1.1 Advantages of networks

Computer networking has become one of the most successful ways of sharing information, where all computers are wirelessly linked together by a common network. Now, businesses and organizations heavily rely on it to get messages and information across to essential channels. Not only has that it benefited establishments, but also individuals, as they also need to share important information every day. But no matter how useful computer networking is, it does not come without drawbacks. Here are its advantages:

1. It enhances communication and availability of information.

Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

2. It allows for more convenient resource sharing.

This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

3. It makes file sharing easier.

Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

4. It is highly flexible.

This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

1.2 Structure of the communications network



Types of Communication Networks

Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



(Different Topologies interconnected in a Local Area Network)

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) *Applications of LAN*

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Metropolitan Area Network (MAN)

It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

- 1. System interconnection
- 2. Wireless LANs
- 3. Wireless WANs

System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

Wireless LANs

These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

Wireless WANs

The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

- The first generation was analog and for voice only.
- The second generation was digital and for voice only.
- The third generation is digital and is for both voice and data.



Inter Network

Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.



INTERNETWORK

1.3 Point-to-point and multidrop circuits

Physical Structures

Types of connections:

- 1. Point-to-Point
- 2. Multipoint





b. Multipoint

a) Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

b) Multipoint

A multipoint (also called multi drop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

1.4 Data flow and physical circuits

Data Flow

Circuits can be designed to permit data to flow in one direction or in both directions. Actually, there are three ways to transmit: simplex, half-duplex, and full-duplex.

Simplex is one-way transmission, such as that with radios and TVs.

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) **Half-duplex is two-way transmission,** but you can transmit in only one direction at a time. A half-duplex communication link is similar to a walkie-talkie link; only one computer can transmit at a time.



Figure 3.2 Multipoint circuit



Figure 3.3 Simplex, half-duplex, and full-duplex transmissions

Computers use control signals to negotiate which will send and which will receive data. The amount of time half-duplex communication takes to switch between sending and receiving is called turnaround time (also called retrain time or reclocking time). The turnaround time for a specific circuit can be obtained from its technical specifications (often between 20 and 50 milliseconds). Europeans sometimes use the term simplex circuit to mean a half-duplex circuit.

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) With full-duplex transmission, you can transmit in both directions simultaneously, with no turnaround time.

How do you choose which data flow method to use? Obviously, one factor is the application. If data always need to flow only in one direction (e.g., from a remote sensor to a host computer), then simplex is probably the best choice. In most cases, however, data must flow in both directions.

The initial temptation is to presume that a full-duplex channel is best; however, each circuit has only so much capacity to carry data. Creating a full-duplex circuit means that the available capacity in the circuit is divided—half in one direction and half in the other. In some cases, it makes more sense to build a set of simplex circuits in the same way a set of one-way streets can speed traffic. In other cases, a half-duplex circuit may work best. For example, terminals connected to mainframes often transmit data to the host, wait for a reply, transmit more data, and so on, in a turn-taking process; usually, traffic does not need to flow in both directions simultaneously. Such a traffic pattern is ideally suited to half-duplex circuits.

1.5 Network topologies

Network topology is the geometric representation of the relationship of all the links and linking devices (nodes)



Topology categories



Mesh Topology: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n - 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n - 1)/2 duplex-mode links.

Advantages of Mesh Topology

- A dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry)
Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages of Mesh Topology

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

- First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- ➢ Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- ➢ For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantages of Star Topology

- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others which also makes it easy to install and reconfigure.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages of Star Topology

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

Bus Topology

The preceding examples all describe point-to-point connections. A **bus topology**, on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of Bus Topology

- Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages

- > Disadvantages include difficult reconnection and fault isolation.
- ➤ A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- > Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology

Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

A hybrid topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure below.



A star backbone with three bus networks

1.6 The telephone network, switched and non-switched options

The Public Switched Telephone Network (PSTN) is the global collection of interconnects originally designed to support circuit-switched voice communication. The PSTN provides traditional Plain Old Telephone Service (POTS) - also known as landline phone service - to residences and many other establishments. Parts of the PSTN are also utilized for Internet connectivity services including Digital Subscriber Line (DSL) and Voice over Internet Protocol (VoIP).

PSTN is one of the foundation technologies of telephony - electronic voice communications. While the original forms of telephony including PSTN all relied on analog signaling, modern telephony technologies employ digital signaling, work with digital data, and also support Internet connectivity. The rollout of Internet telephony allows both voice and data to share the same networks, a convergence that the worldwide telecommunications industry is moving toward (for largely financial reasons). A key challenge in Internet telephony is to achieve the same extremely high reliability and quality levels that traditional telephone systems achieved.

History of PSTN Technology

Telephone networks were expanded worldwide during the 1900s as telephones became a routine fixture in homes. Older telephone networks used analog signaling but were gradually upgraded to use digital infrastructure. Most people associate the PSTN with the copper wiring found in many homes although modern PSTN infrastructure also uses fiber optic cables and leaves copper only for the so-called "last mile" of wiring between home and the telecommunication provider's facilitates. The PSTN utilizes the SS7 signaling protocol.

Household PSTN telephones are plugged into wall jacks installed in homes using telephone cords with RJ11 connectors. Residences don't always have jacks in all the right locations, but homeowners can install their own telephone jacks with some basic knowledge of electrical wiring.

One PSTN link supports 64 kilobits per second (Kbps) of bandwidth for data.

The PSTN phone line can be used with traditional dial-up network modems for connecting a computer to the Internet. In the early days of the World Wide Web (WWW), this was the primary form of home Internet access but was made obsolete by broadband Internet services. Dial-up Internet connections supported up 56 Kbps.

PSTN vs. ISDN

Integrated Services Digital Network (ISDN) was developed as an alternative to PSTN that provides both telephone service and also digital data support. ISDN gained popularity in larger businesses due to its ability to support large numbers of phones with low installation costs. It was also offered to consumers as an alternative form of Internet access supporting 128 Kbps.

