

COMPUTER NETWORKS

ICS 2306: Computer Networks

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

Chapter 1: Introduction/Overview

1.1. Content:

- i. Topology and architecture of computer networks.
- ii. Layered protocols.
- iii. OSI and TCP/IP protocols. Local area networks.
- iv. Wide area networks. Routing protocols. Gatewaying.

1.2 Course Objectives

- i. Understand the basic principles of data communication and computer networks
- ii. Appreciate the complex trade-offs that are inherent in the design of networks
- iii. Provide a guided tour of network technologies from the lowest levels of data transmission up to network applications
- iv. Learn about current network technologies especially Internet protocols

1.3 Recommended texts

- i. Computer Networks and Internets by Douglas E. Comer, Prentice Hall 2nd ed or higher
- ii. Tannenbaum, Computer Networks, Prentice Hall
- iii. Halsall, Data and Computer Communications, Macmillan
- iv. Supplementary texts

1.4 What is a computer network?

An interconnection of autonomous computers that communicate via a hierarchy of protocols (as opposed to communication between separate but interdependent parts of a single computer).

1.5 Some goals of computer networks

- Access to remote resources - sharing reduces cost implications.
- Human communication - e.g. email has made work a lot easier.
- Mobile computing – which is the ability to connect portable devices to wireless-enabled networks to access data and services while on the move.
- Computing power through parallelism – which is the process where large compute problems are broken down into smaller problems that can be solved simultaneously by multiple processors.
- Optimizing resources – load balancing via proper scheduling of jobs/processes.
- Incremental growth of computer systems (reduced cost and risk) – enhancements to meet increasing computing demands.

- Increased robustness through graceful degradation – the ability of a system or network to maintain limited functionality even when a large portion of it has been destroyed or rendered inoperative.

1.6 Uses of computer networks

- Email
- WWW
- Video conferencing
- File transfer
- Collaborative virtual environment
- Remote control of robots and machines
- Dial up databases
- Webcasting
- Distributed programs
- Hacking
- Banking
- Internet telephone etc.

1.7 Classifying networks

- By size – LANs vs. WANs
- By connectivity – p2p (peer to peer) vs. broadcast networks (a type of network where a machine can send data to all other machines within the network simultaneously)
- By communication medium – wire, fiber etc.
- By mobility – fixed vs. mobile

1.7.1 Size – differences between local and wide area networks

- Speed – bandwidth and latency
- Management – which is the sum total of applications, tools and processes used to provision, operate, maintain, administer and secure network infrastructure.
- Security - which is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.
- Reliability - the measure of the length of time infrastructure operates without disruption.
- Billing - processes of communications service providers that are responsible to collect consumption data, calculate charging and billing information, produce bills to customers, process their payments and manage debt collection.
- Heterogeneity - platform where devices and operating systems are different, and
- Standards – define how communication occurs during transmission and between devices.

1.7.2 Connectivity – p2p networks

- Star
- Tree
- Irregular
- Mesh

1.7.3 Connectivity – broadcast networks

- i. Satellite/radio
- ii. Wire etc.

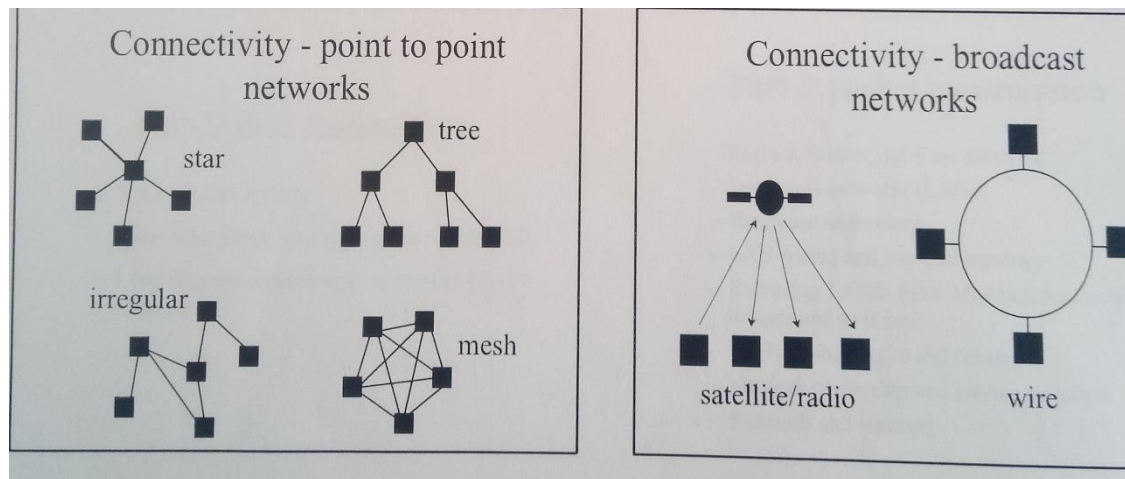


Fig. 1.1: Two major types of Networks: P2P and Broadcast.

1.7.4 Medium – differences between communication media

- i. Speed – considers bandwidth and latency.
- ii. Range – defines the area covered.
- iii. Sharing – media access protocols coordination on the use of a shared resource by multiple host.
- iv. Topology – the architecture.
- v. Installation and maintenance costs – implications (feasibility aspect).
- vi. Reliability – proper functioning of a system with minimal probability of failure.

1.7.4 Mobility – issues arising in mobile networks

Mobile networking has emerged in the last years. Introduces new issues of:

- i. Location and tracking e.g. for fixed and mobile computing.
- ii. Semi-persistent connections – non-permanent connections.
- iii. Complex administration and billing as devices and users move around the network.

1.8 Common issues in networking

- i. Addressing - assigning unique identifiers to each device on a network.
- ii. Routing - selecting a path across one or more networks.
- iii. Framing (unit of transmission) and decoding (converting encoded format back to its original characters).
- iv. Error detection and correction – errors that occur must be corrected/handled appropriately.
- v. Flow and congestion – to minimize e.g. lost data and delays.

Chapter 2: Data Transmission

2.1 Transmission media

All computer communication involves encoding data in a form of energy and sending the energy across a transmission medium. Examples include electric current transferring data across wire and radio waves through the air. Some of the common media include the following hereunder.

2.2 Copper wire

It is the primary medium to connect computers since it is inexpensive and easy to install. Its low resistance allows signals to travel farther. The wiring style is chosen to minimize interference that arises due to electrical signal travelling across a wire i.e. the wire emits some electromagnetic energy that travels through the air and when it meets the effect of another wire, some electric current is generated in the wire. This is worse for wires running in parallel. Such generated current may be strong enough to prevent normal communication.

Networks therefore use two types of wiring schemes to minimize interference: Twisted Pair (TP) and Coaxial.

2.2.1 Twisted pair – also used in telephone. Each wire is coated with an insulating material and twisted together. Such twists change the electrical properties of the wire making it suitable for use because the twists help prevent electric currents on the wire from radiating energy that interfere with other wires and they also prevent signals in other wires from interfering with the pair.



Fig. 2.1 Twisted pair cable

2.2.2 Coaxial cable – provides more protection from interference than twisted pair. The metal shield (heavier) provides a barrier to electromagnetic radiation. Copper mesh is the metal shield.



Fig 2.2: Coaxial cable

The inner wire transmits and the outer wire returns. It provides more protection from interference than twisted pair. The metal shield (heavier) provides a barrier to electromagnetic radiation in both directions. There are also shielded twisted pair. Such shielded wiring is often used when wires from a network pass near equipment that generates strong electric or magnetic fields e.g. a large air conditioner.

Benefits of Copper Ethernet Cables

- Lower cost: Cheaper, making them a good choice for companies on a limited budget.
- Installation: Easier to install, test and maintain.
- Flexibility: Available in various configurations, lengths, and colours.

2.3 Glass fibers (optical fiber)

It uses light to transmit data. A miniature glass fiber is encased in a plastic jacket allowing the fiber to bend without breaking. A transmitter at one end of the fiber uses a light emitting diode (LED) or a laser to send pulses of light down the fiber while a receiver at the other end uses a light sensitive transistor to detect the pulses.

Advantages over wires include

- Because they use light, they neither cause electrical interference in other cables nor are they susceptible to the same.
- They carry light pulses farther since they can reflect most of the light inward.
- They carry more information than wire since light encodes more information than electric current.
- Light can travel over a single fiber unlike in case of wires which have to be in pairs for a complete electric circuit.

Disadvantages:

- Installing fiber requires special equipment that polishes the ends to allow light to pass through (expensive)
- If a fiber breaks inside the jacket, finding the location of the problem is difficult.
- Repairing a broken fiber is difficult since it requires special equipment to join two fibers so that light can pass through the joint (expensive).

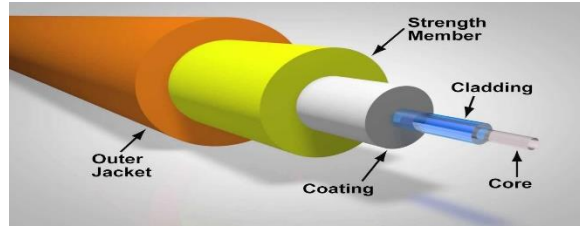


Fig. 2.3: Optic Fiber

2.4 Radio

Such electromagnetic radiation can be used to transmit computer data. Such networks are said to operate at *radio frequency* commonly referred to as RF transmissions. They do not require a direct physical connection between computers, but each participating computer attaches to an antenna that both transmits and receives RF. Small antennas are enough for shorter distances e.g. 20cm while up to 2m may be required for across city communication.

2.5 Satellites

Radio transmissions do not bend around the surfaces of the earth but RF technology combined with satellites provides communication across longer distances (*See fig 1.3 below*). The satellite contains a transponder that consists of a radio transmitter/receiver. The transponder receives a signal, amplifies it and sends it back in another direction. One satellite normally contains multiple transponders, between 6 to 12 operating independently, and each transponder uses a different frequency (channel) thus making multiple communication to be possible simultaneously. This is because satellites are very expensive. The different forms of satellites, grouped by height at which they orbit include:

2.5.1 Geosynchronous Satellites

They are also called geostationary, are placed in an orbit that is exactly synchronized with the earth's rotation i.e. satellite remains exactly at the same position at all times. The height is normally approximately 36,000 km (20,000 miles) and this distance is usually determined by the laws of Physics. The angular separation of the satellites is normally 4 – 8 degrees depending on the power of the transmitter implying that 45 – 90 satellites e.g. on the Equator (360 degrees). Such satellites can be used to relay transmissions at all times since it stays at the same spot throughout.

2.5.2 Low Earth Orbit Satellites (LEO)

They are placed at approximately 200 – 400 miles above the earth's surface. They do not stay stationary since their period of rotation is faster than that of the earth, and this is their disadvantage. They can cover an entire orbit in 1.5 hours. Two problems are hereby implied: such satellites can only be used when its orbit passes between two ground stations, and, optimum utilization requires complex control systems that continuously move the ground stations so that they point directly at the satellite.

2.5.3 Low Earth Orbit Satellite Arrays

They are a set of satellite arrays in low earth orbit. Even though they orbit quickly, the set is chosen such that each point on the ground has at least one satellite overhead at any time (66

satellites are adequate for the entire earth's surface). In addition to transponders, they also have radio equipment to communicate with each other in the array to help in forwarding information.

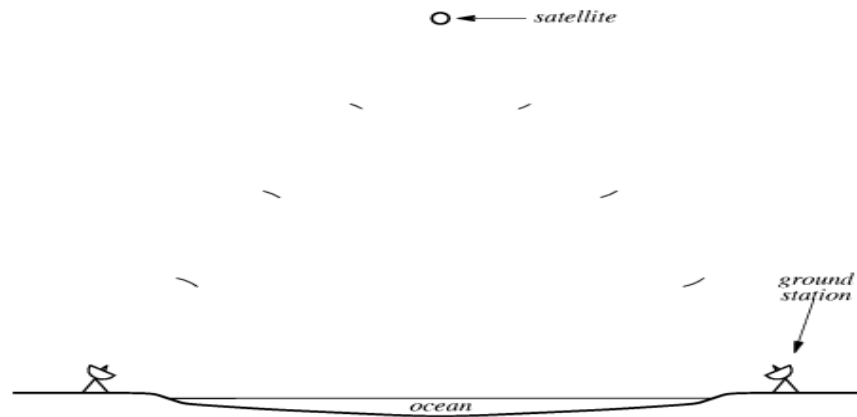


Fig. 2.4: Satellite used to provide communication across an ocean. The satellite receives radio signals from one ground station, and transmits them to another.

