**JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY**

**B.SC. COMPUTER SCIENCE: THIRD YEAR SECOND SEMESTER.**

**ICS 2306: COMPUTER NETWORKS**

NB: Additional notes may be given if/when found to be necessary.

**Course Outline**

Topology and architecture of computer networks. Layered protocols. OSI and TCP/IP protocols. Local area networks. Wide area networks. Routing protocols. Gatewaying.

|  |  |  |
| --- | --- | --- |
| **Chapter** | **Chapter Name** | **Chapter Content** |
| **1.** | Introduction to computer networks | Definitions; components of a computer network; characteristics of an effective computer network; the network criteria; classification of computer networks; peer to peer vs client-server networks. |
| **2.** | Network Topologies | Physical topologies: the bus, star, ring, mesh and tree topologies; logical topologies. |
| **3.** | Networking Components | Data communication equipment and data terminal equipment; networking and internetworking devices; routers, switches, bridges, brouters, MODEMs, Network Interface Cards, gateways, firewalls among other devices. |
| **CAT 1 AND ASSIGNMENT 1** | | |
| **4.** | Networking software | The OSI reference model, the TCP/IP model; Networking protocols; routing software; network Operating Systems. |
| **5.** | Transmission Media | Bounded/Physical transmission media: twisted-pair cables, coaxial cables, fibre optic cables; Unbounded/wireless transmission media: microwaves, radio waves, infrared waves. |
| **6.** | Network Node Addressing | MAC Addresses, IP addresses. IP version 4 addresses: The format of IPv4 addresses, class A, B and C IP addresses; sub-netting, IP version 6 addresses. |
| **CAT 2 AND ASSIGNMENT 2** | | |
| **7.** | Gatewaying |  |
| **END OF SEMESTER EXAM** | | |

**CHAPTER 1: INTRODUCTION TO COMPUTER NETWORKS**

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. One way of having remote communications is by use of a computer network. A computer network refers to a set of infrastructure made up of hardware components, networking software as well as communication channels that enable two or more computers to communicate with each other.

The effectiveness of a computer network depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. The system should not feature jitter during data delivery.

**Adavntages of Computer Networks** - FIND MORE!!

* Mode of information sharing among different people

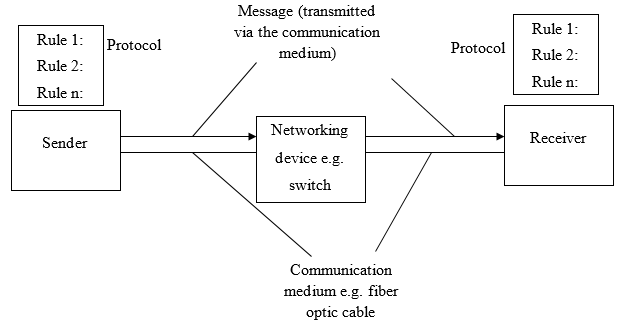
**Disadvantages of Computer Networks** - FIND MORE!!

* Security issues
* Increased cost

**Components of a Computer Network**

1. **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Nodes**. Nodes are computers that are used for sending and receiving information on a network. The sender is the device that sends the data message. The receiver on the other hand is the device that receives the message. Senders and receivers can be computers, workstations, telephone handsets and so on.
3. **Transmission medium**. The transmission medium is the physical or wireless path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fibre-optic cable, and radio waves.
4. **Networking/internetworking devices.** These devices act as network junctions joining various communication media together which in turn are linked to the various nodes in the network.
5. **Networking software**. Networking software include protocols and routing algorithms and sometimes a network operating system. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

The diagram below shows how these various components are interconnected to form a network.



*Figure 1: Components of a computer network*

**Network Criteria**

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1. ***Performance***

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

1. ***Reliability***

Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

1. ***Security***

Network security issues include protecting data from unauthorized access, protecting data from damage, and implementing policies and procedures for recovery from breaches and data losses.

**Classification of Computer Networks**

Computer networks are classified into different types based on the following principles:

1. Categorization based on the geographic spread of the network.
2. Categorization based on access restrictions.
3. Categorization based on the communication model.
4. Categorization based on the switching model.
5. Categorization based on the role of nodes on the network.
6. **Categorization based on the geographic spread of the network**

Under this principle, we have three types of computer networks as explained below.

LAN, MAN, and WAN.

1. **Local Area Networks (LANs)**

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

* Their size,
* Their transmission technology, and
* Their topology.

LANs are restricted in size (smallest in coverage), which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have a low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

1. **Metropolitan Area Network (MAN)**

A metropolitan area network, or MAN, covers a city. MANs can be used where an organization has different offices or branches across a town linked together by a computer network. Because the software and hardware architectures may be different, internetworking principles may have to be applied.

1. **Wide Area Network (WAN).**

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called hosts. The hosts are connected by a communication subnet or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet Service Provider (ISP). The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design. In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fibre, or even radio links. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells.

The principle of a packet-switched WAN is so important. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.

Not all WANs are packet-switched. A second possibility for a WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases, they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna. Satellite networks are inherently broadcast and are most useful when the broadcast property is important.

1. **Categorization based on access restrictions**

Networks under this principle are classified into the following two types:

1. **Private Networks**: these are networks that are set up for use by a particular organization. Users usually provide a username and a password to get access.
2. **Public networks**: these are networks that can be accessed by anyone, and sometimes users are required to pay a fee for their use. Examples of public networks are the internet and public WIFI such as the one offered in hotels. However, by using a public network you expose your device and the data you are communicating to security threats.
3. **Classification based on the Communication Model**

This principle classifies networks into the following two categories.

1. **Point to Point Networks**

In these networks, data is sent from source to destination through direct links. There is no broadcasting in the network.

1. **Broadcast Networks**

In a broadcast network, the transmission is by the broadcast method whereby the source advertises a message to all the nodes in the network. The destination node then picks up the message from the network. Examples of these types of networks include the normal TV channels.

1. **Categorization Based on the Switching Model**

Here we have three types of networks.

Circuit switching, packet switching, and message switching.

1. **Circuit Switching Networks**

In this type of network, a dedicated path from source to destination is created before any message is sent on the network. Although this method of data transfer gives a good dedicated channel for communication, it is wasteful in that the channel cannot be utilized by someone else even when no data is being transmitted.

1. **Packet Switching Networks**

Here, the data being transmitted is broken down into small units called packets. The packets are then sent onto the network and they are allowed to follow different paths to the destination. At the destination, the original message is reconstructed.