PSTN vs. VoIP

Voice over Internet Protocol (VoIP), sometimes also called IP telephony, was designed to replace the circuit-switched phone services of both PSTN and ISDN with a packet switched system based on Internet Protocol (IP). The first generations of VoIP services suffered from reliability and sound quality issues but have gradually improved over time.

1.7 Connecting the analog and digital worlds

Analog and Digital

Both data and the signals that represent them can be either **analog or digital** in form.

Analog and Digital Data

Data can be analog or digital. The term **analog data** refers to information that is continuous; **digital data** refers to information that has discrete states. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Analog and Digital Signals

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B*, it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O.

The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. The following figure illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.



Periodic and Non-periodic Signals

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic or non-periodic

PERIODIC ANALOG SIGNALS

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves A sine wave



We can mathematically describe the sine wave as

where, s is the instantaneous amplitude

- A is the peak amplitude
- f is the frequency
- φ is the phase
- t is the time
- π is a constant (~3.14159)

Two signals

Same phase and frequency, but different amplitudes



Period and frequency

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

• Denoted by *T*, measured in seconds.

Frequency refers to the number of periods in one second

• Denoted by *f*, measured in Hertz (Hz)

Note

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry)

Frequency and period are the inverse of each other.

$$f = \frac{1}{T}$$
 and $T = \frac{1}{f}$

Units of period and frequency

Unit	Equivalent	Unit	Equivalent
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10 ⁻³ s	Kilohertz (kHz)	10 ³ Hz
Microseconds (µs)	10 ⁻⁶ s	Megahertz (MHz)	10 ⁶ Hz
Nanoseconds (ns)	10 ⁻⁹ s	Gigahertz (GHz)	10 ⁹ Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10 ¹² Hz

More about frequency

- Frequency is the rate of change with respect to time.
- Change in a short span of time means high frequency.
- Change over a long span of time means low frequency.

Two extremes

- If a signal does not change at all, its frequency is zero.
- If a signal changes instantaneously, its frequency is infinite.

Phase

Phase describes the position of the waveform relative to time 0.

Three sine waves

Same amplitude and frequency, but different phases



M.THILLAINAYAKI

Wavelength and period

Wavelength is another characteristic of a signal traveling through a transmission medium.

- The wavelength depends on both the frequency and the medium.
- The wavelength is the distance a signal can travel in one period.



Time-domain and frequency-domain plots of a sine wave



A complete sine wave in the time domain can be represented by one single spike in the frequency domain.

Example

The frequency domain is more compact and useful when we are dealing with more than one sine wave. For example, the following figure shows three sine waves, each with different amplitude and frequency. All can be represented by three spikes in the frequency domain.





a. Time-domain representation of three sine waves with frequencies 0, 8, and 16



Composite signals

A single-frequency sine wave is not useful in data communications; we need to send a composite signal, a signal made of many simple sine waves.

We can use a mathematical technique called **Fourier analysis** to show that any **periodic** signal is made up of an infinite series of sinusoidal frequency components.

If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.

Example

The figure shows a periodic composite signal with frequency f. This type of signal is not typical of those found in data communications. We can consider it to be three alarm systems, each with a different frequency. The analysis of this signal can give us a good understanding of how to decompose signals.



Decomposition of a composite periodic signal in the time and frequency domains



b. Frequency-domain decomposition of the composite signal

Example

The figure shows a nonperiodic composite signal. It can be the signal created by a microphone or a telephone set when a word or two is pronounced. In this case, the composite signal cannot be periodic, because that implies that we are repeating the same word or words with exactly the same tone.



1.8 Bandwidth

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

The bandwidth of periodic and non periodic composite signals



a. Bandwidth of a periodic signal



b. Bandwidth of a nonperiodic signal

1.9 DIGITAL SIGNALS

In addition to being represented by an analog signal information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case,, we can send more than 1 bit for each level.

Two digital signals: one with two signal levels and the other with four signal levels





Bit Rate

Most digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics. Another *term-bit rate* (instead *ofjrequency*)-*is* used to describe digital signals. The bit rate is the number of bits sent in Is, expressed in bits per second (bps). Figure 3.16 shows the bit rate for two signals.

The time and frequency domains of periodic and nonperiodic digital Signals



a. Time and frequency domains of periodic digital signal



b. Time and frequency domains of nonperiodic digital signal

Baseband transmission



A digital signal is a composite analog signal with an infinite bandwidth.

Bandwidths of two low-pass channels



a. Low-pass channel, wide bandwidth



b. Low-pass channel, narrow bandwidth

Baseband transmission using a dedicated medium

Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth.

Input signal bandwidth Bandwidth supported by medium Output signal bandwidth



Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth.

Broadband Transmission:

In broadband transmission the signal is converted to analog for transmission. Bandwidth of a bandpass channel

If the available channel is a bandpass channel, we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) Amplitude



Modulation of a digital signal for transmission on a bandpass channel



Example

An example of broadband transmission using modulation is the sending of computer data through a telephone subscriber line, the line connecting a resident to the central telephone office. These lines are designed to carry voice with a limited bandwidth. The channel is considered a bandpass channel.

We convert the digital signal from the computer to an analog signal, and send the analog signal. We can install two converters to change the digital signal to analog and vice versa at the receiving end. The converter, in this case, is called a **modem**.

