets. There are several network topologies:

1.1.1 Physical Bus Topology

Each node is daisy-chained (connected one right after the other) along the same backbone. Information sent from a node travels along the backbone until it reaches

its destination node. Each end of a bus network must be terminated with a resistor to keep the packets from getting lost.



Physical Bus Topology

Advantages

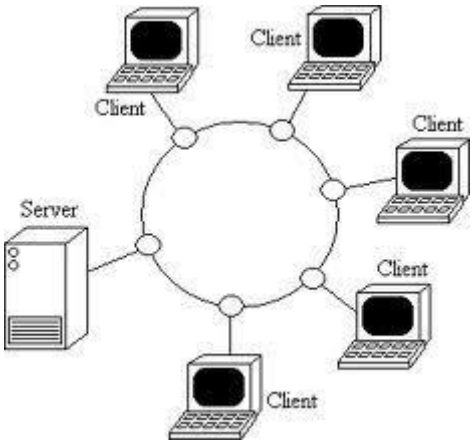
- Inexpensive to install.
- Easy to add stations.
- Use less cable compared to other topologies.
- Works well for small networks.

Disadvantages

- No longer recommended, due to frequent collisions of packets
- If backbone breaks, whole network down
- Limited no of devices can be attached
- Difficult to isolate problems.
- Sharing same cable slows response rates

1.1.2 Physical Ring Topology

Similar to a bus network, rings have nodes daisy chained, but the end of the network in a ring topology comes back around to the first node, creating a complete circuit. Each node takes a turn sending and receiving information through the use of a token. The token along with any data is sent from the first node to the second node which extracts the data addressed to it and adds any data it wishes to send. Then second node passes the token and data to the third node, etc. until it comes back around to the first node again. Only the node with the token is allowed to send data . All other nodes must wait for the token to come to them.



Physical Token Ring

Advantages

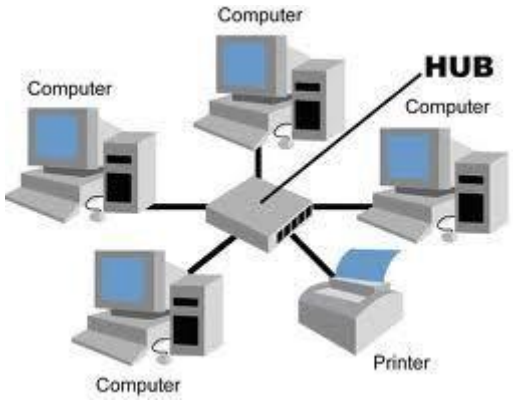
- Data packets travel at great speed
- No collisions
- Easier to fault find
- No terminators required

Disadvantages

- Requires more cable than a bus
- A break in the ring will bring it down
- Not as common as the bus – less devices available

1.1.3 Physical Star Topology

In a star network, each node is connected to a central device called a hub. The hub takes a signal that comes from any node and passes it along to all the other nodes in the network. A hub does not perform any type of filtering or routing of the data. A hub is a junction that joins all the different nodes together.



Advantages

- Easy to add devices as the network expands
- One cable failure does not bring down the entire network (resilience)
- Hub provides centralised management
- Easy to find device and cable problems
- Can be upgraded to faster speeds
- Lots of support as it is the most used

Disadvantages

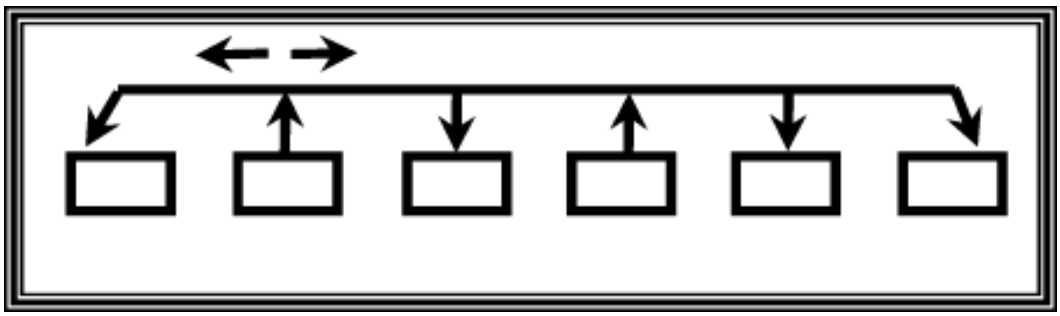
- A star network requires more cable than a ring or bus network
- Failure of the central hub can bring down the entire network
- Costs are higher (installation and equipment) than for most bus networks

Star networks can be extended by interconnecting several hubs to form segments.