**Differences between circuit switching and Packet Switching**

The table below has some differences between circuit switching and packet switching.

|  |  |  |
| --- | --- | --- |
| **SNO.** | **Circuit Switching** | **Packet Switching** |
| 1. | In circuit switching, each data unit knows the entire path address which is provided by the source. | In Packet switching, each data unit knows the final destination address. The intermediate path is decided by the routers. |
| 2. | In circuit switching, data is processed at the source system only. | In Packet switching, data is processed at all intermediate nodes including source node. |
| 3. | The delay between data units in circuit switching is uniform. | The delay between data units in packet switching is not uniform. |
| 4. | Resource reservation is the feature of circuit switching because the path is fixed for data transmission. | There is no resource reservation because bandwidth is shared among users. |
| 5. | Circuit switching is more reliable. | Packet switching is less reliable. |
| 6. | Wastage of resources is more in circuit switching. | Less wastage of resources as compared to circuit switching |
| 7. | It is not a store and forward technique. | It is a store and forward technique. |
| 8. | Transmission of the data is done by the source. | Transmission of the data is done not only by the source but also by the intermediate routers. |
| 9. | Congestion can occur during connection establishment time. | Congestion can occur during the data transfer phase. |

1. **Message Switching Networks**

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Before the advancements in packet switching, message switching acted as an efficient substitute for circuit switching. It was initially employed in data communications such as telex networks and paper tape relay systems. Message switching has largely been replaced by packet switching, but the technique is still employed in ad hoc sensor networks, military networks and satellite communications networks.

In message switching, the source and destination nodes are not directly connected. Instead, the intermediary nodes (mainly switches) are responsible for transferring the message from one node to the next. Thus, every intermediary node inside the network needs to store every message prior to retransferring the messages one-by-one as adequate resources become available. If the resources are not available, the messages are stored indefinitely. This characteristic is known as store and forward.

Every message should include a header, which typically consists of routing information, such as the source and destination addresses, expiry time, priority level, etc. Because message switching implements the store-and-forward technique, it efficiently uses the network. Also, there is no size limit for the messages. However, this technique also has several disadvantages:

* Because the messages are fully packaged and saved indefinitely at every intermediate node, the nodes demand substantial storage capacity.
* Message-switched networks are very slow as the processing takes place in each and every node, which may result in poor performance.
* This technique is not adequate for interactive and real-time processes, such as multimedia games and voice communication.

1. **Categorization based on the role of nodes on the network**
2. **Peer to Peer (P2P) Networks**

A peer to Peer network is one in which hosts in the network have the same status on the network and they have an equivalent processing power. This means that the peers can provide services to each other like file-sharing or they can cooperate to perform some processing together.

1. **Client-Server Networks**

In the client-server networks, one powerful computer or group of computers can work together to listen to the request of other computers on the network and to provide responses. It is important to note that a server may not necessarily be a hardware computer; it can be implemented in software.

**Advantages of Client-Server Networks over Peer to Peer networks**

1. In server-based networks, users can share equipment like printers.
2. The management of users becomes very easy since the administrator can manage all users from a single computer (the server).
3. All data is stored in a central store so it becomes easy to back up.
4. A server-based network has the ability to manage thousands of users (and even more). This is hard in a peer to peer network.

**Disadvantages of Client-Server Networks over Peer to Peer networks**

1. **Congestion in the network:** Too many requests from the clients may lead to congestion, which rarely takes place in the P2P network. Overload can lead to the breaking-down of servers. In peer-to-peer, the total bandwidth of the network increases as the number of peers increase.
2. Client-Server architecture is **not as robust** as a P2P and if the server fails, the whole network goes down. Also, if you are downloading a file from a server and it gets abandoned due to some error, the download stops altogether. However, if they would have been peers, they would have provided the broken parts of the file.
3. Cost: It is very expensive to install and manage this type of computing.
4. You **need professional IT people** to maintain the servers and other technical details of the network.

**Advantages of Peer to Peer Networks**

1. It is easy to install and so is the configuration of computers on this network.
2. All the resources and contents are shared by all the peers, unlike client-server architecture where the server shares all the contents and resources.
3. A P2P network is more reliable as central dependency is eliminated. Failure of one peer doesn’t affect the functioning of other peers. In the case of the client-server network, if the server goes down the whole network gets affected.
4. There is no need for a full-time system administrator. Every user is the administrator of his machine. User can control their shared resources.
5. The overall cost of building and maintaining this type of network is comparatively less than that of a client/server network.

**Disadvantages of Peer to Peer Networks**

1. Network security has to be applied to each computer separately.
2. Backup has to be performed on each computer separately.
3. No centralized server is available to manage and control the access of data and other resources in this network. This makes the administration of a peer to peer network hard.
4. When one peer is being accessed by many other peers, it can slow down the performance for the user.

**CHAPTER 2: NETWORK TOPOLOGIES**

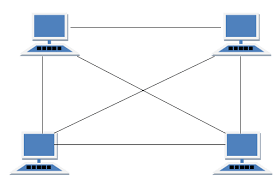
There are two types of network topologies: logical topologies and physical topologies.

**Physical topologies**

Physical topologies refer to the way in which the network of computers is connected. Each topology is suited to specific tasks and has its own advantages and disadvantages. The choice of topology is dependent upon type and number of equipment being used, planned applications, and rate of data transfer required, response time, and cost. Topology can also be defined as the *geometrical interconnection pattern* by which the stations (nodes/computers) are connected using suitable transmission media (which can be point-to-point and broadcast). Various commonly used topologies are discussed in the following sections.

1. **Mesh/Fully-connected Topology**

In this topology, each node or station is connected to every other station as shown in the figure below.



*Figure 2: A mesh network of four nodes*

The key characteristics of the mesh topology are given below:

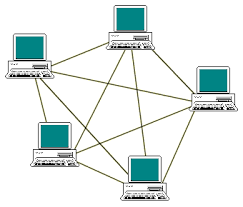
1. Each node in the network is directly connected to all the other nodes.
2. Robust – Highly reliable because there is no broadcasting since there are direct links between communicating nodes.
3. Not flexible.
4. Poor expandability.

Two nodes are connected by dedicated point-point links between them. So the total number of links to connect n nodes = n(n-1)/2.Media used for the connection (links) can be twisted pair, co-axial cable, or optical fiber.With this topology, there is no need to provide any additional information that is from where the packet is coming, along with the packet because two nodes have a point-point dedicated link between them. And each node knows which link is connected to which node on the other end.

The mesh topology:

* is not flexible and
* has poor expandability as to add a new node n links have to be laid because that new node has to be connected to each of the existing nodes via the dedicated link as shown in the figure below.
* For the same reason, the cost of cabling will be very high for a larger area.

And due to these reasons, this topology is rarely used in practice.



*Figure 3: A mesh topology with five nodes*

1. **Bus Topology**

In a bus topology, all stations attach through appropriate hardware interfacing known as a *tap*, directly to a linear transmission medium, or bus as shown in the figure below. Full-duplex operation between the station and the tap allows data to be transmitted onto the bus and received from the bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations. At each end of the bus, there is a *terminator*, which absorbs any signal, preventing the reflection of signals from the endpoints. If the terminator is not present, the endpoint acts as a mirror and reflects the signal back causing interference and other problems.

**Shared**

**Media**



**Terminator**

**Tap**

**Stations**

*Figure 4: Connection of nodes in a bus topology*

The key characteristics of this topology are as outlined below:

1. Flexibility.
2. Expandability.
3. Moderate reliability.
4. Moderate performance.

A shared link is used between different stations. Hence it is very cost-effective. One can easily add any new node or delete any node without affecting other nodes; this makes this topology easily expandable. Because of the shared medium, it is necessary to provide some extra information about the desired destination, i.e. to explicitly specify the destination in the packet, as compared to mesh topology. This is because the same medium is shared among many nodes. As each station has a unique address in the network, a station copies a packet only when the destination address of the packet matches with the self-address. This is how data communications take place among the stations on the bus.