Data Rate Limits:

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

- 1. The bandwidth available
- 2. The level of the signals we use
- 3. The quality of the channel (the level of noise)
- Noiseless channel: Nyquist bit rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

 $C = 2 B \log 2L$

where, C is the channel capacity or bit rate in bps

- B is the bandwidth in Hz
- L is the number of signal levels used to represent data

Noisy channel: Shannon capacity

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) In reality, we cannot have a noiseless channel; In this case, the Shannon capacity formula is used to determine the theoretical highest data rate for a noisy channel:

 $C = B \log 2 (1+SNR)$

where, C is the capacity of the channel in bps

B is the bandwidth in Hz SNR is the signal-to-noise ratio

PERFORMANCE

One important issue in networking is the performance of the network—how good is it? We discuss quality of service, an overall measurement of network performance

Bandwidth

In networking, we use the term bandwidth in two contexts.

- The first, bandwidth in hertz, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.
- The second, bandwidth in bits per second, refers to the speed of bit transmission in a channel or link.

Throughput

The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data. For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Imagine a highway designed to transmit 1000 cars per minute from one point to another. However, if there is congestion on the road, this figure may be reduced to 100 cars per minute. The bandwidth is 1000 cars per minute; the throughput is 100 cars per minute.

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

$$Propagation time = \frac{Distance}{Propagation speed}$$

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the 25 ignal For example, in a vacuum, light is propagated with a speed of 3×108 mfs. It is lower in air; it is much lower in cable.

Queuing Time

The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor; it changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues they arrived messages and processes them one by one. If there are many messages, each message will have to wait.

1.12 Digital worlds - digital signals

Digital to Digital Conversion:

In this section, we see how we can represent digital data by using digital signals. The conversion involves three techniques: line coding, block coding, and scrambling. Line coding is always needed; block coding and scrambling mayor may not be needed.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in digital format, which is binary bits. It is represented (stored) internally as series of 1s and 0s.



Line Coding

Digital signals which represents digital data, represented as discrete signals. There are three types of line coding schemes available:

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry)



Uni-Polar Encoding

Unipolar encoding schemes uses single voltage level to represent data. In this case, to represent binary 1 high voltage is transmitted and to represent 0 no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there's no rest condition i.e. it either represents 1 or 0.



Polar Encoding

Polar encoding schemes multiple voltage levels are used to represent binary values. Polar encodings are available in four types:

Polar-NRZ (Non-Return To Zero)

It uses two different voltage levels to represent binary values, generally positive voltage represents 1 and negative value represents 0. It is also NRZ because there's no rest condition. NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L and NRZ-I

NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

RZ (Return to Zero)

Problem with NRZ was the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



Return-to-Zero Encoding

RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

Manchester

This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transitions at the middle of the bit and changes phase when a different bit is encountered.

Differential Manchester

This encoding scheme is a combination of RZ and NRZ-I. It also transitions at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry)

Bipolar Encoding

Block Coding

To ensure accuracy of data frame received, redundant bits are used. For example, in even parity one parity bit is added to make the count of 1s in the frame even. This way the original number of bits are increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB, that is m-bit block is substituted with nbit block where n > m. Block coding involves three steps: division, substitution and combination. After block coding is done it is line coded for transmission.

Analog-to-digital conversion

Microphones creates analog voice and camera creates analog videos, which here in our case is treated is analog data. To transmit this analog data over digital signals we need an analog to digital conversion.

Analog data is wave form continuous stream of data whereas digital data is discrete. To convert analog wave into digital data we use Pulse Code Modulation.

Pulse Code Modulation:

Pulse Code Modulation is one of the most commonly used method to convert analog data into digital form. It involves three steps: Sampling, Quantization and Encoding.

Sampling



Sampling of Analog Signal

The analog signal is sampled every T interval. Most important factor in sampling is the rate on which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Quantization of sampled analog signal

Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding



Encoding from quantization

In encoding, each approximated value is then converted into binary format.

1.13 The modem, asynchronous and synchronous transmission.

Data is transmitted between communication devices in multiples of fixed-length units, typically 8-bits. For example, if the computer is transferring a source program, the data will be made up of a block of 8-bit binary-encoded characters. On the other hand, if the data is in the form of a compiled object code of the program, the data will be made up of a block of 8-bit bytes. At the receiving end, the following parameters are determined to decode and interpret the message correctly.



1.14 Wide area and local networks, connection oriented and connectionless networks

Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are :

- 1. Connection is established
- 2. Information is sent
- 3. Connection is released

In connection oriented service we have to establish a connection before starting the communication. When connection is established we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Difference between Connection oriented service and Connectionless service

- 1. In connection oriented service authentication is needed while connectionless service does not need any authentication.
- 2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs connectionless service protocol does not guarantees a delivery.
- 3. Connection oriented service is more reliable than connectionless service.
- 4. Connection oriented service interface is stream based and connectionless is message based.

Service Primitives

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets. The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connection-less service. There are five types of service primitives :

- 1. **LISTEN :** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
- 2. **CONNECT :** It connects the server by establishing a connection. Response is awaited.
- 3. **RECIEVE:** Then the RECIEVE call blocks the server.
- 4. **SEND**: Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
- 5. **DISCONNECT** : This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

Connection Oriented Service Primitives

There are 5 types of primitives for Connection Oriented Service :

LISTEN	Block waiting for an incoming connection
CONNECTION	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Sending a message to the peer
DISCONNECT	Terminate a connection

Connectionless Oriented Service Primitives

There are 4 types of primitives for Connectionless Oriented Service:

UNIDATA	This primitive sends a packet of data
FACILITY,	Primitive for enquiring about the performance of the network, like delivery
REPORT	statistics.

Relationship of Services to Protocol

Services

These are the operations that a layer can provide to the layer above it. It defines the operation and states a layer is ready to perform but it does not specify anything about the implementation of these operations.



Protocols

These are set of rules that govern the format and meaning of frames, messages or packets that are exchanged between the server and client.

1.15 Classification of communications protocols

Communication protocols are formal descriptions of digital message formats and rules. They are required to exchange messages in or between computing systems and are required in telecommunications.