2.6 Microwave

They are electromagnetic radiation beyond the frequency range used for radio and tv (wavelength ranging from 1m to as short as 1mm implying frequencies between 300MHz to 300GHz, includes UHF and EHF millimeter waves) and are used mainly by long-distance telephone companies. Their transmissions can be aimed in a single direction thus preventing others from intercepting the signal. They carry more information than lower frequency RF transmissions. They require a clear path between the transmitter and the receiver since they cannot penetrate metal structures. They also require mounting of two towers each aimed directly at the other i.e. transmitter aimed at receiver.

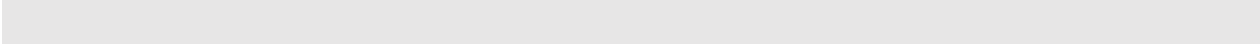
2.7 Infrared

They are electromagnetic radiation with longer wavelengths than those of visible light – frequency range of 430THz to 300GHz and are used in industrial, scientific and medical applications e.g. night vision devices. They are the wireless remote controls used with appliances such as TV and stereos. They are limited to a small area e.g. single room and require the transmitter to point at the receiver. They are comparatively inexpensive and require no antennas. A room equipped with a single infrared connection can provide network access to all computers in the room.

2.8 Light from a LASER

Light Amplification by Stimulated Emission of Radiation (LASER) are used in common consumer devices e.g. DVD players, laser printers, barcode scanners, laser surgery in medicine,

various skin treatments in the industry for cutting/welding, in military for marking targets, and measuring range and speed. It is a beam of light that carries data through the air and requires two sites to have a transmitter and a receiver fixed on a tower. The transmitter uses a laser to generate a beam of light because a coherent laser beam stays focused over a long distance. The disadvantage is that it cannot penetrate vegetation or snow or fog and so has limited use. It must travel in a straight line and must not be blocked.



Chapter 3: Local Asynchronous Communication (RS-232)

3.1 The need for asynchronous communication

Communication is called asynchronous if the sender and receiver do not need to coordinate before data is transmitted i.e. sender and receiver do not synchronize before each transmission. Sender transmits data whenever it is available and receiver accepts data whenever it arrives. This is useful for devices e.g. keyboards where data is generated when keyboard is touched and no data flows when keyboard is idle.

3.2 Using electric current to send bits

Simplest electronic communication systems use a small electric current to encode data over electric wire e.g. negative voltage may represent 1 and positive 0. When a sender transmits a +ve voltage, receiver records 0 and vice versa. (See fig 3.1 below)

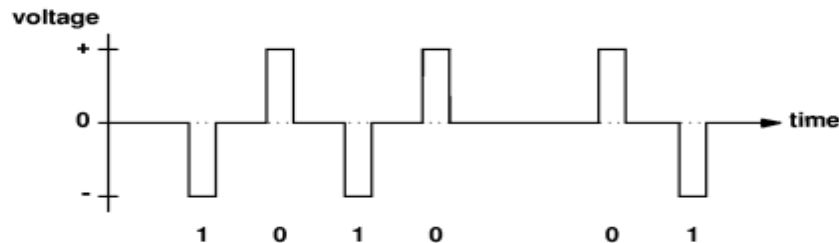


Fig. 3.1 Waveform diagram

NB: Notice the delay between the 4th and 5th bits.

3.3 Standards for communication

Specifications for communication systems are standardized. International Telecommunications Union (ITU), Electronic Industries Association (EIA) and the IEEE publish specifications in documents known as standards. A standard specifies both the timing of signals and the electrical details of voltage and current. The EIA's RS-232-c (i.e. RS-232+) specifies details of physical connection e.g. connections must be <50ft long and voltage of -15 to +15 for data transmission. The RS-232 is designed for use with devices such as modems and terminals, keyboard etc. it specifies the transmission of characters. It can be used to send 8-bit characters but often configured so that each character consists of seven data bits. RS-232 defines serial asynchronous communication (serial because bits travel on the wire one after another) RS-232 never leaves zero volts on the wire i.e. when there is no transmission, it leaves the wire with a -ve voltage => 1.

3.4 Baud rate, Framing and Errors

Baud defines the number of changes in the signal per second that the hardware generates. For RS-232 baud rate = the number of bits per second. Baud rate can be set manually or automatically.

Framing errors are the errors that occur if the stop bit does not occur exactly at the time expected.

The sending and receiving hardware must agree on the length of time the voltage will be held for each bit. Thus technically, transmission hardware is rated in baud. But usually to make RS-232 hardware more general, manufacturers usually design each piece of hardware to operate at a variety of baud rates. The baud rate can then be set either manually using switches in hardware installed in the computer or automatically by device driver software in the computer. After this, the sending and receiving hardware must be configured to use the same baud rate otherwise framing errors occur.

3.5 Full duplex asynchronous communication

All electric circuits require a minimum of two wires for current to flow to and fro. The send wire is often referred to as “ground” e.g. in coaxial, the center wire transmits and the shield provides the return path. Thus, simultaneous transfer in two directions is referred to as full-duplex while single direction is half-duplex or simplex transmission. (See fig 3.2 below)

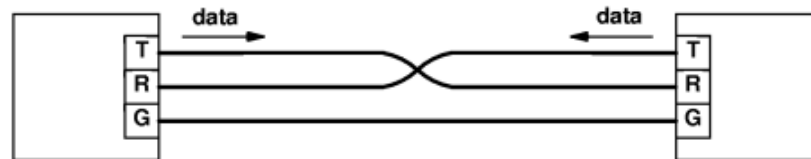


Fig 3.2: A diagram showing minimal wiring required for full-duplex RS-232 communication. Although the two wires carry data independently, it is possible for them to share a single ground wire.

3.6 Limitations of Real Hardware

Note that in practice, no electronic device produces an exact voltage or change from one voltage to another instantly. Also, no wire conducts electricity perfectly i.e. there is energy loss as current travels down the wire. Therefore, it takes a small time for the voltage to rise and fall and the signal received is not perfect (*See fig. 2.3 below*). Thus, standards for RS-232 specify how close to a perfect waveform a transmitter must emit and how tolerant of imperfection a receiver must be.

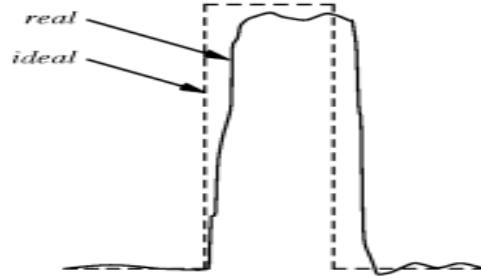


Fig 3.3: An illustration of the voltage emitted by a real device as it transmits a bit. In practice, voltages are often worse than this.

3.7 Hardware bandwidth and the transmission of bits

Defn: Bandwidth – the fastest continuously oscillating signal that can be sent across the hardware.

Each transmission system has a limited bandwidth which is the maximum rate at which the hardware can change a signal. It is measured in cycles per second, Hz.

A fundamental relationship exists between the bandwidth of a transmission system and the maximum number of bits per second that can be transferred over that system. This is Nyquist's sampling theorem (1920) which provides a theoretical bound on the maximum speed at which data can be sent. For RS-232 that uses two values of voltage to encode data, it states that the maximum data rates in bits per second that can be achieved over the transmission system of bandwidth B is $2B$.

Generally, if the transmission system uses K possible values of voltage instead of two, it becomes

$$D = 2B \log_2 K,$$

D = maximum data rates in bits/second.

3.8 Effect of Noise in communication

Real communication systems are subject to small amounts of background interference called "noise" which make it impossible to achieve the theoretical maximum transmission rate. Claude Shannon, (1948), extended Nyquist's theorem as below.

$$C = B \log_2(1 + S/N), \text{ effectively lower than Nyquist's value.}$$

Where,

C = effective limit in b/s	B = hardware bandwidth	S = average signal power
N = average noise power	S/N = signal-noise ratio	

Chapter 4: Long-Distance Communication (Carriers, Modulation and Modems)

4.1 Sending signal across long distances

An electric signal cannot travel arbitrarily far over copper wire since current weakens with distance. This is called signal loss which occurs due to resistance in the wire causing small amounts of electrical energy converted to heat. Thus, long distance communication systems send a continuously oscillating signal, usually a sine wave called a “carrier”. (See fig 4.1 below)

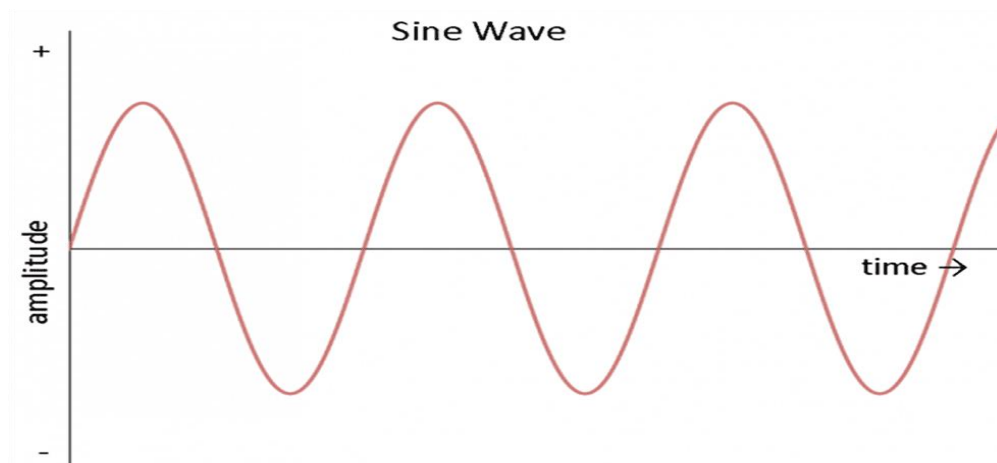


Fig 4.1: Sine wave. The carrier oscillates continuously even when no data is being sent.

To send data, a transmitter modifies the carrier slightly. This is called modulation. E.g. a radio station uses a continuous carrier wave that oscillates at an assigned frequency and uses an audio signal to modulate the wave. Receivers on the other side use it to reconstruct the original audio signal.

Network technologies use a variety of modulation techniques e.g. amplitude or frequency modulation, AM or FM., where AM varies the strength of the outgoing signal in proportion to the information being sent, while FM varies the frequency of the underlying carrier in proportion to the information being sent.

4.2 Modem hardware used for modulation and demodulation

A modem hardware is a device that modulates and demodulates implying that long-distance communication requires a modulator at one end and a demodulator at the other end. This is constructed in one gadget. (See fig 4.2 below).

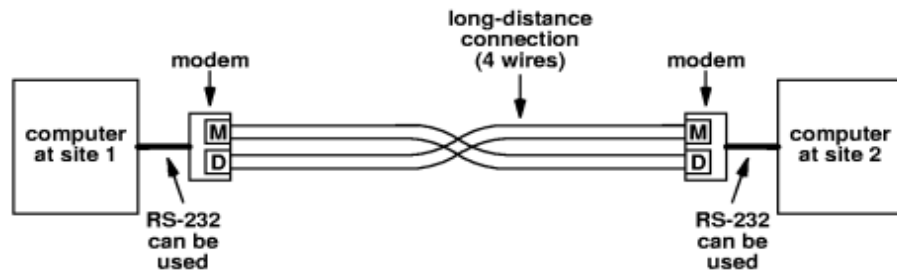


Fig 4.2: Four wires for long distance communication

NB: Users are forced to use leased lines as each cannot single handedly bear the costs i.e. utility companies provide the service to which you subscribe.