As there are dedicated links in the mesh topology, there is a possibility of transferring data in parallel. But in a bus topology, only one station is allowed to send data at a time and all other stations listen to it, as it works in a broadcast mode. Hence, only one station can transfer the data at any given time. A suitable medium access control technique should be used so as to provide some way to decide “who” will go next to send data.

As the distance through which signal traverses increases, attenuation increases. If the sender sends data (signal) with a small strength signal, the farthest station will not be able to receive the signal properly. While on the other hand if the transmitter sends the signal with a larger strength (more power) then the farthest station will get the signal properly but the station near to it may face over-drive. Hence, delay and signal unbalancing will limit the maximum length of the shared medium, which can be used in bus topology.

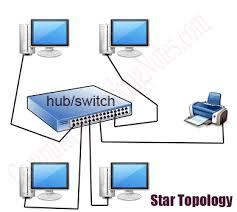
The advantages of the bus topology are as listed below.

1. The network is easy to expand. It is easy to add and remove nodes from the bus.
2. The network is easy and cheap to set up.
3. It is easy to troubleshoot and manage.

However, despite these advantages, the bus topology has the following disadvantages.

1. Because of broadcasting, the network is less secure.
2. There can be a single point of failure if the bus breaks.
3. **Star Topology**

In the star topology, each station is directly connected to a common central node as shown in the figure below. The central node can either be a hub or a switch, and the connection is usually via two point-to-point links, one for transmission and one for the reception.



*Figure 5: The Star Topology*

Key features:

1. High speed.
2. Very flexible.
3. High reliability.
4. High maintainability.

In general, there are two alternatives for the operation of the central node.

One approach is for the central node to operate in **a broadcast fashion**. The transmission of a frame from one station to the node is retransmitted on all of the outgoing links. In this case, although the arrangement is physically a star, it is logically a bus; a transmission from any station is received by all other stations, and only one station at a time may successfully transmit. In this case, the central node acts as a *repeater or a hub*.

Another approach is for the central node to act as **a frame-switching device**. An incoming frame is buffered in the node and then retransmitted on an outgoing link to the destination station. In this approach, the central node acts as a *switch*and performs the switching or routing function. This mode of operation can be compared with the working of a telephone exchange, where the caller party is connected to a single called party, and each pair of a subscriber who needs to talk have a different connection.

Very high speeds of data transfer can be achieved by using star topology, particularly when the central node is used in the switch mode. This topology is the easiest to maintain, among the other topologies. As the number of links is proportional to n, this topology is very flexible and is the most preferred topology.

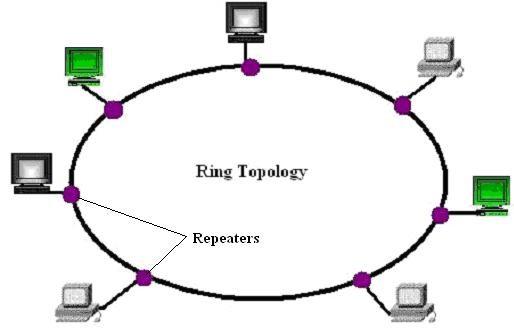
The advantages of the star topology include the following:

1. The network is not difficult to set up - easily expandable without network disruption.
2. The network is easy to maintain - troubleshoot and isolate problems.
3. Different nodes have dedicated links to the central node - cable failure only affects a single user.

Disadvantages:

1. The topology requires a lot of cables to connect every device to the central node.
2. The central node can form a single point of failure.
3. More expensive than bus topologies because of hub costs and extra cables.
4. **Ring topology**

In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop as shown in the figure below. The repeater is a comparatively simple device, capable of receiving data on one link and transmitting them, bit by bit, on the other link as fast as they are received, with no buffering at the repeater. The links are unidirectional; that is, data are transmitted in one direction only and all are oriented in the same way. Thus, data circulate around the ring in one direction (clockwise or counterclockwise).



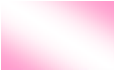
*Figure 6: The ring topology*

Each station attaches to the network at a repeater and can transmit data onto the network through that repeater. As with the bus and tree, data are transmitted in frames. As a frame circulates past all the other stations, the destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed. Because multiple stations share the ring, medium access control is needed to determine at what time each station may insert frames.

The repeater works in the following three modes:

Listen, transmit, and by-pass mode.

1. **Listen mode**: In this mode, the station/repeater listens to the communication going over the shared medium as shown in the figure below.



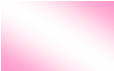
Incoming packets Outgoing packets

To the station

*Figure SEQ Figure \\* ARABIC 7: The repeater in listen mode*

1. **Transmit mode**: In this mode, the station transmits the data over the network as shown in the figure below.

Outgoing packets



Incoming packets

To the station

*Figure SEQ Figure \\* ARABIC 8: The repeater in transmit mode*

1. **By-Pass mode**: When the node is faulty then it can be bypassed using the repeater in bypass mode, i.e. the station doesn’t care about what data is transmitted through the network, as shown in the figure below. In this mode, there is no delay introduced because of this repeater.



The station is bypassed

Incoming packets Outgoing packets

*Figure SEQ Figure \\* ARABIC 9: The repeater in bypass mode*

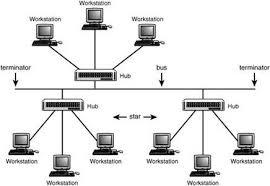
The advantages of the ring topology include the ones outlined below:

1. The network is simple to install.
2. The network uses less cable - cable faults are easily located - easier troubleshooting.
3. The network is more secure since there is no broadcasting.

The ring topology has the following disadvantages

1. This topology is not very reliable, because when a link fails the entire ring connection is broken. This forms a single point of failure. But reliability can be improved by using a *wiring concentrator*, which helps in bypassing a faulty node and somewhat is similar to a star topology.
2. The network may be difficult to troubleshoot in case the ring breaks.
3. Network expansion will cause disruption.
4. **Tree/Hierarchical/Star-Bus Topology**

This is a hybrid topology, where both the bus and the star topology are used. This topology is suitable for interconnecting large networks, whereby groups of star networks are linked to each other via a bus. The figure below depicts how nodes and devices in this topology are interconnected.



*Figure 10: The tree topology*

* This tree topology is very good in an organization as incremental expansion can be done this way. The main features of this topology are scalability and flexibility. This is because when the need arises for more stations that can be accomplished easily without affecting the already established network.
* Another advantage of this network is that if one segment of the network is damaged, other segments are not affected.

The disadvantages of this network include one,

* the topology requires high maintenance, and two,
* the bus forms a single point of failure.

**6) Irregular network** - [See image in file]

**Logical Topologies**

These consist of how nodes communicate with one another on the network. Sometimes they are referred to as communication architecture. Below are some of the available logical topologies. All these logical topologies have been named and classified by the IEEE.

1. **The Ethernet Standard**

This was the earliest classification, mainly of the protocol CSMA/CD that runs on the bus network. There are several standards within the Ethernet standard, depending on the data frame format that is being used to transfer data. The most common standards are Ethernet 802.2 and Ethernet 802.3.