Communications protocols cover authentication, error detection and correction, and signaling. They can also describe the syntax, semantics, and synchronization of analog and digital communications. Communications protocols are implemented in hardware and software. There are thousands of communications protocols that are used everywhere in analog and digital communications. Computer networks cannot exist without them.

Communications devices have to agree on many physical aspects of the data to be exchanged before successful transmission can take place. Rules defining transmissions are called protocols.

There are many properties of a transmission that a protocol can define. Common ones include: packet size, transmission speed, error correction types, handshaking and synchronization techniques, address mapping, acknowledgement processes, flow control, packet sequence controls, routing, address formatting

Popular protocols include:

- 1. File Transfer Protocol (FTP),
- 2. TCP/IP,
- 3. User Datagram Protocol (UDP),
- 4. Hypertext Transfer Protocol (HTTP),
- 5. Post Office Protocol (POP3),
- 6. Internet Message Access Protocol (IMAP),
- 7. Simple Mail Transfer Protocol (SMTP).

1.16 Time division multiple access (TDMA), time division multiplexing (TDM), carrier sense (Collision) systems, token passing, peer-to-peer priority systems; priority slot, carrier

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) sense (collision free) systems, token passing (priority) systems.

In TDMA, the bandwidth of channel is dividend amongst various stations on the basis of time.

• Each station is allocated a time slot during which it can sent its data *i.e.* each station can transmit its data in its allocated time slot only.

- Each station must know the beginning of its slot and the location of its slot.
- TDMA requires synchronization between different stations.

• Synchronization is achieved by using some synchronization bits (preamble bits) at the beginning of each slot.

• TDMA is different from TDM, although they are conceptually same.

• TDM is a physical layer technique that combines the data from slower channels and transmits then by using a faster channel. This process uses physical multiplexer.

• TDMA, on other hand, is an access method in the data link layer. The data link layer in each station tells its physical layer to use the allocated time slot. There is no physical multiplexer at the physical layer.



For digital sources, two alternative technologies have evolved for multiplexing. These are **Time Division Multiplexing** (*TDM*) and Code division Multiplexing (CDM). TDM provides a way to merge data from several sources into a single channel for communication over telephone lines, a microwave system or a satellite system. TDM can be implemented in two ways. These are

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) synchronous TDM and asynchronous TDM. Asynchronous TDM is popularly known as Statistical TDM.

In synchronous TDM, a single channel is divided into time slots and each transmitting device is assigned at least one of the time slots for *its* transmission



Time slots are assigned in such a way that each transmitting device gets its required share of the available bandwidth. 'Because of this time-bandwidth multiplexing technique, TDMs are protocol insensitive and are capable of combining various protocols onto a single high-speed transmission link. In other words, we can say that multiplexer allocates exactly-the same time slot to each device at all times whether the device is active or idle.

Some devices such as voice and video systems may require more slots to ensure that data arrives at the distant link-end without becoming distorted from slower data rates. These different time slots are grouped into frames. A frame consists of one complete cycle of time slots.



Alternatively, Figure explains more clearly the concept of TDM in a data communication environment where three PCs are sharing the common circuit. The packets generated by each PC are multiplexed on the common line as A1, B1, and C1 and so on.
Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) It is more flexible than the FDM unlike FDM. the whole bandwidth for a certain amount of time is provided to the user. All the users are using the same frequency but at a different time. This time allotment may be varied as per the requirement and priority of the users' services. In the Figure spaces between different time slots are shown, these are known as guard spaces in time dimension. These are used to eliminate co-channel interference.

The main disadvantage of this scheme is that a precise synchronization between different senders is necessary to avoid co-channel interference.

The **Token-Passing Protocol** relies on a control signal called the token. A token is a 24-bit packet that circulates throughout the network from NIC to NIC in an orderly fashion. If a workstation wants to transmit a message, first it must seize the token. At that point, the workstation has complete control over the communications channel. The existence of only one token eliminates the possibility of signal collisions. This means that only one station can speak at a time.

Logical Ring Physical Star topology for Token-Passing Standard.

It is sure that any break in the ring at any point will interrupt communications for all machines. To solve this problem, IBM developed a modified ring topology, which they called the logical ring physical star. The central point of the physical star configuration is Token Ring hub called the multi-station access unit (MSAU, pronounced as masow).

Workstations and servers attached to the MSAU through special STP adapter cables. IBM converted stars into a logical ring by connecting all MSAU hubs together through special ring-in (RI) and ring-out (RO) ports.

Advantages of Token Ring.

Here are Token ring's most useful advantages:

a. It offers excellent throughput under high-load conditions.

b. Token Ring facilitates LAN-to-LAN mainframe connections especially for interfacing with IBM's broader connectivity strategies.

c. It has built-in troubleshooting mechanisms such as beaconing and auto-reconfiguration and may now be used with UTP cabling.

d. It has the most reliable protocol (token-passing), the most trouble-free configuration (physical star) and the fastest connectivity scheme (r or 16 mb/s).

Unit – 1 Introduction to Computer Network Computer Networks Year(PG 2017-2018 Lateral Entry) **Disadvantages of Token Ring.**

Few of the disadvantages of Token Ring are:

a. Token Ring is very expensive. All topology components cost much more than other more popular standards.

b. It is relatively proprietary. Token Ring's complexity is built into the hardware components. This means hat you need to choose a manufacturer and stick with it.

c. Engineers must have considerable expertise to manage and troubleshoot token ring components.