4.3 Carrier frequencies and multiplexing

Two or more signals that use different carrier frequencies can be transmitted over a single medium simultaneously without interference. In this case, frequency division multiplexing (FDM) can be applied to mean a network system that uses multiple carrier frequencies to allow independent signals to travel through a medium. It can be used to send signals over a wire, RF or optical fiber. (See fig 4.3 below)

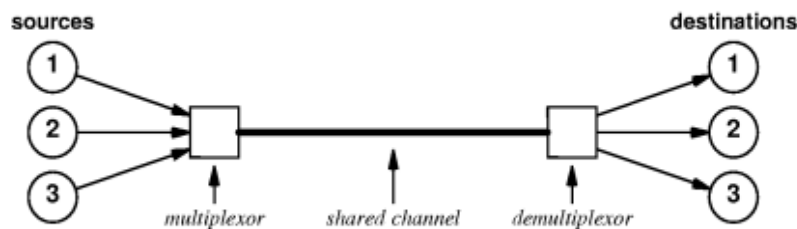


Fig 4.3: The concept of Frequency Division Multiplexing. Each pair of source and destination can send data over the shared channel without interference. In practice, each end requires a multiplexor and demultiplexor for 2-way communication, and a multiplexor may need circuitry to generate the carrier waves.

A minimum separation between carriers is maintained to keep off interference. Thus, FDM is often used only in high-bandwidth transmission systems i.e. systems that can send a wide range of frequencies.

NB: There is also Wave Division Multiplexing (WDM) which operates by sending multiple light waves across a single optical fiber. At the receiving end, an optical prism is used to separate the frequencies. This is possible because light at a given frequency doesn't interfere with light at another frequency.

Time Division Multiplexing (TDM) – the general alternative to FDM in which sources sharing a medium take turns to use a channel.

4.4 Spread spectrum

It is a special case of frequency division multiplexing which involves the use of multiple carriers to improve reliability. Reasons for its use include: to improve reliability when the underlying transmission system has sporadic interference at some frequencies i.e. the transmitter is arranged to send the same signal on a set of frequencies and the receiver configured to check all carrier frequencies and to use whichever is presently working.

Chapter 5: Packets, Frames and Error Detection

5.1 Concept of Packets

Packets are small blocks of data which the network divides and sends individually. Computer networks are often called “packet networks” or “packet switching networks” because they use packet technology. Sender and receiver need to coordinate transmission to ensure data arrives correctly. Multiple computers often share the underlying connections and hardware because the communication circuits and associated modem hardware are expensive. Packets help ensure fairness to every computer in a network over data transmission.

5.2 Packets and Time-Division Multiplexing

Time-division multiplexing is the process whereby a network permits many sources to take turns accessing a shared communication resource. (See fig. 5.1 below).

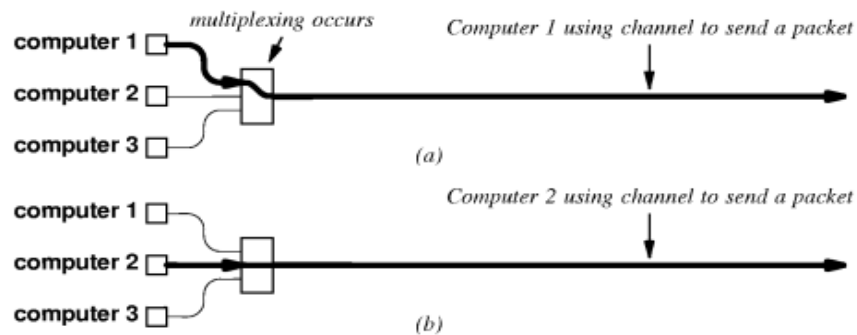


Fig: 5.1: Computers take turns to send packets

5.3 Packets and hardware frames

Frame denotes the definition of a packet used with a specific type of network. Blocks of data are sent in a frame.

NB: A disadvantage of *overhead* occurs in framing i.e. a framing scheme that delimits both the beginning and the end of each frame sends an extra unnecessary character between blocks of data. The chief advantage of sending a character at the beginning and ending of a frame is clear when one considers large delays and computers that crash.

5.4 Byte stuffing

Because network systems usually insert bits or bytes to change data for transmission, the technique is called “data stuffing”. Byte stuffing and character stuffing thus refer to data stuffing used with character-oriented hardware. Bit stuffing refers to data stuffing used with bit-oriented hardware.

5.5 Transmission errors

Lightning, power surges and other electromagnetic interference can introduce unwanted electrical currents in the electronic components or wires used in the communication. Interference normally changes the signal used for transmission without damaging equipment. A change in electrical signal causes the receiver to misinterpret one or more bits of the data. These are termed “transmission errors”.

5.6 Parity bits and parity checking

Use odd or even parity checks. The sender and receiver agree on whether to use odd or even parity check. The sender sends and the receiver computes if the bits arrived intact. The sender computes an extra bit and attaches it to bits being sent. The receiver then detaches it, this is the parity bit.

5.7 Probability, mathematics and error detection

Parity cannot detect transmission errors that change an even number of bits and all error detection methods are approximate and the goal is simply to produce a low probability of accepting corrupted data.

5.7.1 Detecting errors with checksums

Many computer network systems send a “checksum” along with each packet to help the receiver to detect errors. To compute a checksum, the sender treats data as a sequence of binary integers and computes their sum. If the sum grows larger than 16 bits, the carry bits are added into the final sum.

Advantage: the size and ease of computation.

Disadvantage: Not able to detect all common errors e.g. if a transmission error reverses a bit (0 => 1 or 1 => 0).

5.7.2 Detecting errors with Cyclic Redundancy Check (CRC)

This method can more detect errors than checksum. The hardware that calculates the CRC uses two simple components: a “shift register” and an “exclusive or” (XOR) unit. (See page 66 of the recommended text for more).

Combining the building blocks

Those interested in the method can check pg. 66 section 6.11 of the recommended text.

5.8 Burst errors

These are errors that involve changes to a small set of bits near a single location e.g. electrical interference such as lightning often produces burst errors as does electrical interference caused when an electric motor starts near a cable that carries data.

Chapter 6: LAN Technologies and Network Topology

6.1 Direct Point-To-Point communication

Also known as mesh network was the first method used for computer communication in which each communication channel connected to exactly two computers. Its main three useful properties are:

Because each connection is installed independently, appropriate hardware can be used.

Because they have exclusive access the connected computers can decide exactly how to send data across the connection.

Because only two computers have access to the channel, it is easy to enforce security and privacy.

The main disadvantage is that for each pair of computers, the number of connections grows quickly as the size of the set increases i.e.

$$\text{Direct connections required} = (n^2 - n) / 2$$

where n is the number of computers. It is therefore expensive in this respect.

6.2 Shared communication channels

LANs therefore (discovered late 60s - early 70s) were devised as an alternative to the expensive dedicated p2p connections, by relying on sharing the network. The computers take turns to send packets across the medium.

Several LAN designs exist based on e.g. the voltages and modulation techniques used, and the approach to sharing i.e. mechanisms used to coordinate access and transmit packets. The net economic impact of sharing is reduced costs.

Shared networks are used only for local communication because:

a large geographic separation between computers introduces delays.

Providing a high bandwidth communication channel over long distances is expensive as compared to short distances,

6.3 Significance of LANs and Locality of Reference

The main reason for the demand of LANs can be attributed to the fundamental principle of computer networking referred to as “locality of reference”. It states that “communication among a set of computers is not random but follows two patterns”:

Temporal locality of reference: if a pair of computers communicate once, they are likely to communicate again and then periodically.

Physical locality of reference: a computer tends to communicate most often with other computers that are nearby.

6.4 LAN Topologies

Implies the general shape (architecture) of a LAN. Include the following:

6.4.1 Star Topology

In this case, all computers attach to a central point (see the fig below). The hub is an electronic device that accepts data from a sending computer and delivers it to the appropriate destination.

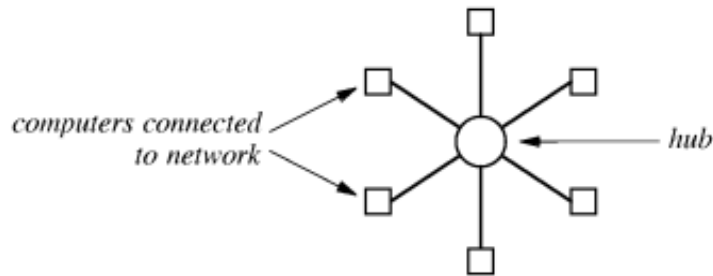


Fig. 6.1: Star network

6.4.2 Ring Topology

Computers are arranged in a closed loop (see fig. 6.2 below).

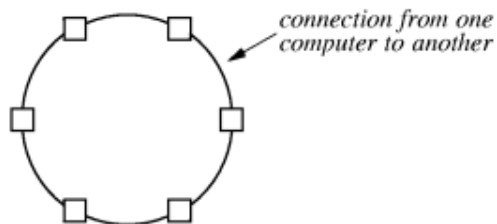


Fig. 6.2: Ring network

6.4.3 Bus Topology

Consists of a single long cable to which computers attach (see diagram below). Any computer sends a signal and all computers receive such signal but they must coordinate while sending signals.

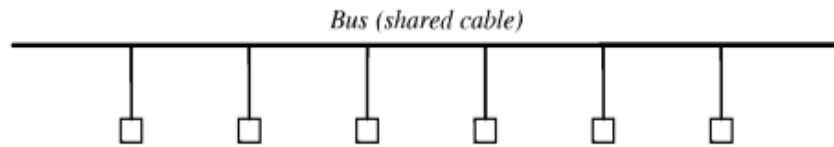


Fig. 6.3 Bus network

The various topologies have their advantages and disadvantages e.g. a ring topology makes it easy for computers to coordinate access and to detect whether the network is operating correctly, but the entire network is disabled if one of the cables is cut. The star topology is more protective since one faulty channel does not render the others dead. The bus requires fewer wires than the star but the network is disabled if the main cable is cut.

6.5 Examples of Bus Network:

6.5.1 Ethernet

It employs bus topology and controlled by IEEE. Ethernet LAN consisted originally of a single coaxial cable called segment, to which multiple computers attached. Each segment is limited to 500m and computer separation is 3m. Originally it operated at 10 megabits per second. Fast Ethernet operates at 100Mbps while gigabit Ethernet operates at 1000Mbps.

Sharing on the Ethernet (See fig. 6.4 below)

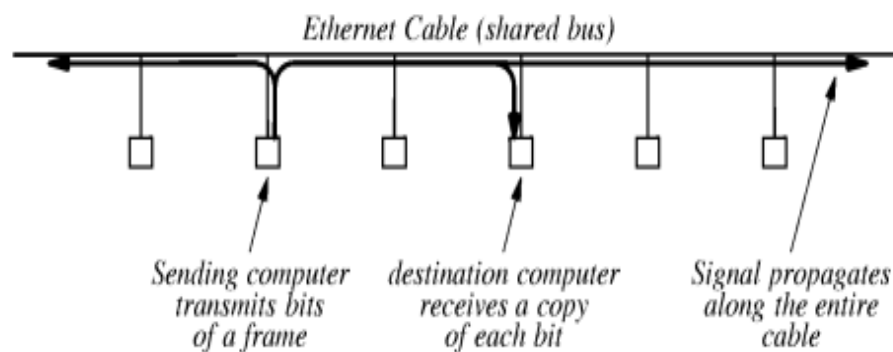


Fig. 6.4: Sharing on bus network

The sender sends a signal that propagates to both ends of the cable. It has exclusive use of the cable and the rest must wait. The others can then transmit once it completes.

Carrier Sense on Multiple Access Networks (CSMA)

Ethernet has no centralized controller to help computers coordinate communication instead all such computers attached participate in a distributed coordination scheme called “carrier sense multiple access” (CSMA). A sender transmits electrical signals used to encode bits called carrier, and the others can check for that before transmitting. If carrier is present, the other computers must wait until the sender finishes. To check for a carrier wave is called “carrier sense”.