The Ethernet protocol works as follows: All the computers connected to the medium listen to the medium for any activity. At any given time, only one device is allowed to transmit data. If two devices try to transmit data at the same time, then a collision occurs and they both refrain for a random time interval, before trying to transmit again. This particular scenario is called the conflict resolution mechanism. The switched Ethernet does not use broadcasting on the whole cable, but divides the network into logical segments, therefore allowing multiple nodes to transmit as long as they are in separate logical segments of the network. Initially, Ethernet speeds were pegged at 100mbps. However, improved technology has seen the emergence of the gigabit Ethernet which is able to run at 1gbps. Faster Ethernet speeds have been achieved, even of up to 10 Gbps.

1. **The Local Talk Standard**

The local talk protocol utilizes the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), and it was designed by Apple Computers for use to interconnect their computers. In this protocol, a computer that wants to transmit data sends out a signal to all the others and if no objection is raised, the computer transmits the data. This way, collision is minimized on the network.

1. **The Token Ring Standard**

In this strategy,one workstation/node called the active monitor acts as the controller of the network. It generates a token and places it on the ring for it to move in a unidirectional manner. For a computer to transmit data, it must capture the token and place data and the destination address in it, then release the token on the ring again. The token, upon reaching the destination, is captured and the data read. An acknowledgment is sent back to the sender that the message has been received.

1. **The Fiber Distributed Data Interface (FDDI)**

This standard came about originally with the introduction of the fiber optic cables but it was later adopted, also for non-fiber optics networks like the token ring network. The FDDI is made up of two logical rings, which are concentric. The idea behind this is to increase redundancy such that one ring is the primary ring and the other one is the secondary or back up ring. In case the primary ring breaks, then the secondary ring can take over and transmit data. In situations where the primary ring is functioning well, then the secondary ring can also transmit data and double the speed of data transmission in the network. At any given point, the data flows in opposite directions in the primary and secondary rings.

1. **The Asynchronous Transfer Mode (ATM)**

This type/protocol of data transfer involves breaking down data into simple, fixed-size units called cells. Using virtual circuits, the cells are transferred from source to destination. This protocol makes use of two modes of transmission: baseband transmission and broadband transmission. In baseband transmission, when one computer is transmitting data, it utilizes the whole bandwidth of the cable, hence only one computer can transmit data at a time. Broadband transmission, on the other hand, allows more than one computer to transmit data at the same time since the bandwidth is broken down into pathways (channels), where different data can pass. Broadband transmission depends on multiplexing.

In ATM, the cells are transmitted through a virtual channel in a sequential manner from source to destination, and this enables reliable data transport for the data.

**CHAPTER 3: NETWORKING COMPONENTS**

Networking components can be divided into two categories:

1. **Data Terminal Equipment (DTE)**

These are components that are used by the end-user to send and receive data. Examples of Data Terminal Equipment include computers, mobile phones, etc. These devices are usually located at the user’s premises.

1. **Data Communication Equipment (DCE)**

These devices provide connectivity to a local network and to external networks. Examples of this equipment include routers and switches.

There is a marked difference between networking components and internetworking components. Networking components are usually used on LANs while internetworking components are used to connect networks to each other, therefore they are utilized on WANs. Examples of networking devices include hubs, modems, bridges, LAN switches, the Wireless Access Point (WAP), and Network Interface Cards (NICs). Internetworking devices include routers, the WAN switch, gateways, firewalls, etc.

**Networking Devices**

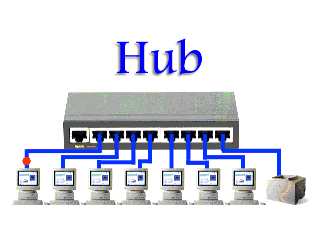
1. **Hubs**

A hub, also known as a concentrator, is a networking device that enables the interconnection of computers on a small network. A hub is a repeater in that once a transmitting computer releases a message unto it, it broadcasts the same message to the other computers on the network. The simplest method to extend a network is to interconnect hubs. But the disadvantage of doing this is that the broadcast domain will be increased and this can cause a decrease in the quality of service, as more computers are added to the network. This can cause a broadcast storm on the network. It is important to note that these days there are switched hubs, which incorporate the switching technology in the hub to avoid broadcasting.

In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a *passive/non-powered* hub. Far more common nowadays is the *active/powered* hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices. A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly referred to as *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as *high-density devices*. Because hubs don’t perform any processing, they do little except enabling communication between connected devices. For today’s high-demand network applications, something with a little more intelligence is required. That’s where switches come in.

The diagram below shows a hub.



*Figure 11: A hub*

1. **Switches**

Like hubs, *switches* are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive. Whereas a hub forwards the data it receives to all of the ports on the device (broadcasting), a switch forwards it only to the port that connects to the destination device. It does this by *learning* the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives.

By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high. The figure below shows a D-link 24-port networking switch.



*Figure 12: D-Link 24-port networking switch*

Below are some switching methods used by switches to forward incoming messages.

1. **Cut-through switching**

In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast but creates the possibility of errors being propagated through the network, as there is no error checking.

1. **Store-and-forward switching**

Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and errors checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes time, and store-and-forward switching is considerably slower as a result.

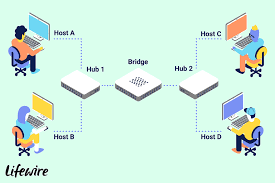
1. **Fragment-free switching**

To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, fragment-free switching can be used. In a fragment-free switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

1. **Bridges**

*Bridges* are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came). When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually, a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network. Such devices are called *learning bridges* because of this functionality.

The figure below shows how a bridge is used to partition a network into different sections. In this figure, when Host A sends a message to Host B, the bridge restricts the message to the left side of the network only, but when, for example, Host A sends a message to Host D, the bridge allows the message to be transmitted from the left side to the right side of the network.



*Figure 13: A network that uses a bridge*

The advantage of partitioning a network using bridges are that one, it reduces the broadcast domain hence raising the quality of service on the network and two, it enables computers in different segments to communicate simultaneously with each other within their segments.

**Types of Bridges**

Three types of bridges are used in networks:

1. **Transparent bridges**

Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.

1. **Source-route bridges**

These bridges were designed by IBM for use in Token Ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet. However, with the decline in the use of token ring networks, these types of bridges are becoming less common by the day.

1. **Translational bridges**

Used to convert one networking data format to another; for example, from Token Ring to Ethernet and vice versa.

Today, bridges are slowly but surely falling out of favor. Ethernet switches offer similar functionality; they can provide logical divisions, or segments, in the network. In fact, switches are sometimes referred to as multiport bridges because of the way they operate.

1. **Routers**

In a common configuration, routers are used to create larger networks by joining two network segments. For example, the SOHO router is used to connect a user to the Internet. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. All modern network operating systems include the functionality to act as a router.

A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router.

Routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to be two things. It must be up-to-date, and it must be complete. There are two ways that the router can get the information for the routing table—through static routing or dynamic routing.

1. **Static Routing**

In environments that use *static routing*, routes and route information are entered into the routing tables manually. Not only can this be a time-consuming task, but also errors are more common. Additionally, when there is a change in the layout, or topology, of the network, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

1. **Dynamic Routing**

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple; they enable routers to pass on information about themselves to other routers so that other routers can build routing tables. There are two types of routing protocols used—the older **distance vector protocols** and the newer **link-state protocols**.