	Karpagam Academy of Higher Education						
	Department of Computer Applications						
	BCA (2018-2021 Batch)						
	ADVANCED NETWORKING (18CAU303)						
		UN	IIT- I				
S.No	Question	Option1	Option2	Option3	Option4	Answer	
1	A is a set of devices conneted by a communication links	process	network	topology	protocol	network	
2	Any device that connected to a network is referred as	node	client	server	link	node	
3	LAN stands for	Local Access Network	Local Area Network	Local Architect ure Network	Local Addressing Network	Local Area Network	
4	is the set of rules.	protocol	communica tion	network	topology	protocol	
5	Multipoint connection is also referred as	point-to- point	multidrop	multi node	multilink	multidrop	
6	In a star topology , each device has a dedicated point to point link only to a central controller called	repeater	controller	hub	router	hub	
7	Full duplex mode is also referred as	duplex	half-duplex	simplex	half- simplex	hub	
8	Aconnection provides a dedicated link between two devices.	point-to- point	multi-point	multidrop	physical	point-to- point	
9	A connection is one in which more than two specific devices share a single link	point-to- point	multi-point	multilink	dedicated	multi-point	
10	In topology, every device has a dedicated point-to-oint link to every other device	bus	mesh	star	ring	mesh	
11	In topology one long cable acts as a backbone to link all the devices in a network.	bus	mesh	star	ring	bus	

S.No	Question	Option1	Option2	Option3	Option4	Answer
12	Combination of more than one topologies is called	bus	mesh	hybrid	star	hybrid
13	size is limited to few kilometers	MAN	LAN	WAN	Internet	LAN
14	NIC stands for	Network Interface Card	Network Informatio n Centre	Network Interface Centre	Network Informatio n Card	Network Interface Card
15	There are layers in ISO OSI model	4	5	6	7	7
16	The physical layer coordinates the functions required to carry a over a physical medium	frame	packet	segment	bit stream	bitstream
17	The layer coordinates the functions required to carry a bitstream over a physical medium.	datalink	physical	applicatio n	session	physical
18	Hop to hop delivery is done by the	session layer	datalink layer	network layer	transport layer	datalink layer
19	Thelayer is responsible for process to process delivery.	physical	presentatio n	network	transport	transport
20	Thelayer is responsible for dialog control and synchronization.	transport	session	applicatio n	presentatio n	session
21	The layer is responsible for the souce to destination delivery of a packets.	physical	network	transport	presentatio n	network
22	The layer is responsible for process to process delivery.	transport	session	applicatio n	presentatio n	transport
23	The layer is concerned with the syntax and semantics of the information exchanged between two systems.	physical	network	transport	presentatio n	physical
24	There are layers in TCP/IP Protocol Suite	4	5	6	7	4
25	TCP/IP is aprotocol.	hyper text	transfer	internet	hierarchical	hierarchical
26	TCP stands for	Transfer Control Protocol	Transmissio n Control Protocol	Transport Control Protocol		

S.No	Question	Option1	Option2	Option3	Option4	Answer
27	OSI stands	open	open	open	open	open
	tor	systems	system	symantic	system	systems
		interconn	internetwo	interconn	internet	interconne
		ection	rking	ection		ction
28	Network layer delivers	frame	bits	data	раскет	packet
	data in the form					
20	OT	0.00	+	three	four	+11/0
29	session layer	one	two	three	Tour	two
	services					
30	ARP stands for	Address	Access	Access	Address	Address
50		Resolutio	Resolution	Resource	Resolution	Resolution
		n	Prototype	Protocol	Prototype	Protocol
		Protocol	i i ococype	11000001	i i ototype	11000001
31	is used to	ARP	RARP	ICMP	IGMP	ARP
	associate a logical					
	address with a physical					
	address					
32	RARP stands for	Reverse	Revised	Repeat	Random	Reverse
		Address	Access	Access	Address	Address
		Resolutio	Resolution	Resource	Resolution	Resolution
		n	Prototype	Protocol	Prototype	Protocol
		Protocol				
33	allows a host to	ARP	RARP	ICMP	IGMP	RARP
	discover its Internet					
	address when it knows					
24	ICMP stands for	Interface	Internet	Interface	Internet	Internet
54		Control	Control	Control	Control	Control
		Message	Message	Medium	Medium	Message
		Protocol	Protocol	Protocol	Protocol	Protocol
35	sends guery	ARP	RARP	ICMP	IGMP	ICMP
	and error reporting					
	messages					
36	IGMP stands for	Interface	Internet	Interface	Internet	Internet
		Group	Group	Gateway	Gateway	Group
		Message	Message	Medium	Medium	Message
		Protocol	Protocol	Protocol	Protocol	Protocol
37	provides	SCTP	SMTP	ICMP	IGMP	SCTP
	support for newer					
	applications such as voice					
	over Internet					
38	UDP	user data	user	user	user	user
		protocol	datagram	defined	dataframe	datagram
20		filo	file	file	flip transfer	file transfer
39	FIP	transmit	transmissio	transfor	nip transfer	nie transfer
		nrotocol	n protocol	nrotocol	protocor	ριστοςοι
40	The first sten in PCM is	samnling	quantizing	encoding	decoding	sampling
		5000 P	99911021118	cheoding	accounts	Samhing
		1		1	1	

S.No	Question	Option1	Option2	Option3	Option4	Answer
41	SMTP	single mail transfer protocol	simple mail transfer protocol	simple mail transmissi on protocol	single mail transmit protocol	simple mail transfer protocol
42	Complete a cycle is called as	period	frequency	non periodic	periodic	period
43	A MAN is a network with a size between a and	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
44	Thelayer is responsible for providing services to the user.	presentati on	datalink	applicatio n	network	application
45	The layer is responsible for translation, compression encryption.	transport	data link	presentati on	application	presentatio n
46	does not define any specific protocol.	ТСР	НТТР	TCP/IP	SMTP	TCP/IP
47	The TCP/IP protocol suite was developed prior to themodel.	OSI	ISO	ТСР	IP	OSI
48	How many sampling methods are available?	2	3	4	5	3
49	PCM stands for	Pulse Coding Modulati on	Pulse Coded Modulation	Pulse Code Modulati on	Pulse Card Modulation	Pulse Code Modulation
50	The process is referred as pulse amplitude modulation	sampling	quantizing	encoding	decoding	sampling
51	PAM stands for	Pulse Amplitud e Modulati on	Pulse Amplified Modulation	Pulse Amplify Modulati on	Pulse Amplifing Modulation	Pulse Amplitude Modulation
52	The signals which are obtained by encoding each quantized signal into a digital word is called as	PAM signal	PCM Signal	FM signal	sampling & quantizatio n	PCM Signal
53	prvides synchronization without increasing the number of bits	sampling	quantizing	encoding	scrambling	scrambling

2.1 Goals of Layered Protocols

The **Open Systems Interconnection model** (**OSI model**) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a *horizontal* connection in that layer.