Collision Detection and Back Off With CSMA/CD

CSMA therefore prevents a computer from interrupting an ongoing transmission, but cannot prevent all possible conflicts. For example, two computers far apart may transmit their frames simultaneously having sensed no carrier. At some point in the cable they interfere. Such is called a “collision” and causes the frames not to be received correctly. To ensure no other computer sends simultaneously, the sender monitors signals on the cable and if they differ from the original signal, a collision must have occurred, the sender then stops transmitting immediately. Such monitoring is called “collision detect” and the whole mechanism is CSMA/CD.

CSMA/CD both detects and recovers from such collisions. Each computer randomly chooses a delay less than d , the maximum possible, and so the computer with the smallest delay will transmit first.

If two or more computers use the same delay to bring further collision, they are required to double such delays for each subsequent collision until a solution is found e.g. from $0 - d$, then $0 - 2d$, then $0 - 4d$ etc. This doubling of delay range is referred to as “binary exponential back off”.

Wireless LANs and CSMA/CA (See fig. 6.5 below)

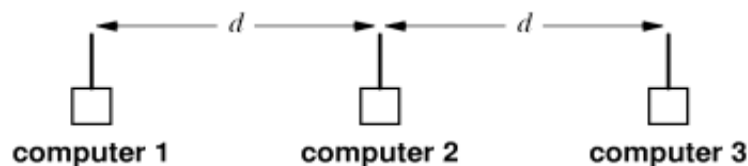


Fig. 6.5: Sharing on wireless network

Wireless LANs hardware uses antennas to broadcast RF signals through the air unlike cables. Participating computers in this case are configured to the same RF and so must take turns in sending packets. Wireless LAN transmitters have only enough power to transmit a short distance and so cannot use CSMA/CD technique, but apply CSMA with collision avoidance, CA.

In the above diagram, comp1 and comp3 are too far apart to receive each other's transmission, e.g. when both send to comp2 simultaneously they have no idea of collisions except comp2 knows. The CSMA/CA triggers a brief transmission from the intended receiver before a packet is transmitted i.e. comp1 sends first a brief control message to comp2 before it transmits. The response from comp2 is received by all computers within the range of its antenna.

Collision of control messages can still occur with CSMA/CA but the transmitting computers will apply the idea of random back offs.

NB: Another example of bus topology is local talk (discuss it).

Example of ring network

6.5.2 IBM token ring

It uses an access mechanism called "token passing". Operates a single shared medium. See diagram below

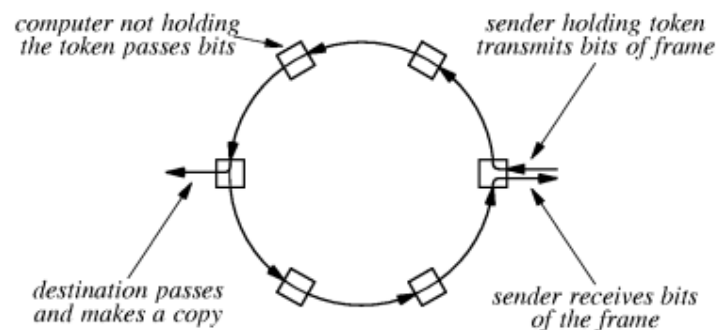


Fig. 6.6: Transmission on ring network

As the sending computer transmits a frame, the bits pass through all the other computers and back to the sender. This allows the sender to verify that what is received is what was sent. Only the recipient makes a copy of the transmission but the others simply forward it i.e. the frames.

Token ring does not use CSMA/CD but the token ring hardware moves among all the computers to ensure that the permission is passed to each computer in turn. Such coordination uses a special reserved message called "token". It gives a computer permission to send one frame only at a time. This ensures fairness.

6.5.3 Fiber Distributed Data Interconnect, FDDI (an example of ring network)

Problem with token ring is susceptibility to failures e.g. failure on one machine disables the entire network.

FDDI is a very fast token ring technology transmitting data at 100 million bits per second and uses optical fiber instead of copper cables to interconnect computers. It also applies the concept of redundancy to overcome failures i.e. two complete rings if one fails the other takes over. (See fig. 6.7 below).

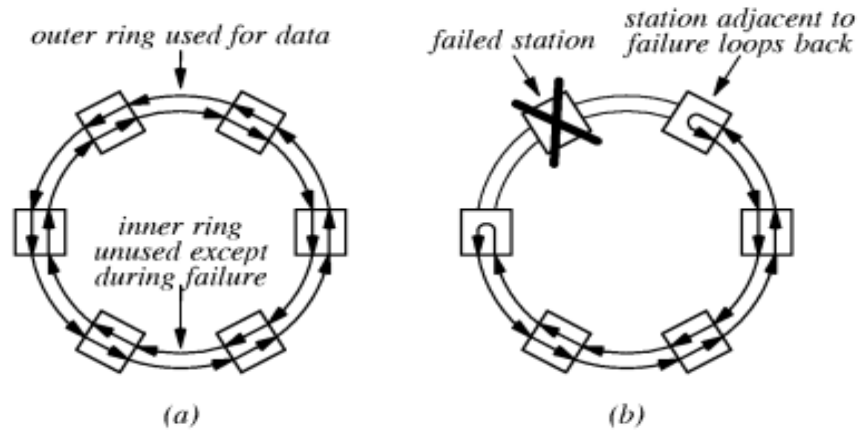


Fig. 6.7: Transmission in FDDI

Data flows opposite in each of the two rings. If breakage occurs, the computers reconfigure to use the inner network. Such process to reconfigure is referred to as “self healing”.

6.5.4 Example of Star Network

Asynchronous Transfer Mode (ATM) (See fig. 6.8 below).

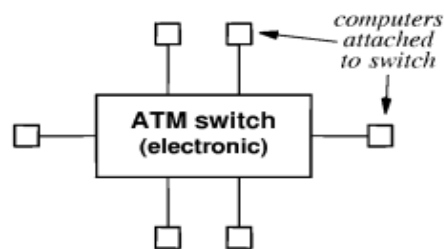



Fig. 6.8: Star network

It was developed by telephone companies. It uses an electronic switch to which several computers attach. Propagates data only to the communicating pair of computers. If connection breaks between a computer and switch, the others are not affected. Designed to provide high bandwidth e.g. 155 Mbps or higher and so uses optical fiber instead of copper cables and usually a pair of fibers to allow faster simultaneous communication.



Chapter 7: Hardware Addressing and Frame Type Identification

7.1 Specifying a Recipient

A frame transmitted across a LAN reaches all stations. The network interface hardware on a station detects the electrical signal and extracts a copy of the frame. For two computers to communicate directly on a LAN, the technology uses an addressing scheme to provide direct communication. This is “physical address” or “hardware address” or “media access address” (MAC). The LAN hardware checks on the address and determines whether to accept or reject the frame. Each frame has a header for both the destination and source addresses.

7.2 How LAN Uses Address to Filter Packets

The LAN hardware interface is separate from the computer’s CPU and memory, and handles all the details of sending and receiving frames on the shared medium e.g.

- It checks the length of incoming frames to ensure that they lie between the minimum and maximum sizes in the standard.
- Checks the CRC to ensure bits arrive intact.
- Discards frames with errors.

See fig.7.1 below

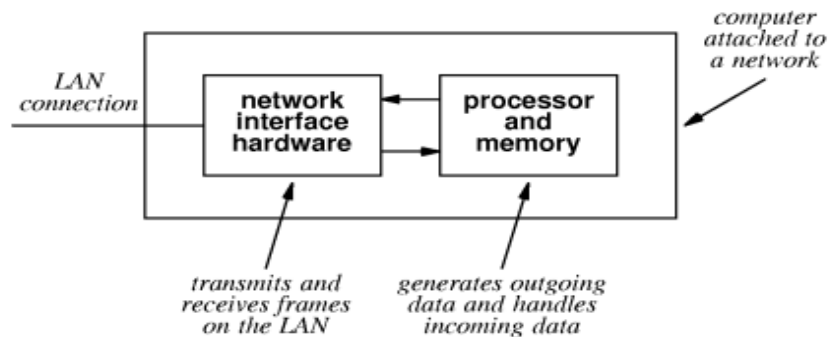


Fig 7.1: LAN hardware interface

A frame addressed to a non-existent station is ignored and since the hardware interface and CPU are separate, the capture and address comparisons do not interfere with normal computing.

7.3 Format of a Physical Address

Each LAN technology uses its own way of addressing e.g. with respect to what numeric values to use and how such addresses are assigned etc. The address forms can broadly be categorized as:

- i. **Static** – the scheme relies on the hardware manufacturer to assign a unique physical address to each network interface. It does not change unless the hardware is replaced.

- ii. **Configurable** – provides the computer with a mechanism to set the physical address. This is done when the hardware is first installed. It is permanent across reboots.
- iii. **Dynamic** – has the mechanism to automatically assign the address when a station first boots. The station tries random numbers until it finds a unique one to use and this may change each time it reboots.

NB: State the advantages and disadvantages of each form of addressing scheme.

- *Static addressing:* has the advantage of ease of use and permanence. The addresses are globally unique across the various manufacturers.
- *Dynamic addressing:* has the advantage of eliminating the need for hardware manufacturers to coordinate in assigning addresses and allows each address to be smaller, since uniqueness of an address is important only within a single LAN. Its disadvantage includes lack of permanence and potential conflict since each time of reboot, a station obtains a new address.
- *Configurable addressing:* provides a compromise between the two, i.e. it is permanent across reboots and the address space is small as in dynamic addressing.

7.4 Broadcasting

Refers to transmissions available to a large audience i.e. any broadcast avails data to all other computers on the network. It is useful e.g. when a computer is trying to find a particular printer in a network i.e. it broadcasts and only the specified printer responds.

In this case, even though all stations receive a signal, the hardware interface on each station uses the frame's destination address to determine whether to keep a copy. To be efficient, most LAN technologies extend the addressing scheme such that both the computer's address and a special reserved address called "broadcast address" are included. A frame arriving with either of the two addresses will therefore be delivered to the computer's operating system.

7.5 Multicasting

Broadcasting is wasteful in the sense that discarding frames involves using the CPU to make a decision. Multicasting therefore is a restricted form of broadcasting but in this case the network interface does not automatically forward frames to the CPU. The hardware is programmed to know which multicast frames to accept or reject i.e. it is the one that decides and not the CPU now.

Multicasting extends the addressing scheme by reserving some addresses for multicast, and extends the network interface hardware by allowing it to recognize additional set of addresses. On booting, the interface is programmed to recognize only the computer's address and the broadcast address. If therefore an application on the computer wishes to receive multicast frames, it must inform the interface which multicast address to use. The interface then adds the address to the set it will recognize and begins accepting frames sent to that address.

7.6 Identifying Packet Contents

Two methods exist to identify a frame's contents:

- i. **Explicit frame type** – the network hardware designers specify how type information is included in the frame and the values used to identify various frame types. It is termed “self-identifying”.
- ii. **Implicit frame type** – the network hardware does not include a type field in each frame, instead the frame carries only data. The sender and receiver therefore must agree on the contents of a frame or agree to use part of the data portion of the frame as a type field.

NB: Each LAN technology defines a frame format and most technologies consist of a header followed by a data area. All frames used with a given technology have the same header format because the size and format of the header is fixed, but data area depends on the amount of data sent.

For networks that do not have self-identifying frames, i.e. do not have a type field in the frame header, the approaches they use to know the type of data are:

- i. Before any data is sent, the sender and receiver agree to use a single format.
- ii. Before any data is sent, the sender and receiver agree to use the first few octets of the data field to store type information.

7.7 Network Analyzers, Physical Addresses, Frame Types

A network analyzer or monitor is a device that determines how well a network system is performing. They report statistics e.g. the average number of frames per second or the average frame size.

Analyzers consist of a standard portable computer e.g. notebook PC with a standard LAN interface and it must be dedicated i.e. specific to analyzing only.

To read packets, the analyzer software places the computer's network interface hardware into promiscuous mode i.e. accept all frames. It places a copy of each frame in the computer's memory and interrupts the CPU to inform it that a frame has arrived.

NB: The analyzer is configurable and the exact configuration a user selects determines what field the analyzer examines and what information it keeps.