1.1.4 Logical Topologies

There are three logical topologies (bus, ring, and switching) which are usually implemented as a physical star.

1.1.5 Logical Bus Topology



HUB

Modern Ethernet networks are Star Topologies (physically) but logically they are bus topologies. The Hub is at the centre, and defines a Star Topology.

In any network, computers communicate by sending information across the media as a series of signals. In a logical bus topology, the signals travel along the length of the cable in all directions until they weaken enough so as not to be detectable or until they encounter a device that absorbs them. This traveling across the medium is called **signal propagation**

When a computer has data to send, it addresses that data, breaks it into manageable chunks, and sends it across the network as electronic signals

- All computers on a logical bus receive them
- Only the destination computer accepts the data
- All users must share the available amount of transmission time, implying network performance is reduced
- Collisions are bound to occur since all nodes are sharing same bus.

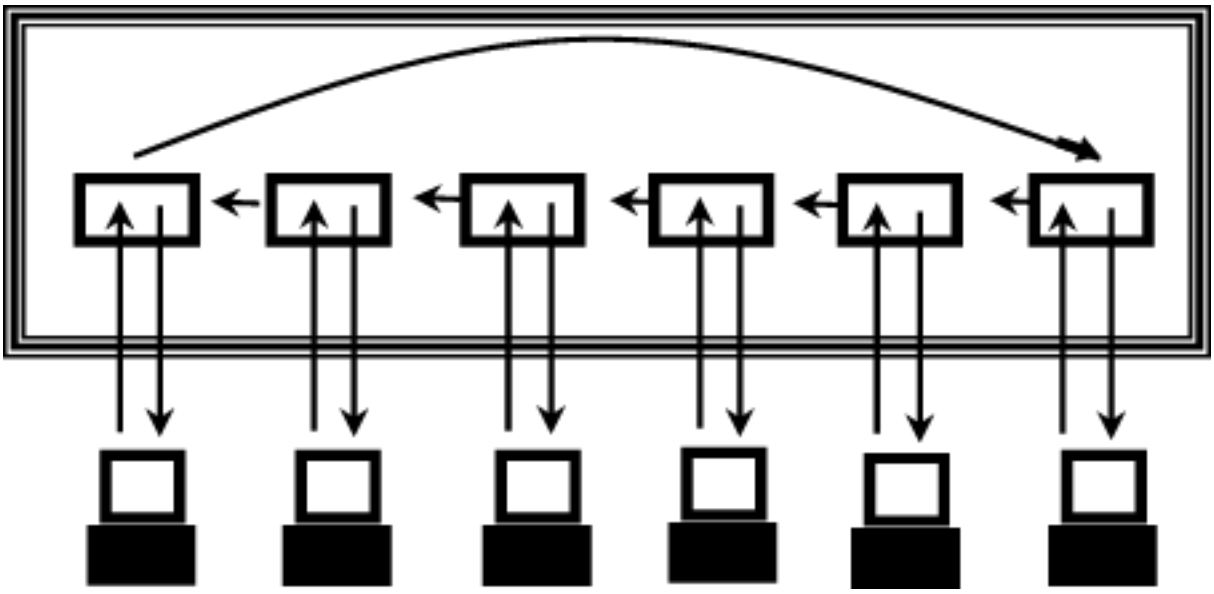
Advantages

- A single node failure does not bring the network down
- Most widely implemented topology
- Network can be added to or changed without affecting other stations

Disadvantages

- Collisions can occur easily
- Only one device can access the network media at a time

1.3.2 Logical Ring Topology



Multiple Access Unit(MAU)

Data in a logical ring topology travels from one computer to the next computer until the data reaches its destination. Token passing is one method for sending data around a ring

Token is a small packet which passes around the ring to each computer in turn.

If a computer (sender) has packets to send, it modifies the token, adds address and data, and sends it around the ring. The receiver returns an acknowledgement packet to the sender.

Upon receiving the acknowledgement packet, the sender releases the tokens and sends it around the ring for another sender to use.

Logical ring can be implemented on a physical star. Modern logical ring topologies use ―smart hubs‖ that recognize a computer‘s failure and remove the computer from the ring automatically. One advantage of the ring topology lies in its capability to share network resources fairly.