The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

2.2 The OSI model, standards organizations, Layers of OSI, OSI status.

OSI Model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to world wide agreement on international standards.

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Seven layers of the OSI model



Peer-to-peer processes



Physical communication

Encapsulation



- The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a header is added to the data unit.
- At layer 2, a trailer is added as well.
- When the formatted data unit passes through the physical layer (layer 1) it is changed into an electromagnetic or optical signal and transported along a physical link
- At the destination the reverse process is performed

THE OSI MODEL AND LAYERS

In this section we briefly describe the functions of each layer in the OSI model. **Physical Layer**





- The physical layer is responsible for movements of individual bits from one hop (node) to the next
- Mechanical and electrical specification, the procedures and functions

Duties:

- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

Data link layer

- The data link layer is responsible for moving frames from one hop (node) to the next
- Transform the physical layer to a reliable (error-free) link





Network layer



The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Duties:

- Logical addressing
- Routing

Source-to-destination delivery



Transport layer



The transport layer is responsible for the delivery of a message from one process to another. Duties:

- Service-point (port) addressing
- Segmentation and reassembly
- Connection control

Session layer

- Flow control
- Error control

Reliable process-to-process delivery





The session layer is responsible for dialog control and synchronization.



The presentation layer is responsible for translation, compression, and encryption.

Application layer



The application layer is responsible for providing services to the user.

Services:

- Network virtual terminal
- Mail services
- File transfer, access, and management
- Directory services

The TCP/IP Reference Model:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.

2. To survive after partial subnet hardware failures.

3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer

- 2. Internet Layer
- 3. Transport Layer

4. ApplicationLayerApplicationLayerTransportLayerInternet LayerHost-to-Network LayerLayer

Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Internet Layer:

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. Fig. shows this correspondence.

The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.



Fig.1: The TCP/IP reference model.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since the model was developed, IP has been implemented on many other networks.



Fig.2: Protocols and networks in the TCP/IP model initially.

The Application Layer:

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The

virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

2.3 Local Area Networks

Why LANs?

In the modern office environment, each worker is equipped with a personal computer, containing its own disk drives and processor. Each of these computers can communicate with another by the way of a local area network (LAN), which is a computer network that covers a small area, usually a single building or group of buildings. In addition, the LAN may also connect the network of computers with a series of printers, a mainframe computer or file server with even greater processing power and memory storage, and with other devices that can send messages from the network over telephone lines to another location.

As the name suggests, a LAN is local, meaning that it is a proprietary system limited to a finite number of users. It generally serves an area of less than one mile. It is also a network, affording users both functional and communicative diversity through a distribution of resources. A LAN permits workers—isolated in separate offices—to operate off the same system, as if they were all sitting around a single computer.

One of the great attributes of a LAN is that it may be installed simply, upgraded or expanded with little difficulty, and moved or rearranged without disruption. LANs are also useful because they can transmit data quickly. Perhaps most importantly, anyone familiar with the use of a personal computer can be trained to communicate or perform work over a LAN. But despite their great potential and capabilities, LANs have yet to demonstrate an increase in office productivity. They have certainly eliminated paper and speeded the flow of information, but in many cases they have also created additional work in terms of organization, maintenance, and trouble-shooting.

THE HISTORY OF LANS

The advent of personal computers changed the type of information sent over office computer networks. Terminals were no longer "dumb," but contained the power to perform their own

instructions and maintain their own memories. This took considerable pressure off mainframe devices, whose energies could now be devoted to more complex tasks.

LANs allowed for the transmission of data between workers. In turn, they enabled this shared data to be directed to a common printer, serving a larger group of users. This eliminated the need for each worker to have a printer and ensured that the one printer provided was not underutilized. In addition, LANs allowed data to be called up directly on other workers' computers, providing immediate communication and eliminating the need for paper. The most common application was in interoffice communications, or electronic mail (e-mail). Messages could be directed to one or several people and copied to several more over the LAN. As a result, an e-mail system became something of an official record of communications between workers. Addressees became obligated to respond to e-mail messages in a timely manner because their failure to answer could be easily documented for supervisors.

Personal computers transformed LANs from mere shared processors to fully integrated communication devices. With processing power distributed among several computers, the mainframe's main role was eclipsed and complex processing, administrative functions, and data file storage became the job of a new device, the file server. Today, there are many different types of LANs. For example, many Macintosh computers use Appletalk, while IBM computers commonly use Ethernets.

PHYSICAL COMPONENTS OF LANS

The physical properties of a LAN include network access units (or interfaces) that connect the personal computer to the network. These units are actually interface cards installed on computer motherboards. Their job is to provide a connection, monitor availability of access to the LAN, set or buffer the data transmission speed, ensure against transmission errors and collisions, and assemble data from the LAN into usable form for the computer.

The next part of a LAN is the wiring, which provides the physical connection from one computer to another, and to printers and file servers. The properties of the wiring determine transmission speeds. The first LANs were connected with coaxial cable, the same type used to deliver cable television. These facilities are relatively inexpensive and simple to attach. More importantly, they provided great bandwidth (the system's rate of data transfer), enabling transmission speeds initially up to 20 megabits per second.