Chapter 8: LAN Wiring, Physical Topology and Interface Hardware

Networks are designed to operate at the highest rate the hardware can support and the speed at which they operate is fixed in design i.e. does not depend on the CPU rates of the attached computer.

The network interface hardware i.e. NIC or network adapter card, handles all the details of packet transmission and reception. The NIC understands the electrical signals used on the network, the rate at which data must be sent or received and the details of the network frame format. Thus, NIC for Ethernet cannot be used for Token Ring network etc.

To transmit on the network, the CPU forms a packet in memory and instructs NIC to start transmission. The NIC uses the computer's interrupt mechanism to inform the CPU when transmissions complete. Again, NIC can receive incoming packets without the CPU's intervention. The CPU only allocates buffer space in memory and instructs NIC to read in. The NIC then interrupts the CPU accordingly.

The connection between the NIC and the network may take different forms i.e. depends on the network technology i.e. the NIC may or may not contain all the intelligence required and so may or may not require extra devices to help it join on the network. We will use an example of Ethernet wiring schemes as a case study.

- i. **Original Thick Ethernet Wiring:** - also called "thick wire Ethernet" or "thick net" or 10Base5. Consists of a large coaxial cable. Includes an NIC with circuitry to handle the digital aspects of communication, including error detection and address recognition. The NIC does not include analog hardware and so does not handle analog signals e.g. does not detect a carrier, convert bits to appropriate voltages for transmission, or convert incoming signals to bits. This is achieved by a separate device called "transceiver" which is required for each computer. (See fig. 8.1below)

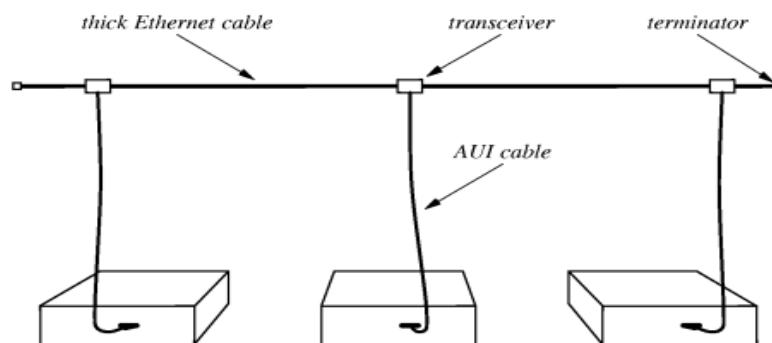


Fig. 8.1: Original Thick Ethernet Wiring. An AUI connects the NIC in each computer to its corresponding transceiver.

Since it can be cumbersome and expensive to use a single transceiver for each computer, connection multiplexing is advisable, that allows multiple computers to attach to a single transceiver. (See fig. 8.2 below)

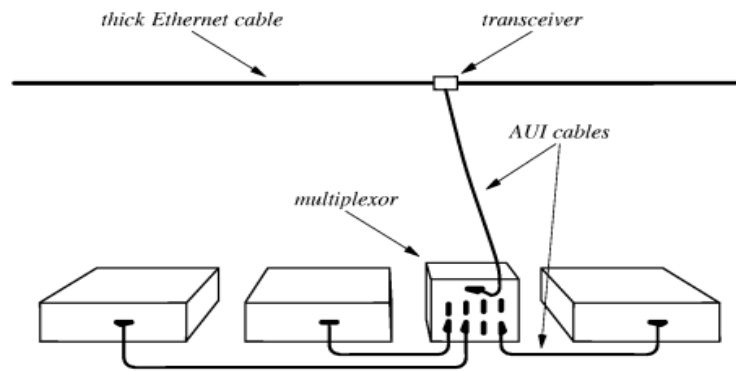


Fig. 8.2: A Connection Multiplexor, Multiplexor attaches to a single transceiver, multiple computers connect to multiplexor, each computer operates as if it connects directly to a transceiver.

ii. **Thin Ethernet (Thinnet or 10Base2)**

It uses thinner coaxial cable. Costs less to install and operate than thicknet. No external transceivers are required since the hardware that performs the function is inbuilt. Does not use AUI cable but attaches directly to the back of a computer using a BNC connector. (See fig. 8.3 below)

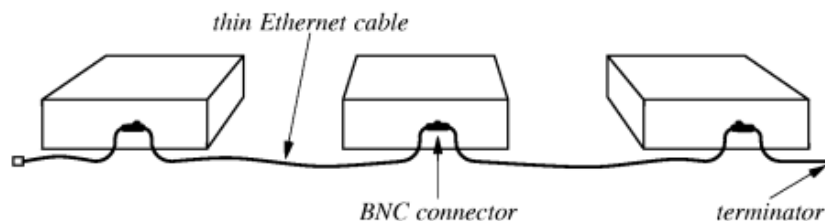


Fig. 8.3: Thin Wire Ethernet. Flexible cable connects from NIC on one computer to the NIC on another computer.

iii. **Twisted Pair Ethernet – (10 BaseT)**

It has become the standard for Ethernet. Extends the idea used with connection multiplexing i.e. consists of an electronic device (hub) serving as the network

center. Uses twisted pair wiring and RJ-45 connectors (larger than for telephone). Each computer uses CSMA/CD to access the network. Hubs come in different sizes e.g. 4 or 5 to hundreds. (See fig. 8.4 below).

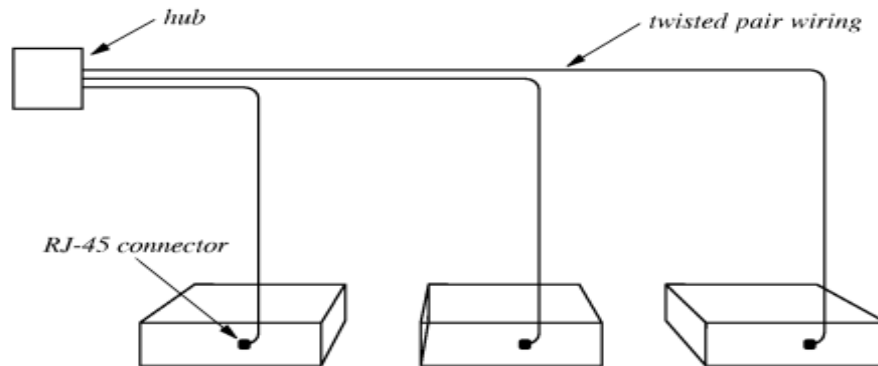


Fig. 8.4: Computer connect to Ethernet hub using 10Base-T wiring, each computer has a dedicated connection.

Advantages and disadvantages of the wiring schemes

- The transceiver type allows network to continue operating even if one transceiver is removed, but finding, testing and replacing a failed transceiver is difficult.
- The thinnet is susceptible to disconnection.
- The hub type is more immune to disconnection.

NB:

- It is possible to mix the wiring schemes in one network since they use a standard frame format.
- To make it possible to change wiring schemes without changing NIC, they may support multiple wiring schemes e.g. the three wiring schemes on one NIC (See fig. 8.5 below).
- But only one scheme may be active at a time (i.e. activated by software)
- The computer's physical address remains the same when moving to a new wiring scheme since the physical address is assigned to the NIC.

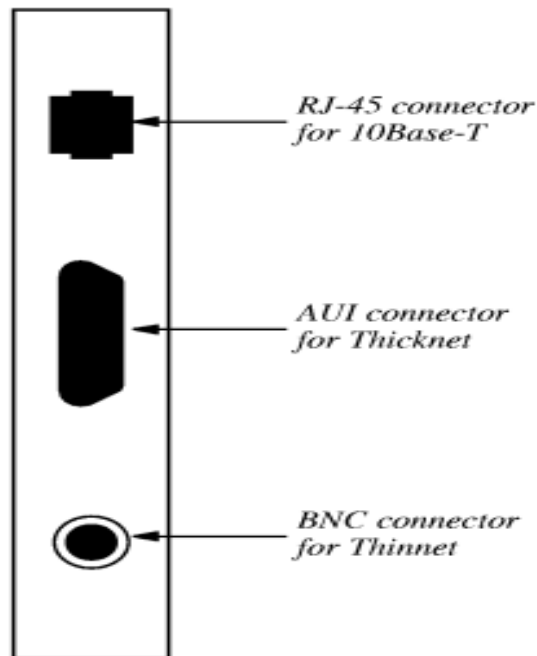


Fig. 8.5: Ethernet Interface Card, each wiring scheme uses a different style connector.

Notes:

- i. **Category 5e (Category 5 enhanced)** Ethernet cables are newer than **category 5** cables and support faster, more reliable data transmission through networks. CAT5 cable is able to transmit data at 10 to 100Mbps speeds, while the newer CAT5e cable should be able to work at up to 1000Mbps. The CAT5e cable is also better than the CAT5 at ignoring "crosstalk," or interference from the wires within the cable itself. Though CAT6 and CAT7 cables exist and can work with even faster speeds, CAT5e cables will work for most small networks.
- ii. **Cat6 and Cat6a**
The most distinctive difference between Cat6 and Cat6a is the data transmission speed. Both Cat6 cables and Cat6a cables can support data transmission rates to 10 Gbps. But Cat6 cables can only keep 10 Gbps to 37~55 meters (121~180 feet), and Cat6a cables can relay 10 Gbps up to 100 meters (328 feet).

Chapter 9: Extending LANs: Fiber Modems, Repeaters, Bridges and Switches

9.1 Distance limitation and LAN

Network design needs to consider capacity, maximum delay and distance achievable at given cost. There is need for fair access mechanisms that provide for one main motivation to limit LAN length. Also, the longer the length, the weaker the signals.

i. Fiber optic extensions

They use optical fibers and a pair of fiber modems. Fiber has low delay and high bandwidth. It can extend to several kilometers. Advantage is the ability to provide connection to a remote LAN without changing the original LAN or the computer. Used commonly to connect a computer in one building to a LAN in another building. (See fig.9.1 below),

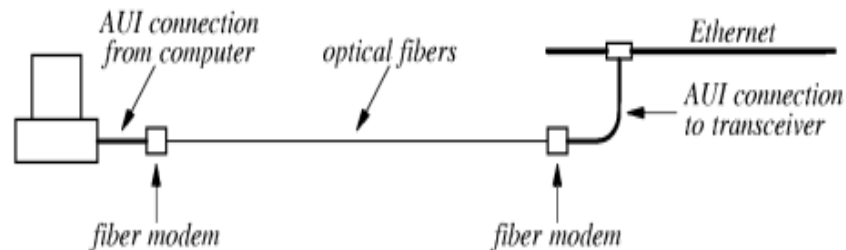


Fig 9.1: Optical Fiber and Fiber Modems used to provide connection between a computer and a distant Ethernet.

ii. Repeaters

They are analog devices and transmit an amplified copy of a signal from one segment to another. They do not understand frames and have no physical addresses. Do not wait for complete frames to retransmit. The maximum Ethernet size is 500m. With repeaters, the source/destination cannot determine whether they are/are not on the same segment. There should be no more than four repeaters separating a pair of stations. Originally designed for close proximity e.g. in a building, but can now be extended via fiber modems to separate buildings. Problem is that they can even retransmit interfered with signals.

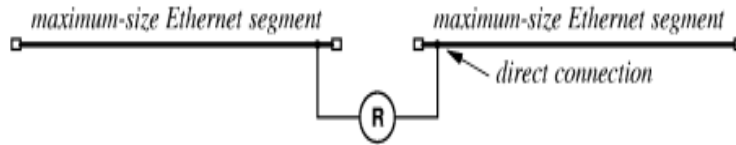


Fig 9.2: A repeater R connecting two Ethernets

- iii. **Bridges** (*Network bridges are considered digital devices, as they operate at the data link layer of the OSI model, which deals with binary data and MAC addresses, making them inherently digital in their function.*)

They handle complete frames. They listen to traffic on each segment in promiscuous mode (promiscuous mode – it is a network security, monitoring and administration technique that enables access to the entire network data packets by any configured network adapter on a host system ie used to monitor traffic). They help in isolating problems on different segments and use same network interface as conventional computer i.e. consists of a conventional computer, CPU, memory and two NICs.