1. **Gateways**

A gateway is an internetworking device that translates one data format to another. In other words, a gateway is a protocol converter. It connects a network to external networks. Therefore, a gateway can be able to interconnect networks of different architectures seamlessly. For this reason, a gateway operates on all levels of the OSI reference model.

Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. A gateway is usually a software, and in many cases, the gateway functionality is incorporated into another device.

1. **Channel Service Unit/Digital Service Unit / (CSU/DSU)**

A Channel Service Unit/Digital Service Unit (CSU/DSU), sometimes called the Data Service Unit, is a device that converts the digital signal format used on LANs into one used on WANs. Such translation is necessary because the networking technologies used on WANs are different from those used on LANs.

The CSU/DSU sits between the LAN and the access point provided by the telecommunications company. Many router manufacturers are now incorporating CSU/DSU functionality into their products.

1. **Network Interface Cards (NICs)**

This is the most basic networking device, and its function is to create a physical connection between the computer and the network. It’s important to install the right network interface card for the right network, although modern networks can support many networking standards. The other function of NICs is to receive data in digital format from a computer and change it to a format that is acceptable to the transmission medium.

For wireless communication, one requires a wireless interface card, also known as a PCMCIA card.

1. **MODEMs**

A *modem*, short for modulator/demodulator, is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up to a LAN.

Modems are slowly becoming obsolete because transmission lines are also becoming digital. They are being replaced by special devices called codecs, whose main function is just to arrange the digital signal from the computer in a particular format for transmission on digital lines.

1. **Transceivers (Media Converters)**

The term transceiver does describe a separate network device, but it can also be technology built and embedded in devices such as network interface cards and modems. In a network environment, a transceiver gets its name from being both a transmitter and a receiver of signals-thus the name transceivers. Technically, on a LAN, the transceiver is responsible for placing signals onto the network media and also detecting incoming signals traveling through the same wire. Given the description of the function of a transceiver, it makes sense that that technology would be found with network interface cards.

Although transceivers are found in network cards, they can be external devices as well. As far as networking is concerned, transceivers can ship as a module or chip type. Chip transceivers are small and are inserted into a system board or wired directly on a circuit board. Module transceivers are external to the network and are installed and function similarly to other computer peripherals, or they can function as standalone devices.

1. **Firewalls**

A *firewall* is a networking device, either hardware or software-based, that controls access to your organization’s network. This controlled access is designed to protect data and resources from an outside threat. To do this, firewalls are typically placed at entry/exit points of a network-for example, placing a firewall between an internal network and the Internet. Once there, it can control access in and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network, for example, placing a firewall between the Accounts and the Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through network operating systems (NOS) such as Linux/UNIX, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or permit certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and configured to control traffic. Many third-party firewalls are available.

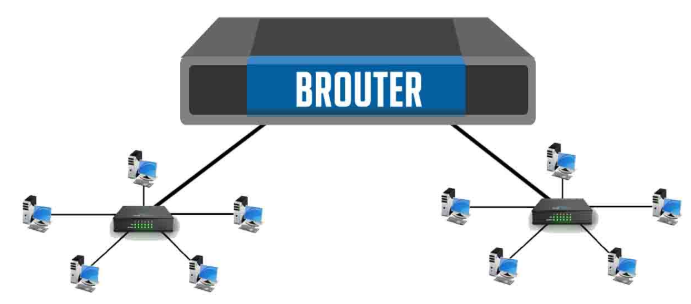
Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with very little configuration and protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built-in. In such a case, the router or WAP might have a number of ports available to plug systems in to.

1. **Brouters**

**Brouter** in networking is a combination of a **Bridge** and a **Router**, hence it is called as a Brouter. It provides functions of a **bridge and a router** so it can operate at the data link and network layers of the **OSI Model**. Brouter connects networks that use different **protocols**. It can be programmed to work only as a bridge or only as a router. When it is configured as a bridge, it forwards data packets to the appropriate segment using a specific protocol. When it is configured as a router, it routes the data packets to the appropriate network using a routed protocol such as **IP**.

Brouters in networking are pretty rare. Instead, most brouters are simply routers that have been configured to also function as a bridge. The main function of a bridge is to connect two different **LAN** segments using the same protocol. A router, on the other hand, used to route the packets in a network.

The diagram below shows two networks making the use of a brouter.



*Figure 14: Two networks making use of a brouter.*

### **Advantages of Brouter in Networking**

1. It works on Both LAN and WAN
2. NAT can be configured which hides the real IP Address of your internal network.
3. Supports packet filtering.
4. Uses packet switching.
5. Can be used to separate a LAN into segments.
6. Allows you to set the best path for data packets.
7. Reduce network traffic.

### **Disadvantages of Brouter in Networking**

1. It is more expensive then hub switch and router.
2. It is complex to manage.

**Wireless Network Components**

1. **Wireless Access Points**

Wireless access points (WAPs) are a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). WAPs are typically a separate network device with a built-in antenna, transmitter, and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. WAPs also typically have several ports allowing a way to expand the network to support additional clients.

Depending on the size of the network, one or more WAPs might be required. Additional WAPs are used to allow access to more wireless clients and to expand the range of the wireless network. Each WAP is limited by a transmissions range—the distance a client can be from a WAP and still get a useable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the WAP.

Note: The region within which wireless devices can access network resources through a wireless access point is called a hotspot.

1. **The PCMIA (Personal Computer Memory Card International Association) card**

This is a special wireless interface card that enables a computing device to access wireless networks. It is important to have the right driver for the device on the computer in order to enable the wireless functionality.

**CHAPTER 4: NETWORKING SOFTWARE**

Networking software enables a network to function correctly. The most common networking software can be divided into three categories:

1. Networking protocols
2. Routing software/protocols/algorithms
3. Network operating systems

Networking protocols govern how data is communicated from one node to the next, while routing software determines the strategy of moving data from one point to the next on the network.

The International Standards Organization (ISO) has developed a framework that acts as a guideline to protocol developers called the ISO-OSI reference model. OSI is an acronym for Open Systems Interconnection. The OSI standard enables protocol developers to come up with software that meets a particular standard, and that can interoperate across a wide spectrum of platforms.

Large internetworks need protocols that allow systems to be identified by the address of the network to which they are attached, and by an address that uniquely identifies them on that network. Network protocols that provide these features are said to be routable. Examples of these routable protocols include:

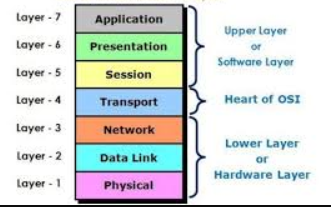
1. TCP/IP – Transmission Control Protocol/Internet Protocol
2. IPX/SPX - Internetwork Packet Exchange/Sequenced Packet Exchange
3. Apple Talk

**The OSI Reference Model**

The acronym OSI stands for Open Systems Interconnection and it refers to a seven layer architecture for networks. The architecture which was defined by the International Standards Organization (ISO) seeks to define a blueprint within which network and internetworking protocols should be designed and developed.

Each layer of the OSI reference model is characterized by a set of standard protocols that perform a particular function and behave in a particular way.