Another type of wiring, developed in the 1980s, used ordinary twisted wire pair (commonly used for telephones). The primary advantages of twisted wire pair are that it is very cheap, simpler to splice than coaxial, and is already installed in many buildings. The downside of this simplicity is that its bandwidth is more limited.

A more recent development in LAN wiring is optical fiber cable. This type of wiring uses thin strands of glass to transmit pulses of light between terminals. It provides tremendous bandwidth, allowing very high transmission speeds and because it is optical rather than electronic, it is impervious to electromagnetic interference. Still, splicing it can be difficult and requires a high degree of skill. The primary application of fiber is not between terminals, but between LAN buses (terminals) located on different floors. As a result, fiber distributed data interface is used mainly in building risers. Within individual floors, LAN facilities remain coaxial or twisted wire pair.

When a physical connection cannot be made between two LANs, such as across a street or between buildings, microwave radio may be used. However, it is often difficult to secure frequencies for this medium. Another alternative in this application is light transceivers, which project a beam of light similar to fiber optic cable, but through the air rather than over cable. These systems do not have the frequency allocation or radiation problems associated with microwave, but they are susceptible to interference from fog and other natural obstructions.

LAN TOPOLOGIES

LANs are designed in several different topologies, or physical patterns, connecting terminals. These shapes can range from straight lines to a ring. Each terminal on the LAN contends with other terminals for access to the system. When it has secured access to the system, it broadcasts its message to all the terminals at once. The message is picked up by the one or group of terminal stations for which it is intended. The branching tree topology is an extension of the bus, providing a link between two or more buses.

A third topology, the star network, also works like a bus in terms of contention and broadcast. But in the star, stations are connected to a single, central node (individual computer) that administers access. Several of these nodes may be connected to one another. For example, a bus serving six stations may be connected to another bus serving 10 stations and a third bus connecting 12 stations. The star topology is most often used where the connecting facilities are coaxial or twisted wire pair.

The ring topology connects each station to its own node, and these nodes are connected in a circular fashion. Node 1 is connected to node 2, which is connected to node 3, and so on, and the final node is connected back to node 1. Messages sent over the LAN are regenerated by each node, but retained only by the addressees. Eventually, the message circulates back to the sending node, which removes it from the stream.

TRANSMISSION METHODS USED BY LANS

LANs function because their transmission capacity is greater than any single terminal on the system. As a result, each station terminal can be offered a certain amount of time on the LAN, like a timesharing arrangement. To economize on this small window of opportunity, stations organize their messages into compact packets that can be quickly distributed. When two messages are sent simultaneously, they could collide on the LAN causing the system to be temporarily disrupted. Busier LANs usually utilize special software that virtually eliminates the problem of collisions by providing orderly, non-contention access.

The transmission methods used on LANs are either baseband or broadband. The baseband medium uses a high-speed digital signal consisting of square wave DC voltage. While it is fast, it can accommodate only one message at a time. As a result, it is suitable for smaller networks where contention is low. It also is very simple to use, requiring no tuning or frequency discretion circuits. This transmission medium may be connected directly to the network access unit and is suitable for use over twisted wire pair facilities.

By contrast, the broadband medium tunes signals to special frequencies, much like cable television. Stations are instructed by signaling information to tune to a specific channel to receive information. The information within each channel on a broadband medium may also be digital, but they are separated from other messages by frequency. As a result, the medium generally requires higher capacity facilities, such as coaxial cable. Suited for busier LANs, broadband systems require the use of tuning devices in the network access unit that can filter out all but the single channel it needs.

THE FILE SERVER

The administrative software of the LAN resides either in a dedicated file server; in a smaller, less busy LAN; or in a personal computer that acts as a file server. In addition to performing as a kind of traffic controller, the file server holds files for shared use in its hard drives, administers applications such as the operating system, and allocates functions.

When a single computer is used as both a workstation and a file server, response times may lag because its processors are forced to perform several duties at once. This system will store certain files on different computers on the LAN. As a result, if one machine is down, the entire system may be crippled. If the system were to crash due to undercapacity, some data may be lost or corrupted.

The addition of a dedicated file server may be costly, but it provides several advantages over a distributed system. In addition to ensuring access even when some machines are down, its only duties are to hold files and provide access.

OTHER LAN EQUIPMENT

LANs are generally limited in size because of the physical properties of the network including distance, impedance, and load. Some equipment, such as repeaters, can extend the range of a LAN. Repeaters have no processing ability, but simply regenerate signals that are weakened by impedance. Other types of LAN equipment with processing ability include gateways, which enable LANs operating dissimilar protocols to pass information by translating it into a simpler code, such as ASCII. A bridge works like a gateway, but instead of using an intermediate code, it translates one protocol directly into another. A router performs essentially the same function as a bridge, except that it administers communications over alternate paths. Gateways, bridges, and routers can act as repeaters, boosting signals over greater distances. They also enable separate LANs located in different buildings to communicate with each other.

The connection of two or more LANs over any distance is referred to as a wide area network (WAN). WANs require the use of special software programs in the operating system to enable dial-up connections that may be performed by a telephone lines or radio waves. In some cases, separate LANs located in different cities—and even separate countries—may be linked over the public network.

LAN DIFFICULTIES

LANs are susceptible to many kinds of transmission errors. Electromagnetic interference from motors, power lines, and sources of static, as well as shorts from corrosion, can corrupt data. Software bugs and hardware failures can also introduce errors, as can irregularities in wiring and connections. LANs generally compensate for these errors by working off an uninterruptable power source, such as batteries, and using backup software to recall most recent activity and hold unsaved material. Some systems may be designed for redundancy, such as keeping two file servers and alternate wiring to route around failures.

Security problems can also be an issue with LANs. They can be difficult to manage and access because the data they use is often distributed between many different networked sources. In addition, many times this data is stored on several different workstations and servers. Most companies have specific LAN administrators who deal with these issues and are responsible for the use of LAN software. They also work to backup files and recover lost files.