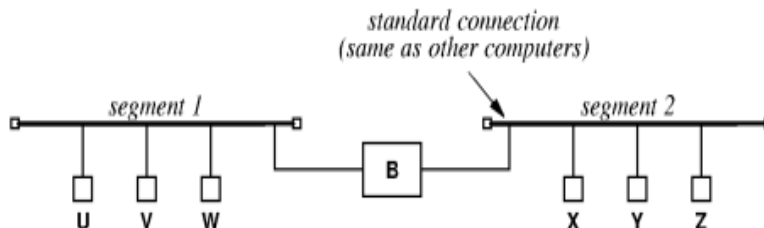


Fig 9.3: Six computers connected to a pair of bridged LAN segments. Bridge receives complete frames.

They perform frame filtering and are dedicated to a single task i.e. do not run application software i.e. CPU executes code from ROM. They do not unnecessarily forward frames from one segment to segment unless under broadcast/multicast. Most are called adaptive/learning bridges since they automatically learn computer locations on a LAN. See the list below.

Event	Segment 1 List	Segment 2 List
Bridge boots	–	–
U sends to V	U	–
V sends to U	U, V	–
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

Fig 9.4: A sequence of events for the example network fig 7.3 above and the locations of computers that the bridge has learnt.

When planning a bridged network, it must be noted that the bridge hardware is designed to permit communication on separate segments simultaneously i.e. parallelism. Thus, a set of computers that interact frequently should be on the same segment.

Note that fiber modems can be used to extend LANs with bridges as in repeaters.

Bridging across longer distances can be achieved via the use of leased serial lines or leased satellite channels.

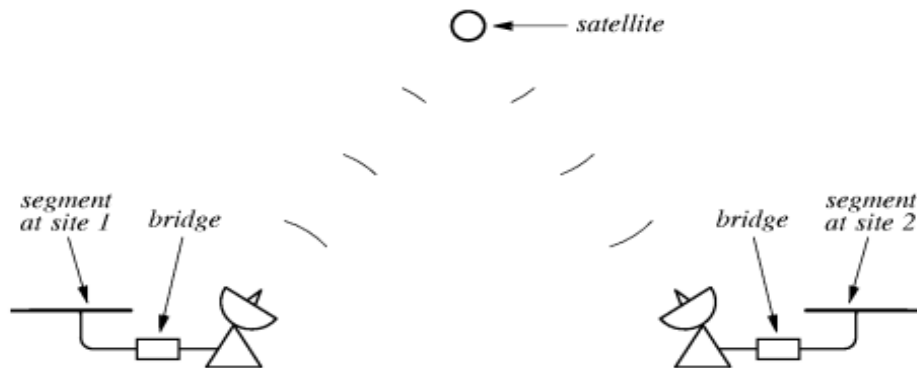


Fig 9.5: A bridge using a leased satellite channel to connect LAN segments at two sites. A satellite bridge can span arbitrary distance.

The leased line is cheaper than the satellite. Bridged LANs or leased type use low-bandwidth connections to reduce costs. The bridge hardware must perform buffering because the LAN

segment forwards frames faster than the satellite. If the buffer is full, some frames are discarded or some method of control must be implemented.

NB: Not all bridges can be allowed to forward frames or a cycle of bridges introduces the problem of infinite forwarding. See fig below.

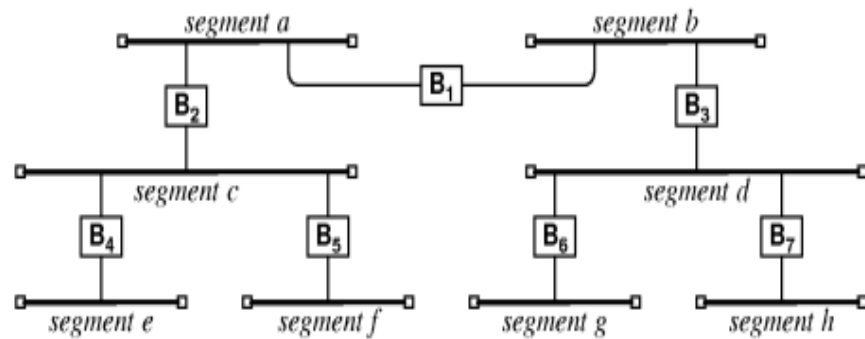


Fig 9.6: A bridged network that consists of eight segments connected by seven bridges. Computers can be attached to any of the segments.

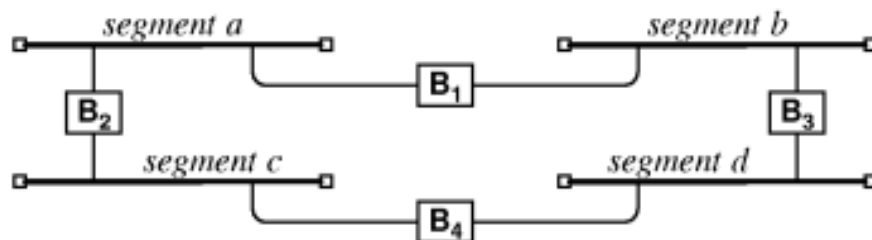


Fig 9.7: Bridges connected in a cycle, problem occurs if all bridges forward broadcast frames.

Therefore, in order to prevent the problem of infinite loops, a bridged network must not allow both of the following conditions to occur simultaneously:

- All bridges forward frames
- The bridged network contains a cycle of bridged segments.

Bridges configure themselves automatically to avoid loops. The scheme is referred to as *distributed spanning tree DST* i.e. when a bridge first boots, it communicates with other bridges on the segment to which it connects. They then perform the DST algorithm computation to decide which bridges will not forward frames. The bridges that then agree to forward frames form a graph that does not contain any cycles i.e. a tree.

9.2 Switched LANs (*Network switches are considered digital devices, as they manage and route digital signals within a network, meaning they transmit data in the form of binary bits (ones and zeros) rather than continuous analog waves.*)

Consist of an electronic device i.e. switch, that allows multiple computers to attach to it and to send and receive data. Similar to a hub though a hub simulates a single shared medium while a switch simulates a bridged LAN with one computer per segment. Since switches are more expensive than hubs due to the higher aggregate data rates than a hub, some organizations mix the two. Each hub connects to a switch port and multiple computers attach to the hub. Computers on a hub therefore behave as segments on their own while parallelism is maintained by the switch across such segments.

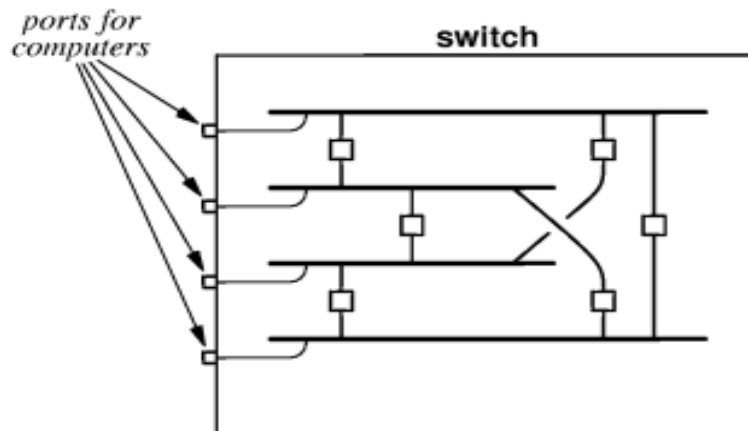


Fig. 9.8: The concept underlying a switched LAN. Electronic circuits in the switch provide each computer with the illusion of a separate LAN segment connected to other segments by bridges.

Chapter 10: WAN Technologies and Routing

10.1 Network technologies can be classified as:

- LAN – spans a single building or campus
- MAN – spans single city
- WAN – spans several cities, countries or continents.

The main difference between a LAN and a WAN is that a WAN must be able to grow as needed to connect many cities spread across large geographic distances, with many computers at each site.

10.2 Packet Switches

A WAN is constructed from many switches to which individual computers attach. Referred to as a packet switch since it moves complete packets from one connection to another, it was conventionally constructed from minicomputers dedicated to the task of switching. Nowadays it is made of a special-purpose hardware having two types of I/O connections, one I/O type operates at high speed and connects the switch to a digital circuit that leads to another packet switch and the other I/O operates at low speeds and connects to individual computers. See fig. 10.1 below.

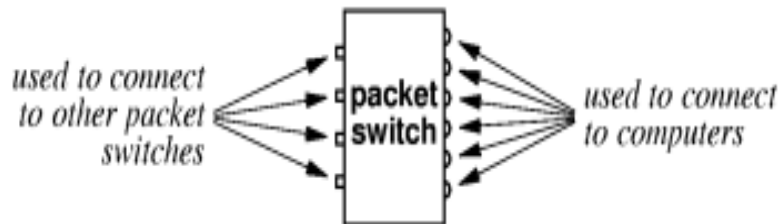


Fig. 10.1: A packet switch with two types of I/O connectors. One connects to other packet switches and the other to computers.

To form a WAN, you require a set of interconnected switches. See fig 10.2 below.

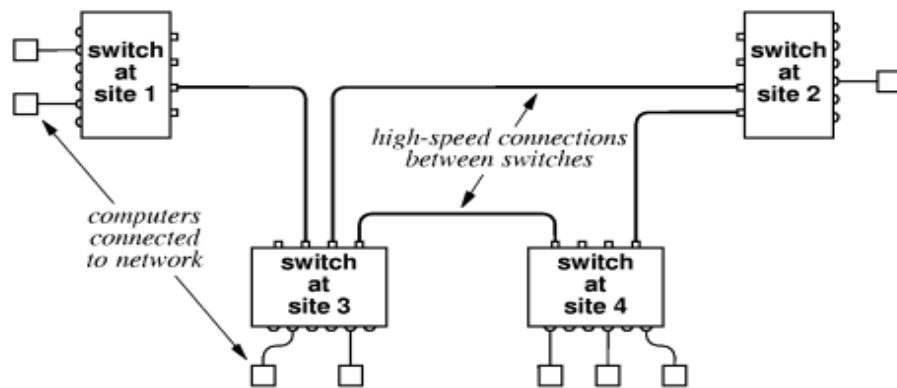


Fig 10.2: A small WAN formed by interconnecting packet switches. Connections between packet switches usually operate at a higher speed than connections to individual computers.

10.3 Store-and-Forward

This is the technique that enables computers to communicate in a WAN simultaneously by buffering packets in memory. During store, the I/O hardware inside the packet switch places a copy of the arriving packet in the switch's memory, informs the processor via interrupt. During forward, the processor examines the packet, determines over which interface it should be sent and starts the output hardware device to send the packets.

Addressing in a WAN is done hierarchically, usually divided into two parts, first identifies a packet switch, and second identifies a computer attached. The address otherwise is represented as a single binary value allowing users and applications to treat the address as a single integer. See fig. 10.3 below.

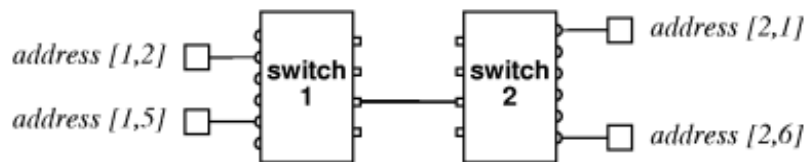


Fig 10.3: Example of hierarchical addressing in WAN. Each address consists of two parts: first part identifies switch; second part identifies computer connected to the switch.

10.4 Next-Hop Forwarding

It is the technique packet switches use to forward packets to their eventual destinations. This is because packet switches do not keep complete information about how to reach all possible destinations, but just the next place. This is then stored in a table that lists the destination and the next hop e.g.