The table below shows the seven layers of the OSI reference model and the functions that each layer plays for successful transmission of data in the network from source node to the destination node.

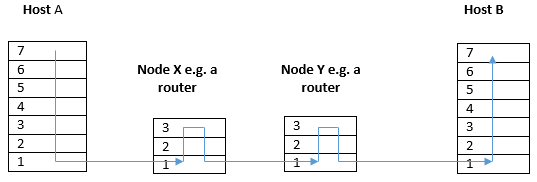


*Figure 15: The seven layers of the OSI reference model.*

|  |  |  |  |
| --- | --- | --- | --- |
| Layer | Name | Data Unit | Function |
| 7. | Application | Message | Adds meaning to the presentation layer data and represents it in a way that can be understood by humans. |
| 6. | Presentation | Message | Comes up with a context specific binary representation of application data. |
| 5. | Session | Message | Negotiation of the establishment and termination of sessions/connections. |
| 4. | Transport | Message | Ensures efficient and cost effective transportation of data across the network. |
| 3. | Network | Packet | Routing of data packets within the network and inter-network. |
| 2. | Data-link | Frame | Provision of a reliable communication line to the network layer. |
| 1. | Physical | Bit | The physical layer deals with transmission of raw data bits over communication lines. |

The seven layers represent the protocol architecture for the communications components of the host. The sending and receiving nodes will normally work with all the seven layers of the OSI reference model but the intermediate nodes only need the first three layers to route data across the network.

The figure below shows the transmission of data from Host A to Host B via two intermediary nodes, X and Y.



When computer A sends a message to computer B, the message moves down the successive layers of A from the application layer to the physical layer and then it is forwarded to the next node on the network along the route. The intermediate nodes X and Y do not need to utilize all the seven layers because they are simply routing the message to the destination and therefore utilize only up to layer three (the network layer).

When the message reaches the destination, it is received through the physical layer and it goes up the successive layers to the application layer where it can be received by the recipient.

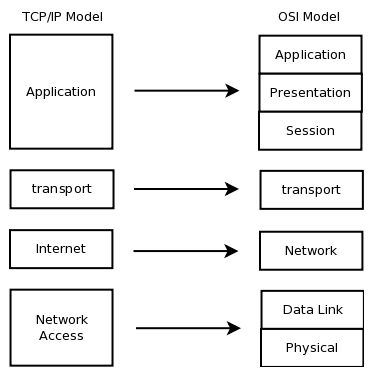
For the data to move across the network, each layer must perform its function. The layers perform this by prefixing a header on the message/data that originates from the application layer. The header has special control and communication instruction that determines how the data should be treated by the other layers on the network and how the receiving computer should interpret the received message until it finally extracts the data.

**The TCP/IP Model**

Just like the OSI reference model, the TCP/IP model is an open standard networking model. They are both very similar. However, the latter (TCP/IP model) has found more acceptance today and the TCP/IP protocol suite is more commonly used. Just like the OSI reference model, the TCP/IP model takes a layered approach.

The TCP/IP model is a condensed version of the OSI reference model consisting of the following 4 layers:

* Application Layer
* Transport Layer
* Internet Layer
* Network Access Layer



1. **Application Layer**

 The Application Layer of the TCP/IP Model consists of various protocols that perform all the functions of the OSI model’s Application, Presentation and Session layers. This includes interaction with the application, data translation and encoding, dialogue control and communication coordination between systems.

1. **Transport Layer**

The Application layer protocols take the user data and add a header and pass it down to the transport layer to be sent across the network to the destination. The TCP/IP transport layer’s function is same as the OSI layer’s transport layer. It is concerned with end-to-end transportation of data and setups up a logical connection between the hosts. The most common protocols in this layer are the TCP and UDP protocols.

1. **Internet Layer**

Once TCP and UDP have segmented the data and have added their headers, they send the segment down to the Network layer. The destination host may reside in a different network far from the host divided by multiple routers. It is the task of the Internet Layer to ensure that the segment is moved across the networks to the destination network.

 The Internet layer of the TCP/IP model corresponds to the Network layer of the OSI reference model in function. It provides logical addressing, path determination and forwarding.

1. **Network Access Layer**

The Network Access layer of the TCP/IP model corresponds with the Data Link and Physical layers of the OSI reference model. It defines the protocols and hardware required to connect a host to a physical network and to deliver data across it. Packets from the Internet layer are sent down the Network Access layer for delivery within the physical network. The destination can be another host in the network, itself, or a router for further forwarding. So the Internet layer has a view of the entire Internetwork whereas the Network Access layer is limited to the physical layer boundary that is often defined by a layer 3 device such as a router.

The Network Access layer consists of a large number of protocols. When the physical network is a LAN, **Ethernet** at its many variations are the most common protocols used. On the other hand when the physical network is a WAN, protocols such as the **Point-to-Point Protocol (PPP)** and **Frame Relay** are common.

**Note**: Network Access layer uses a physical address to identify hosts and to deliver data.

* The Network Access layer PDU is called a **frame**. It contains the IP packet as well as a protocol header and trailer from this layer.
* The Network Access layer header and trailer are only relevant in the physical network. When a router receives a frame, it strips of the header and trailer and adds a new header and trailer before sending it out the next physical network towards the destination.

**Network Operating Systems**

Unlike other operating systems, such as Windows, which are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network.

In most cases, both the client/server and peer-to-peer networking models use network operating systems, and as such, NOSs must be able to handle typical network duties such as the following:

1. Providing access to remote printers, managing which users are using which printers when, managing how print jobs are queued, and recognizing when devices aren't available to the network.
2. Enabling and managing access to files on remote systems, and determining who can access what—and who can't.
3. Granting access to remote applications and resources, such as the Internet, and making those resources seem like local resources to the user (the network is ideally transparent to the user).
4. Providing routing services, including support for major networking protocols, so that the operating system knows what data to send where.
5. Monitoring the system and security, so as to provide proper security against viruses, hackers, and data corruption.
6. Providing basic network administration utilities (such as SNMP, or Simple Network Management Protocol), enabling an administrator to perform tasks involving managing network resources and users.

**Examples of Network Operating Systems include: Unix/Linux, Netware, Windows Server and** MAC OS X Server.

**Routing Algorithms**

The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on so that it can eventually reach its destination node.

**Properties of Routing Algorithm**:

1. ***Correctness*** – The routing of data should be done properly so that each packet reaches its correct destination.
2. ***Simplicity*** - The routing should be done in a simple manner so as to reduce the cost of transmitting data. Increasing the complexity of the routing algorithm often increases the cost of data transmission.
3. ***Robustness*** - The routing algorithm should be able to continue functioning even in the event of failures such as hardware and software failures. It should be able to recalculate a different route for the data when the original route becomes impossible as a result of failures or congestion.
4. ***Stability*** – The routing algorithm should be stable under all conditions and should able to find a routing table quickly.
5. ***Fairness*** – All the nodes on the network should get a fair chance of transmitting their data whenever need arises.
6. ***Optimality*** – An algorithm which is optimal aims at increasing the throughput of the network while at the same time reducing mean packet delay. Often, the number of hops is used as a metric to be minimized since it relates to both throughput and mean packet delay.