Advantages

- The amount of data that can be carried in a single message is greater than on a logical bus.
- There are no collisions.

Disadvantages

- A broken ring will stop all transmissions.
- A device must wait for an empty token to be able to transmit.

1.2.6 Switching

A switch takes a signal coming from a device connected and builds a circuit on the fly to forward the signal to the intended destination computer

Superior to other logical topologies because unlike bus and ring, multiple computers can communicate simultaneously without affecting each other. Switching is the dominant logical topology in LAN design.

1.2 Transmission Media

This refers to the mode in which messages are delivered from one node to another over the network. There are several types of media:

1.2.1 Guided Transmission Media - uses a conductor cable to transmit data e.g. twisted pair(shielded/unshielded), coaxial cable.

Twisted pair Cable

Twisted pair is two insulated copper wires that are twisted around each other to minimize interference and noise from other wires. Based on the presence of individual shield and overall (outer) shield, there are three types of twisted pair, i.e. UTP, STP, and ScTP. Individual shield encloses a single twisted pair, while outer shield encloses all twisted pairs in a cable. A shield is a protective sheath that is made from conductive material (metal) and functions to protect the twisted

pair from external interference. An insulator is made from non-conductive material, such as plastic.

UTP (Unshielded Twisted Pair) is a cable containing several twisted pairs that is only insulated but not shielded. UTP is the most widely used cable in telephone and computer networks because it is relatively cheaper than other cables and performs well in normal electrical environment such as inside an office or a house.
Coaxial cable contains a solid or stranded wire in the core that is insulated with a dielectric layer, then protected with a solid or braided metallic shield, and covered with an outer insulator. Electromagnetic wave propagation in a coaxial cable is confined within the space between the core and the outer conductors. The structure of a coaxial cable makes it less susceptible to interference, noise, and crosstalk than the twisted pair cable.

Coaxial Cable

1.2.2 Glass or plastic - Uses optical technology to transmit data using light waves e.g. fiber optics

Fibre Optic Cable

Fiber-optic cable or optical fiber provides a medium for signals using light rather than electricity. Light waves are immune to electromagnetic interference and crosstalk. Optical fiber can be used for much longer distances before the signal must be amplified. Data transmission using optical fiber is many times faster than with electrical methods.

1.2.3 Wireless transmission - Uses air interface to transmit e.g. microwave, satellite. Microwave links are widely used to provide communication links when it is

impractical or too expensive to install physical transmission media. Two properties of microwave transmission place restrictions on its use. First, microwaves travel in a straight line and will not follow the earth's curvature. Second, atmospheric conditions and solid objects interfere with microwaves. For example, they cannot travel through buildings.

Satellite transmission is microwave transmission in which one of the stations is a satellite orbiting the earth. A microwave beam is transmitted to the satellite from the ground. This beam is received and retransmitted (relayed) to the predetermined destination. Receiver and transmitter in satellites is known as transponder.
The optimum frequency range for satellite transmission is in the range 1 to 10 GHz. Below 1 GHz, there is significant noise from natural sources,

atmospheric noise, and noise from electronic devices. Above 10 GHz, the signal is attenuated by atmospheric absorption.

1.3 Network Protocols

Communication between devices on a network is governed by a set of rules called protocols. There are two types of network protocols, TCP/IP and OSI.

1.3.1 TCP/IP Protocol

TCP/IP is responsible for a wide range of activity: it interfaces with hardware, route data to appropriate nodes, provides error control, and much more.

The developers of TCP/IP designed a modular protocol stack- meaning that the TCP/IP system was divided into separate components or layers. But why use a modular design? Not only does it aid in the education process, but it also lets manufacturers easily adapt to specific hardware and operating system needs.

For example- if we had a token ring network and an extended star network, we surely wouldn‘t want to create entirely different network software builds for each one. Instead, we can just edit the network layer, called the Network Access Layer, to allow compatibility. Not only does this benefit manufacturers, but it greatly aids networking students in education. The TCP/IP suite is divided into four layers.

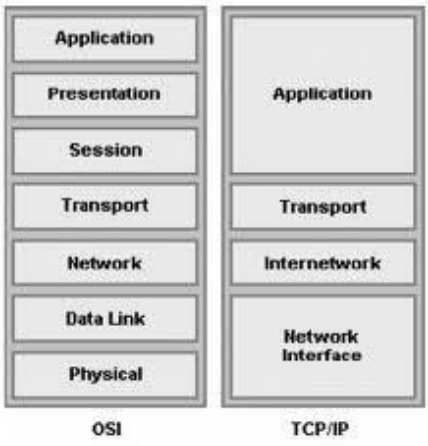
Network Access Layer – The Network Access Layer is fairly self explanatory- it interfaces with the physical network. It formats data and addresses data for subnets, based on physical hardware addresses. More importantly, it provides error control for data delivered on the physical network.