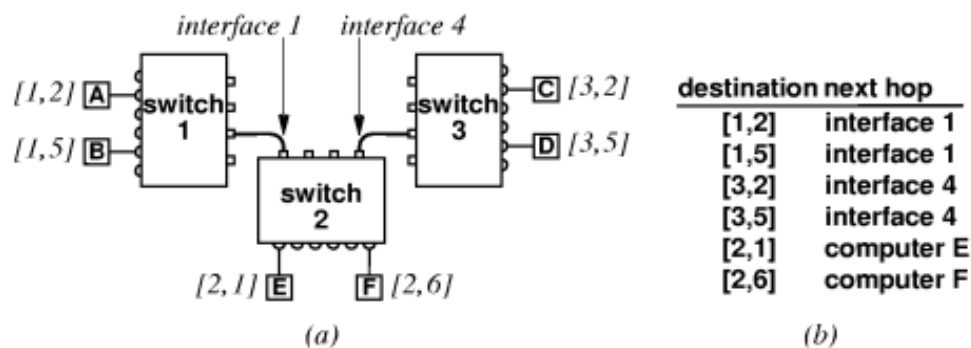


Fig 10.4: (a) A network consisting of three packet switches and (b) the next-hop forwarding information found in switch 2. Each switch has different next-hop information.

Destination	Next hop
[1,2]	Interface 1
[1,5]	Interface 1
etc.	

Table 10.1: Next-hop information in switch 2

The table with next hop information is called “routing table” and the process of forwarding packets is called “routing”.

10.5 Routing in a WAN

To handle small load increases in a WAN, its capacity can be increased by adding I/O interface hardware or a faster CPU. But to handle larger capacities, packet switches are added to the interior of the network called “interior switches” and do not have to attach computers. Those that attach computers are called “exterior switches”.

For the WAN to work well:

- Both switches must have a routing table
- Both switches must forward packets

The values in the table must guarantee:

- Universal routing – the routing table in a switch must contain a next hop for each possible destination
 - Optimal routes – in a switch, the next hop value in the routing table for a given destination must point to the shortest path to the destination. See fig. 10.5 below.
- (See pg 175 to explain routing i.e. fig 12.6 and 12.7)

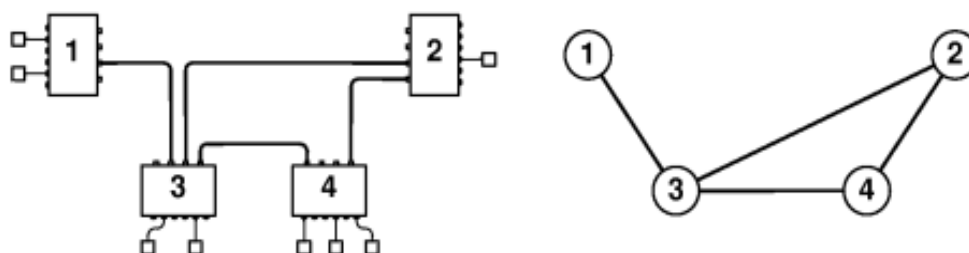


Fig 10.5: The network from fig 10.2 and the corresponding graph. Each node in the graph corresponds to a packet switch, and each edge between two nodes represents a connection between the corresponding packet switches.

destin- ation	next hop	destin- ation	next hop	destin- ation	next hop	destin- ation	next hop
1	-	1	(2,3)	1	(3,1)	1	(4,3)
2	(1,3)	2	-	2	(3,2)	2	(4,2)
3	(1,3)	3	(2,3)	3	-	3	(4,3)
4	(1,3)	4	(2,4)	4	(3,4)	4	-
<i>node 1</i>		<i>node 2</i>		<i>node 3</i>		<i>node 4</i>	

Fig 10.6: The routing table for each node in the graph of fig 10.5. The next-hop field in an entry contains a pair (u, v) to denote the edge in the graph from node u to node v .

10.5.1 Use of Default Routes

In small WANs, a list of duplicate copies can be tolerated (see fig 10.6). But in large WANs, examining such a list can be tedious and so many WAN systems include a mechanism to eliminate the case of duplicating routing. Called default route or default routing table entry, it allows a single entry in a table to replace a long list of entries that have the same next-hop value, and it has a lower priority than other entries, i.e. used as last resort. (See fig. 12.8 which is a revision of fig. 12.7 of the reference text).

10.5.2 Routing Table Computation

Is performed by software in two ways:

- i. *Static routing* – program computes and installs routes when a packet switch boots and the routes do not change.
- ii. *Dynamic routing* – program builds an initial routing table when a packet switch boots and the program alters the table as conditions in the network change.

The first case is simple and has low network overhead but is inflexible. The latter is more preferred to allow modification of routes in case of e.g. failures, congestion etc.

10.5.3 Shortest Path Computation in a Graph

The software computing routing represents the network as a graph and uses the method of Dijkstra's Algorithm that finds the distance along a shortest path from a single source node to each of the other nodes in the graph. A next-hop routing table is hence constructed during the computation of shortest path. See fig. 12.9 of recommended text for explanation.

10.5.4 Distributed Route Computation

Each packet switch computes its routing table locally then sends messages across the network to neighbouring packet switches to inform them of the result. This is done periodically to allow the network to adapt if an individual packet switch or communication link fails.

10.6 Examples of WAN Technologies

- ARPAnet - ARPANET was funded by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA), which is now called DARPA. It was the first wide-area network to use packet switching and distributed control. ARPANET was the foundation of the modern internet.
- X.25 – developed by the ITU. It is rather expensive for the performance it delivers and has limits on the speed at which it can deliver.
- Frame Relay – designed to accept and deliver blocks of data, where each block can contain up to 8k octets of data. Was designed majorly for bridging LAN segments. Is high speed.
- Switched Multi-megabit Data Service (SMDS) – is of high speed and designed to carry data. Uses a small header allowing each packet to contain up to 9188 octets of data.
- ATM – is a single technology design that can be used to provide voice, video and data services across a wide area.

Chapter 11: Network Ownership, Service Paradigm & Performance

A private network is owned by a company or individual while a public network is owned by the common carriers, which must be available to many subscribers in many locations. The chief advantage of private network is that the owner has complete control. The chief advantages of public networks are flexibility and the ability to use state of the art networking without maintaining technical expertise.

11.1 Virtual Private Networks

Combine the advantages of both private and public networks. Allow a company with multiple sites to have a private network over a public network as a carrier. Require a company to buy a special hardware and software for each of its sites, which is then placed between the private network and the public network. Each of the systems must be configured with the addresses of the company's other VPN systems. Software then exchanges packets only with such sites. The VPN also performs encryption.

11.2 Service Paradigm

All network interfaces are placed in one of two paradigms:

- Connection-oriented
- Connectionless-oriented

The first option is where computers communicating first establish a connection before transmitting, and such connection is maintained until they disconnect.

Second option operates by packaging the data appropriately and sends it to the network for delivery. The chief advantage of the first is ease of accounting and the ability to inform the communicating computers immediately when a connection breaks i.e. it is easier to charge for the length of time a connection is open than for the number of packets sent. A failure in a connectionless may go unnoticed and unreported and the sender may continue sending packets even after failure. The chief advantage of the second option is less initial overhead i.e. sends data immediately.

11.3 Switched Connections and Permanent Connections

Early computers achieved permanent connections by the use of dedicated hardware. Modern networks achieve it by configuring the network to form a dedicated path electronically. Such configuration is stored in non-volatile memory allowing the computers to reestablish connections automatically even after power failures.

For switched, computers must establish connections when they need to communicate. They persist for short durations. In case of node failure, computers must reestablish connections.

- Advantages of permanent connections are *persistence* and *guaranteed availability*.
- Advantages of switched are *flexibility* and *generality* i.e. no need to install/change the physical wiring etc.

11.4 Network Performance Characteristics: may include but not limited to the following:

- i. **Delay** – specifies how long it takes for a bit of data to travel across the network from node to node, measured in seconds or its fractions. There are various types of delays including:
 - Propagation delay is the time it takes to travel along a medium while
 - Switching delay is the time introduced by electronic devices in the network e.g. hubs, bridges etc.
 - Access delays are introduced by mechanisms e.g. CSMA/CD etc. Queuing delays are introduced by e.g. store-and-forward process.
- ii. **Throughput** – is a measure of the rate at which data can be sent through the network specified in bps.

Chapter 12: Protocols, Layering and Internetworking

12.1 The Need for Protocols

It is usually software that handles most of the low-level communication details and problems automatically, making it possible for application programs relying on network software to communicate as they do not interact with hardware directly. This requires all parties involved in a communication to agree on a set of rules to be used on message exchanges, i.e. protocol. Thus, a set of rules that specifies the format of messages and the appropriate actions required for each message is known as a “network protocol”.

Protocols are designed in suites i.e. communication problem is divided into sub pieces and a separate protocol designed for each piece. This makes it easier to design, analyze, implement and test. Such divisions increase flexibility because it allows subsets of protocols to be used as needed. The combination of protocols should handle all possible hardware failures or other exceptional conditions although each should handle part of the communication problem.

Task: Read about OSI reference model.

12.2 The 7 Layers of the OSI Model

i. Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

ii. Data Link Layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

Protect Your Network Layers with Forcepoint NGFW

iii. Network Layer

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such

as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

iv. Transport Layer

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

v. Session Layer

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and determined at layer 5. Session layer services also include authentication and reconnections.

vi. Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

vii. Application Layer

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

12.3 Techniques protocols use

Some protocols go beyond just error detection e.g. they may even try to repair or circumvent problems.

12.3.1 Sequencing Out-Of-Order Delivery

A connectionless network system that can change routes may deliver packets out of order. Sequencing thus ensures that the sender attaches a sequence number to a packet and the receiver stores both the sequence number of the last packet received in order as well as a list of additional packets that arrived out of order. If the packet received is the next one, protocol software delivers it to the next higher layer otherwise keeps it in its list.

Another technique is the “sliding window” where the sender and receiver agree on the “window size” i.e. the maximum amount of data that can be sent before an acknowledgement arrives, e.g. 4 packets. The sender keeps a copy for reliability i.e. retransmission in lost cases and the receiver buffers the entire window. (See pg 214/215 for diagrams and for further explanations).

12.3.2 Mechanisms to avoid network congestion

Congestion is a big problem in packet switching systems (See fig below)



Fig 12.1: A graph that represents a network of six packet switches. Such networks can experience congestion.

Assume 1 sends to 5, no congestion. If both 1 and 2 send, congestion occurs. Overtime, the network may become unusable due to long delays e.g. packet switch 3 may start to discard packets. This condition is referred to as “congestion collapse”. Two approaches are used by protocols to avoid this:

- i. Arrange for packet switches to inform the sender when congestion occurs.
- ii. Use packet loss as an estimation of congestion.

In *i*, packet switch either sends a special message to sender or sets a bit in the header of each packet that delays and receiver includes that information in its acknowledgement to sender; while *ii* is more modern, the sender uses timeout and retransmission strategies.

Congestion is therefore responded to by reducing the rate at which packets are being transmitted.

Chapter 13: Internetworking: Concepts, Architecture and Protocols

13.1 Motivation for Internetworking:

Based on no single networking technology being the best for all needs e.g. one large organization may use multiple physical networks.

The concept of “universal service” is therefore achieved i.e. a user on any computer in any part of an organization can communicate to any other user.

Electrical incompatibilities make it impossible to form a large network merely by interconnecting wires from two networks. Also, extension techniques e.g. bridging cannot be used with heterogeneous network technologies since different technologies use incompatible packet formats and addressing schemes. Thus, internetworking requires the use of additional hardware systems i.e. routers to interconnect a set of physical networks and software that provides universal service.

13.2 A Virtual Network

It is the name used for internet since the communication system is an abstraction i.e. even though a combination of hardware and software provides the illusion of a uniform network system, no such network exists.

NB:

- Internet software provides the appearance of a single seamless communication system to which many computers attach.
- Internet protocol software hides the details of physical network connections, physical addresses and routing information.

See Fig 13.1 below (pg. 228 of recommended text).