**Categories of Routing Algorithms**

Routing algorithms can be grouped into two major classes:

1. ***Non-adaptive routing algorithms***

Non-adaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, off-line, and downloaded to the routers when the network is booted. This procedure is sometimes called Static routing. Non-adaptive algorithms are suitable for situations where:

1. The network is small.
2. There is only one route/path to a resource.
3. When the network design is relatively simple.

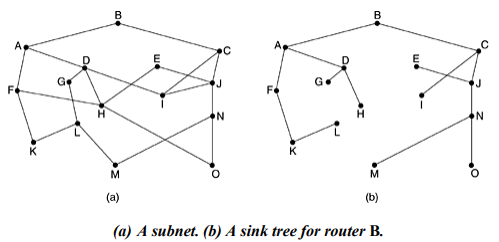
The downfalls of these types of algorithms include: difficulties in the scalability of the network, high administrative overheads, and the fact that these types of algorithms do not react to changes in a network such as congestion in a given route or hardware and software failures.

1. ***Adaptive routing algorithms***

Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well. This procedure is sometimes called dynamic routing.

**The Optimality Principle**

If router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.



As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a **sink tree** where the distance metric is the number of hops. Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist. The goal of all routing algorithms is to discover and use the sink trees for all routers.

**Examples of routing algorithms**

1. Distance-vector routing algorithms.
2. Link state routing algorithms.
3. Path-vector routing algorithms.

Distance vector routing algorithms require that each node exchanges [information](http://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) between neighbors, that is to say between nodes directly connected. Therefore, each node can keep updating its table by adding information on all its neighbors. This table shows the distance of each node and each network to be reached. First to be implemented in the Arpanet, this technique quickly becomes cumbersome when the number of nodes increases since we must carry a lot of information node to node. RIP (Routing Information Protocol) is the best example of a protocol using distance vector.

In this type of algorithm, each router broadcasts to its neighbors a vector that lists each network it can reach and the metric associated with it, that is to say the  number of hops. Each router can therefore build a routing table with information received from its neighbors but has no idea of ​​the identity of the routers that are on the selected route. Therefore, the use of this solution poses numerous problems for external routing protocols. Indeed, it is assumed that all routers use the same metric, which may not be the case between autonomous systems. Furthermore, an autonomous system can have special reasons to behave differently from another autonomous system. In particular, if an autonomous system needs to determine how else autonomous system will pass its messages, e.g. for security reasons, it cannot know.

The link state algorithms had initially intended to overcome the shortcomings of distance vector routing. When a router is initialized, it must define the cost of each of its links connected to another node. The node then broadcasts the information to all nodes in the autonomous system, and therefore not only to its neighbors. From all this information, the nodes can perform their calculation for obtaining a routing table indicating the cost of achieving each destination. When a router receives information that alters its routing table, it notifies all intervening routers in its configuration. As each node has the network topology and costs of each link, routing can be seen as central in each node. OSPF (Open Shortest Path First) implements this technique, which is the second generation of Internet protocols.

The link state algorithms solves the problems mentioned above for external routing but raise other. The various autonomous systems may have different metrics and specific restrictions, so it is not possible to achieve a coherent route. The dissemination of all information necessary for all the autonomous systems can also quickly become unmanageable.

The purpose of the path-vector algorithms is to overcome the shortcomings of the first two categories by providing metrics and seeking to know which network can be reached by any node and autonomous systems which must be crossed for it. This approach is very different from that of distance-vector algorithms because the paths vectors do not take into account the distances or costs. In addition, the fact that each list routing information all autonomous systems that must be traversed to reach the destination router, the path vector approach is much more directed towards the external routing systems. BGP (Border Gateway Protocol) belongs to this category.

**Networking protocols**

Networking protocols are rules that govern communication in computer networks. The table below shows some internet applications and their supporting protocols.

|  |  |  |  |
| --- | --- | --- | --- |
| S.NO. | Application | Application Layer Protocol | Transport layer Protocol |
| 1. | Email | SMTP | TCP |
| 2. | Remote Terminal Access | Telnet | TCP |
| 3. | Web | HTTP | TCP |
| 4. | File Transfer | FTP | TCP |
| 5. | Telephony | SIP (Session Initiation protocol) | UDP |

**Assignment**

Identify the protocols and networking/inter-networking devices used in each of the seven layers of the OSI reference model. These should be presented in a table similar to the one shown below. The networking protocols can be described below the table. A description of the networking/inter-networking devices is not required because we have covered them in class and lecture notes on the same have been provided.

|  |  |  |  |
| --- | --- | --- | --- |
| S.NO | OSI Reference Layer | Networking/inter-networking protocols | Networking/inter-networking Devices |
| 7. | Application |  |  |
| 6. | Presentation |  |  |
| 5. | Session |  |  |
| 4. | Transport |  |  |
| 3. | Network |  |  |
| 2. | Data-link |  |  |
| 1. | Physical |  |  |

**CHAPTER 5: TRANSMISSION MEDIA**

Communication cannot happen without the appropriate transmission media. There are two types of transmission media:

1. ***Bounded/physical transmission media***

This type of media links communicating devices using physical links and the data signal is forced to move through the medium from source to destination through a restricted path. Examples of bounded transmission media include fiber optic cables, twisted pair cables, and coaxial cables.

In order of increasing performance, cost, efficiency, and transmission speeds [possible as each upgrade attempts to improve on the shortcomings of the former]:

UTP – STP – Coaxial cables – Fiber optic cables

1. ***Unbounded/wireless transmission***

In this category of transmission, the data signal is allowed to travel freely through unrestricted paths from source to destination. This is sometimes called wireless transmission. Examples of unbounded transmission media include microwaves and radio waves.

**Bounded Transmission Media**

The cable is the medium through which information usually moves from one network device to another. This device is commonly used with LANs.

1. **Twisted Pair Cables**

Twisted cables exist in pairs with 4 pairs coupled together to form a single jacket.

A twisted pair cable is made up of two copper strands which are insulated and twisted around one another in a helix fashion. The twisting of the cables is meant to reduce interference called cross talk between the cables to support a greater propagation speed. Twisted pair cables have been the mainstream backbone cables for a long time over long distances but they are now being aged out through the introduction of fiber optic backbones.

A less twisted cable is cheaper to acquire. But, more twists imply faster speeds over longer distances as interference reduce the strength and speed of the signal to be transmitted.

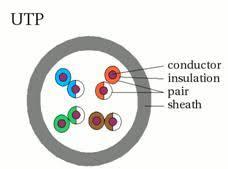
Twisted pair cables can be divided into two categories:

1. **Unshielded twisted pair cable (UTP)**

These cables do not have a shield around them, which would protect them from electromagnetic interference, hence are susceptible to environmental noise. Sources of these environmental noises include power lines. Because of this reason, UTP cables are not suitable for use in electrically noisy places.

[UTP Image - <https://prnt.sc/up8nsz>]

[Connecting a UTP cable - <https://prnt.sc/up8x4e>]



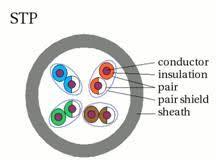
*Figure 16: Parts of unshielded twisted pair cable.*

1. **Shielded twisted pair cables (STP)**

These cables have a foil around them, which protects them from electromagnetic interference noise. The foil is usually aluminum-based. For this reason, STP cables are more resistant to environmental electromagnetic interference radiation.