Internet Layer – The Internet Layer provides logical addressing. More specifically, the internet layer relates physical addresses from the network access layer to logical addresses. This can be an IP address, for instance. This is vital for passing along information to subnets that aren‘t on the same network as other parts of the network. This layer also provides routing that may reduce traffic, and supports delivery across an internetwork. (An internetwork is simply a greater network of LANs, perhaps a large company or organization.)

Transport Layer – The Transport Layer provides flow control, error control, and serves as an interface for network applications. An example of the transport layer

would be Transmission Control Protocol (TCP) - a protocol suite that is connection-oriented. We may also use UDP- a connectionless means of transporting data.

Application Layer – Lastly, we have the Application Layer. We use this layer for troubleshooting, file transfer, internet activities, and a slew of other activities. This layer interacts with many types of applications, such as a database manager, email program, or Telnet.



1.3.2 Open System Interconnection(OSI) Protocol

The International Organization of Standardization (ISO) defined procedures for computer communications which was called Open System Interconnection (OSI) Reference Model or OSI Model for short. The OSI Model describes how data flows from one computer to another computer in a network.

The OSI Model

The Open System Interconnection Model, more commonly known as simply OSI, is another model that can help break the TCP/IP suite into modules. Technically speaking, it is exactly the same as the TCP/IP model, except that it has more layers. This is currently being pushed by Cisco since it aids in learning the TCP/IP stack in an easier manner.

Physical Layer – They Physical Layer converts data into streams of electric or analog pulses- commonly referred to as ―1‘s and 0‘s.‖ Data is broke down into simple electric pulses, and rebuilt at the receiving end.

Data Link Layer – The Data Link layer provides an interface with the network adapter, and can also perform basic error checking. It also maintains logical links for subnets, so that subnets can communicate with other parts of the network without problem.

Network Layer – Much like the Transport Layer of the TCP/IP model, the Network Layer simply supports logical addressing and routing. The IP protocol operates on the Network Layer.

Transport Layer – Since we left out the error and flow control in the Network Layer, we introduce it into the Transport Layer. The Transport Layer is responsible for keeping a reliable end-to-end connection for the network.

Session Layer – The Session Layer establishes sessions between applications on a network. This may be useful for network monitoring, using a login system, and reporting. The Session Layer is actually not used a great deal over networks, although it does still serve good use in streaming video and audio, or web conferencing.

Presentation Layer – The Presentation Layer translates data into a standard format, while also being able to provide encryption and data compression. Encryption or data compression does not have to be done at the Presentation Layer, although it is commonly performed in this layer.

Application Layer – The Application Layer provides a network interface for applications and supports network applications. This is where many protocols such as FTP, SMTP, POP3, and many others operate. Telnet can be used at this layer to send a ping request- if it is successful, it means that each layer of the OSI model should be functioning properly.

In most cases the physical topology will almost certainly be a star, and the logical topology is almost always switching. Ethernet switches are typically used on a LAN,but you might consider other logical topologies for reasons such as:

- Use of legacy equipment – such as token ring
- Network size – using hub-based bus topology
- Cost restrictions – using hub instead of switch
- Difficulty to run cables – consider wireless ?

2.1 Conducting site Survey

The purpose of a site survey is to understand the nature of the business premises interms of how the building, office space and electrical wiring are set up. It helps answer whether or not the type of network requested can be supported by the organization of the building. It also helps estimate how much material will be required to layout the network.

2.2 Capacity Planning

Capacity planning involves trying to determine the amount of network bandwidthnecessary to support an application or a set of applications.
A number of techniques exist for performing capacity planning, including linear projection, computer simulation, benchmarking, and analytical modeling.
Linear projection involves predicting one or more network capacities based on thecurrent network parameters and multiplying by some constant.
A computer simulation involves modeling an existing system or proposed systemusing a computer-based simulation tool.
Benchmarking involves generating system statistics under a controlled environmentand then comparing those statistics against known measurements.
Analytical modeling involves the creation of mathematical equations to calculatevarious network values.

2.3 Creating a Baseline

Involves the measurement and recording of a network‘s state