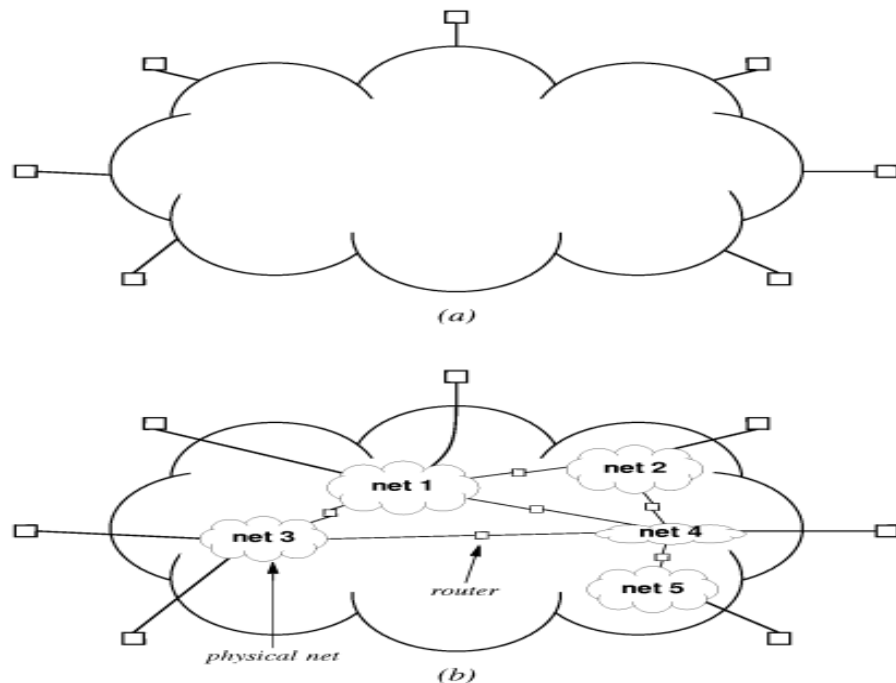


Fig 13.1: The Internet concept. (a) The illusion of a single network that TCP/IP software provides to users and applications, and (b) the underlying physical structure in which a computer attaches to one physical network, and routers interconnect the networks.

13.3 Protocols for Internetworking

The TCP/IP internet protocols are the most widely used over the Internet.

Layering and TCP/IP protocols are as follows:

The 7-layer RM was devised before internetworking was invented and hence had no layer for internet protocols. The new layering model is as below.

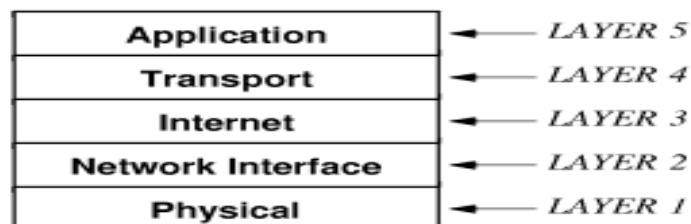


Fig 13.2: The five layers of the TCP/IP reference model

- i. **Physical layer** - corresponds to layer 1 in ISO 7-layer i.e. the basic network interface.
- ii. **Network Interface layer** - specifies how to organize data into frames and how a computer transmits frames over a network.
- iii. **Internet layer** - specifies the format of packets sent across an internet as well as the mechanisms used to forward packets from a computer through one or more routes to a final destination.
- iv. **Transport layer** - like layer 4 in the ISO model, specifies how to ensure reliable transfer.
- v. **Application layer** - like layers 6&7, specifies how one application uses an internet.

Chapter 14: IP: Internet Protocol Addresses

14.1 The goal of internetworking is to provide seamless communication system. The Internet is created entirely by software and the designers are free to choose addresses, packet formats, and delivery techniques independent of the details of the physical hardware. To guarantee uniform addressing for all hosts, protocol software defines an addressing scheme that is independent of the underlying physical addresses. Software uses the destination protocol address when it forwards the packet across the internet to the destination.

14.2 The IP Addressing Scheme

IP standard specifies that each host is assigned a unique 32-bit number known as Internet Protocol Address (IP address). Each 32-bit is divided into two parts, prefix and suffix to provide for IP address hierarchy, meant to make routing efficient. Prefix identifies a particular network and suffix identifies a particular host. The IP address hierarchy guarantees:

- Each computer is assigned a unique address.
- Suffixes can be assigned locally without global coordination.

Note that prefixes must be globally assigned.

14.3 Classes of IP Addresses

A large prefix accommodates many networks but limits hosts and a large suffix accommodates many hosts but limits networks. The compromise was to divide the IP address into three primary classes, each with different prefix and suffix. The first four bits of an address determine the class to which the address belongs, and specify how the remainder of the address is divided into prefix and suffix (pg. 238 of the reference text).

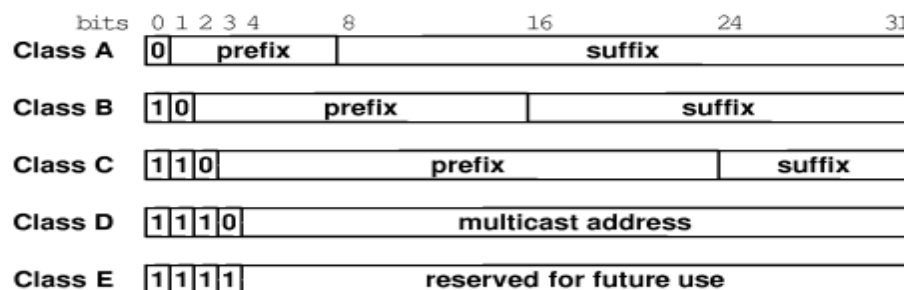


Fig 14.1: The five classes of IP addresses, where addresses assigned to hosts are either class A, B or C. The prefix identifies a network while the suffix is unique to a host on that network.

14.4 Computing the class of an Address

IP software computes the class of the destination address whenever it receives a packet, and IP addresses are termed “self-identifying” because the class of an address can be computed from the address itself. (pg. 239 table 16.2 of the reference text).

First Four Bits Of Address	Table Index (in decimal)	Class of Address
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Fig 14.2: A table that can be used to compute the class of an address. The first four bits of an address are extracted and used as an index into the table.

14.5 Dotted Decimal Notation

It expresses each 8-bit section of a 32-bit number as a decimal value with periods to separate them e.g. 129.52.6.0, for easier human computation. They range from 0.0.0.0 to 255.255.255.255

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

Fig 14.3: Examples of 32-bit binary numbers and their equivalent in dotted decimal notation. Each octet is written in decimal with periods (dots) used to separate the octets.

14.6 Classes and dotted decimal notation

The class must be recognized from the decimal value of the first octet as shown below

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

Fig 14.4: The above figures indicate the range of decimal values found in the first octet of each address class.

14.7 Division of the Address Space

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Fig 14.5: The number of networks and hosts per network in each of the primary IP classes.

NB: The number of hosts or number of networks = 2^n where n is bits in prefix/suffix.

Authority for addresses is obtained from the Internet Assigned Number Authority by service providers. This ensures uniqueness of networks globally. For a private network, the organization concerned determines its own prefixes.

Networks are usually assigned class C addresses unless a class B is needed, while class A is seldom used. (pg. 243 of the reference text for sample addressing).

14.8 Special IP Addresses

Are reserved and can only be used to denote networks or sets of computers. Examples include:

- i. **Network address** – IP reserves host address zero to denote a network e.g. 128.211.0.0 denotes the network of class B assigned prefix 128.211
- ii. **Directed broadcast address** – IP defines this address for each physical network and allows a single copy of packet to be delivered to all hosts on a physical network, it is a suffix of all 1 bits added to the prefix.
- iii. **Limited broadcast address** – consists of all 1 bits and reserved for local network, used during system startup by a computer that does not yet know the network number.
- iv. **THIS computer address** – has address of all zeros to identify “this” computer.
- v. **Loop back address** – tests network applications. Uses class A network prefix 127 (pg. 245 table 16.7)

NB: Routers are also assigned IP address which may be two or more since:

- A router has connections to multiple networks.
- Each IP address contains a prefix that specifies a physical network (pg. 247 fig. 16.8)

Chapter 15: The Future IP (IPv6)

The current IP has worked well over the years, accommodating expansions where necessary. But the primary motivation for change arises from the limited address space. The 32-bit is small and hence larger address spaces are needed to accommodate the exponential growth of the Internet. Secondary motivations include real time delivery of audio and video, new applications that require more complex addressing and routing capabilities e.g. collaborative technologies etc. (see pg. 289, 290 of the recommended text).

IPv6 Addressing

Although it retains most of the features of IPv4, it incorporates lots of changes e.g. all address details are different i.e. addresses do not have defined classes, the boundary between the prefix and suffix can fall anywhere within the address and cannot be determined from the address alone. It does not include a special address for broadcasting. Instead, each IPv6 address falls within three basic types:

Unicast – address corresponds to a single computer.

Multicast – address corresponds to a set of computers possibly at many locations.

Anycast – address corresponds to a set of computers that share a common address prefix e.g. all reside in a single location.

See page 296 of the recommended text.

IPv6 is four times the size of the current IP addressing i.e. $32 \times 4 = 128$ bits

It uses the format shown here called colon hexadecimal notation.

105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

To help reduce the number of characters, IPv6 propose using more compact syntactic form known as colon hexadecimal with a colon separating groups. The above number then reduces to

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

i.e. each group of 16 bits is written in hexadecimal with a colon separating groups.

Colon hex notation requires fewer characters to express an address. An additional optimization known as *zero compression* further reduces the size. Zero compression replaces sequences of zeros with two colons.

Example
FF0C:0:0:0:0:0:0:B1
becomes
FF0C::B1

Chapter 16: TCP: Reliable Transport Service

16.1 Transmission Control Protocol

It uses the unreliable datagram service offered by IP when sending data to another computer, but provides a reliable data delivery service to application programs. It must compensate for loss/delay in an internet to provide efficient data transfer and it must do so without overloading the underlying networks and routers.

16.2 The Services TCP provides to applications

- i. **Connection orientation** – TCP provides connection-oriented service in which an application must first request a connection to a destination and then use the connection to transfer data.
- ii. **p2p communication** – each TCP connection has exactly two end points.
- iii. **Complete reliability** – guarantees that the data sent across a connection will be delivered exactly as sent, with no data missing or out of order.
- iv. **Full duplex communication** – a TCP connection allows data to flow in either direction and allows either application programs to send data at any time. TCP can buffer outgoing and incoming data both ways, making it possible for an application to send data and then continue computation while the data is being transferred.
- v. **Stream interface** – TCP provides a stream interface in which an application sends a continuous sequence of octets across a connection i.e. TCP does not provide a notion of records, and does not guarantee that data will be delivered to receiver in the same size pieces that it was transferred by the sending application.
- vi. **Reliable connection startup** – i.e. applications intending to talk must both agree to such new connection; duplicate packets must not be accepted.
- vii. **Graceful connection shutdown** – it guarantees to deliver all the data reliably before closing the connection.

Connections provided by TCP are called *virtual connections* because they are achieved in software i.e. the TCP software modules on two machines exchange messages to achieve the illusion of a connection. TCP uses IP to carry messages i.e. TCP message is encapsulated in an IP datagram and sent across the Internet (pg. 312 of reference text). TCP must be achieved to achieve reliability which may be compromised by issues e.g. unreliable delivery by the underlying communication system and computer reboots. Such reliability can be achieved through various techniques. One is retransmission. In this case, receiver sends “ack” then it retransmits. This works well for local network but not on long distance connection e.g. satellite the unnecessary traffic consumes network bandwidth and lowers throughput.

The aspect of “adaptive retransmission” makes TCP work more efficiently. In this case, TCP monitors current delay on each connection and adapts i.e. changes the transmission timer to accommodate changing conditions i.e. it estimates round trip delay and builds a weighted average and a variance.

- Using the variance helps TCP to react quickly when delay increases following a burst of packets.

- Using weighted average helps TCP to reset the retransmission timer if the delay returns to lower value after a temporary burst.
- When delay remains constant, TCP adjusts the retransmission timeout to a value that is slightly longer than the mean roundtrip delay.
- When delays start to vary, TCP adjusts the retransmission timeout to a value greater than the mean to accommodate peaks.

16.3 Buffers, Flow Control and Windows

TCP uses a *window* to control the flow of data. Each end allocates a buffer to hold incoming data, and sends the size of the buffer to the other end. The size of buffers available at any time is called a “window” and notification that specifies the window is called “window advertisement” which is sent by the receiver with each acknowledgement (pg. 316 of reference text).

***** *adieu* *****