They can also help extend the maximum distance of the cables.

[3 different configurations of STP - <https://prnt.sc/up8z36>]



*Figure 17: Parts of a shielded twisted pair cable.*

Twisted pair cables are classified into six categories, as below:

[cat is a short form for category]

Cat 1 – voice

Cat 2 – voice and data

Cat 3 –

Cat 4 – 10mbps

Cat 5 – 100mbps

Cat 5e – 1gbps

Cat 6 – 10gbps

**Terminating UTP Cables**

For a cable to be able to connect a computer to a networking device like a switch, it needs to be terminated. The international standard for terminating Cat 5 and above is the RJ45 connector plug.



***Figure 18: A twisted pair cable terminated using RJ45 connector plugs***

**Advantages of Twisted Pair Cables**

1. The cable is readily available in the market.
2. The cable is cheap.
3. The cable is easy to work with since it is not heavy.
4. Since the bulk of telecommunication back bones run on twisted pair cables, it is easy to create connections across different regions easily.

**Disadvantages**

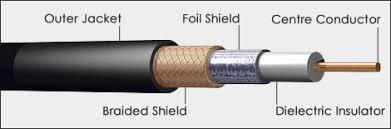
1. They suffer from higher attenuation. UTP has an attenuation distance of 90 meters.
2. UTP cables are sensitive to electromagnetic interference.
3. UTP suffers security problems, since it is susceptible to attacks such as eaves dropping.
4. **Coaxial Cables**

Unlike twisted pair cables that are many in number, a coaxial cable has a single copper conductor at the core, surrounded by dielectric insulators and an earthed wire mesh. The dielectric material protects the cable from electromagnetic interference, and the wire mesh grams any noise signals received from external sources. Coaxial cables have bandwidth of up to 1gbps and have longer attenuation distance that UTP cables. There attenuation distance ranges between 150-200 meters.

Coaxial cables used to be the cable of choice when laying network backbones between two busy points, but they have been literally pushed out into obsolesce with the emergence of fibre optic cables.

[2 types of coaxial cables - <https://prnt.sc/up96fb>]

[Connecting a coaxial cable - <https://prnt.sc/up96y5>]



*Figure 19: The various parts of a coaxial cable.*



*Figure 20: An example of a complete coaxial cable.*

***Advantages of Coaxial Cables***

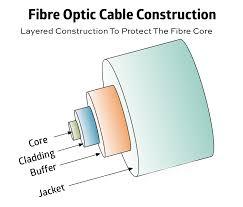
1. They have a higher bandwidth when compared to UTP cables.
2. Their resistance to electromagnetic interference is better than that of UTP cables – higher signal strength upon arrival.
3. Better quality of service in the transmission channel.
4. It allows high transfer rates with coaxial cable having better shielding materials.
5. Support greater cable lengths between network devices than TP cables – implying a signal can move over longer distances without losing its strength
6. Thick coaxial cables have an extra plastic protective cover that keeps moisture away from the center conductor

***Disadvantages of Coaxial Cables***

1. They are slightly more expensive that UTP cables.
2. They are difficult to work with because it is bulky.
3. It is expensive to install for longer distances due to its thickness and stiffness, especially for thick coaxial cables.
4. As a single cable is used for signal transmission across the entire network, in case of failure in one cable the entire network will be down.
5. The security is a great concern as it is easy to tap the coaxial cable by breaking it and inserting T-joint (of BNC type) in between.
6. It must be grounded to prevent interference.

1. **Fibre Optic Cables**

The fibre optic cables transmit data using light rather than electrical signals. The cable is made up of center core, made up of glass or plastic. The center core is surrounded by an outer cover, which is also transparent but has a high refractive index. The cladding is then protected by an outer cover. The cable transmits light through the principle of total internal reflection, which is caused by the refraction of light at the core at the boundary of the core and the cladding. Fibre optic cables disapprove the idea that light travels in a straight line.



*Figure 21: The basic parts of a fiber optic cable*

There are two types of fibre optic cables as outlines below:

1. ***The single mode fibre optic cable***

This type of fibre optic cable has a very thin core. It allows only one ray of light to be fed into the cable. The advantages of the single mode fibre is that it has a higher bandwidth and a longer attenuation distance (40-120 km) than the multimode fibre.

1. ***The multimode fibre optic cable***

It has a thicker inner core, and allows more than one ray of light to be fed into the cable. As a result, it has a shorter attenuation distance of between 5km-15km when compared to the single mode fibre optic cable.

[Categories of fiber optic cables - <https://prnt.sc/up9hhr>]

**Advantages of Fiber Optic Cables**

1. Vastly faster than TP and coaxial cables
2. Light signals do not experience electrical interference, meaning it is ideal for environments experiencing consistent electrical interference.
3. Immune to moisture & lightning, hence, can connect networks between buildings
4. Larger propagation distances.

**Disadvantages of Fiber Optic Cables**

1. Difficult to install and modify
2. Costly

**Attenuation**

Attenuation refers to the loss of signal power as it travels through the transmission medium. For the signal to move from source to destination, repeater stations need to be deployed just before the attenuation point, so that they can receive the weak signal, clean it from deformities, amplify it and resend it down the transmission medium to the next node on the network. The more the repeaters, the more expensive the network will be.

[Installing Guidelines for cables –-<https://prnt.sc/up9j9b> ; <https://prnt.sc/up9k9y>]

**Unbounded Transmission Media**

These refer to electromagnetic waves that are used to transmit data without physically linking the two communicating points. Electromagnetic waves have infinite energy and they travel through space, vacuum, etc, infinitely.

There are several media on the electromagnetic spectrum, and the main ones are radio waves, microwaves and infrared waves.

1. **Radio waves**

Radio waves are omnidirectional in nature, and are of several types as explained below:

1. **The high frequency waves**

Communication by this means involves targeting the earth’s ionosphere with the waves, which are then reflected back to earth. This used to be the only form of beyond the horizon communication in the olden days. These high frequency waves are only used in cases of dire need.

1. **Very high frequency waves**

These ones are mainly used for TV and Radio transmissions, and data transmission through MODEMS. This kind of communication relies on the line of sight principle, meaning that there must be no obstruction between the sender and the receiver. Where there is an obstruction, then repeater stations need to be constructed to create a chain of lines of sight from the source to destination.

1. **Ultra-high frequency waves**

These have smaller wavelength than the very high frequency waves. They are common in radio and TV transmission especially in cosmopolitan regions.

1. **Bluetooth**

This is a short range radio transmission, used to interconnect personal devices like telephones, tablets and laptops, in a radius of around 300 meters.

1. **Microwave transmission**

Microwaves are unidirectional in nature. They are used in satellite communication and terrestrial microwave communication systems like WiMAX (an advanced form of WI-FI which covers longer distances).

1. **Infrared Waves**

These can be used to interconnect devices within short distances, maintaining a line of sight between them. Examples of applications of infrared is the TV remote. Infrared can also be used to connect phones which are infrared enabled, can also connect a computer to a printer so long as they are infrared enabled. Infrared waves have also been used in the army to make infrared goggles that have night vision. It is important to note that while blue tooth can penetrate barriers, infrared waves cannot.