Primary attributes of a LAN

AN's main function is to provide resource sharing and mutual communication, which provides the following main services:

- The sharing of resources, including hardware resource sharing, file sharing, and software inventory data sharing. Users can share a network system software and application software.
- **Data transfer and e-mail**: Data and network file transfer is an important feature of modern LANs not only transmit files, data, information, but also can send voice, images.
- **Improve the reliability** of the computer system. LAN computers can back each other, avoiding the stand-alone system without backup failure may occur when system failures, greatly improving the reliability of the system, particularly in the industrial process control, real-time data processing and other applications, is particularly important.
- **Easy to distributed processing**: Use of network technology you can have more than one computer connected to a high-performance computer system (Server) through a certain algorithm, the larger global issues points to a different computer to complete.

Broadband and baseband and base LANs

Broadband A communications medium that can carry a wide range of signal frequencies, typically from audio up to video frequencies. In telecommunications the significance of a broadband system is that it can carry television and videoconferencing data as well as voice calls. A broadband medium can be made to carry many signals at once by apportioning its total bandwidth into many independent channels, each of which carries only a specific range of frequencies. In contrast, a BASEBAND can carry only a single channel. ATM, ADSL and Cable TV are all broadband media, while standard ISDN barely qualifies.

There exist two LAN transmission options, Baseband and Broadband. Baseband LANs, which is the most prevalent by far, is a Single-channel system that supports a single transmission at any given time.

Broadband LANs, which are most unusual, support multiple transmissions via multiple frequency channels.

Broadband LANs



Broadband LANs are Multichannel, analog LANs as shown in Figure. typically based on coaxial cable as the transmission medium, although fiber optic cable is also used. Individual channels offer bandwidth of 1 to 5 Mbps, with 20 to 30 channels typically supported. Aggregate bandwidth is as much as 500 MHz. Its characteristics are:

- Digital signal modulated onto RF carrier (analog)
- Channel allocation based on FD M
- Head-End for bidirectional transmission

• Stations connected via RF modems, Le. radio modems accomplish the digital-to-analog conversion process, providing the transmitting device access to an analog channel.

Advantages

Data, voice and video can be accommodated on broadband channel

- Greater distances
- Greater bandwidth.

Disadvantages

- Cable design
- Alignment and maintenance
- High cost, requires modems
- Lack of well-developed standards.

Some broadband LANs are referred to as IOBroadband36 where 10stands for 10Mbps, Broadband for multichannel and 36 for 3600 meters maximum separation between devices.

Baseband LANs

Baseband LAN is single channel, supporting a single communication at a time as shown in Figure. They are digital in nature. Total bandwidth of I to 100Mbps is provided over coaxial cable, UTP, STP, or fiber optic cable. Distance limitations depend on the medium employed and

the specifics of the LAN protocol. Baseband LAN physical topologies including ring, bus, tree, and star.

Baseband LANs are by far the most popular and the most highly standardized. Ethernet, Token Passing, Token Ring and FDDI LANs are all baseband. They are intended only for data, as data communications is, after all, the primary reason for the existence of LANs. The characteristics of this system may be summarized as follows:

- Unmodulated digital signal
- Single channel
- Bidirectional propagation of signal
- Stations connected, via T connectors
- No need of modems low cost installation.

Advantages

- Simplicity
- Low cost
- Ease of installation and maintenance
- High rates.

Disadvantages

- Limited distances
- Data and voice only.

IEEE LAN standards

Set of network standards developed by the IEEE. They include:

□ **IEEE 802.1:** Standards related to network management.

□ **IEEE 802.2:** General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the *logical link control (LLC) layer* and the

```
M.THILLAINAYAKI
```

media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.

□ **IEEE 802.3:** Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard. Also see the Ethernet Designations chart in the Quick Referencesection of Webopedia.

□ **IEEE 802.4:** Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).

- □ **IEEE 802.5:** Defines the MAC layer for token-ring networks.
- □ **IEEE 802.6:** Standard for Metropolitan Area Networks (MANs).

Relationship of the 802 standards to the ISO/CCITT model

The IEEE 802 LAN Standards Family

The IEEE 802 Local and Metropolitan Area Network Standards Committee is a major working group charted by IEEE to create, maintain, and encourage the use of IEEE and equivalent IEC/ISO standards. The IEEE formed the committee in February 1980, and this committee meets as a plenary body at least three times per year. The IEEE 802 committee produces the series of standards known as IEEE 802.x, and the JTC 1 series of equivalent standards is known as ISO 8802-nnn.

IEEE 802 includes a family of standards, as depicted in Figure 3.3. The MAC and Physical layers of the 802 standard were organized into a separate set of standards from the LLC because of the interdependence between medium access control, medium, and topology.

2.4 Connection options with LANs, LLC and MAC protocol data units

IEEE 802.2 LLC Overview

The LLC is the highest layer of the IEEE 802 Reference Model and provides functions similar to the traditional data link control protocol: HDLC (High-Level Data Link Control). ISO/IEC 8802-2 (ANSI/IEEE Standard 802.2), dated May 7, 1998, specifies the LLC. The purpose of the LLC is to exchange data between end users across a LAN using an 802-based MAC controlled link. The LLC provides addressing and data link control, and it is independent of the topology, transmission medium, and medium access control technique chosen.

Higher layers, such as TCP/IP, pass user data down to the LLC expecting error-free transmission across the network. The LLC in turn appends a control header, creating an LLC protocol data unit (PDU). The LLC uses the control information in the operation of the LLC protocol (see Figure 3.4). Before transmission, the LLC PDU is handed down through the MAC service access

point (SAP) to the MAC layer, which appends control information at the beginning and end of the packet, forming a MAC frame. The control information in the frame is needed for the operation of the MAC protocol.

Figure 3.4 The LLC provides end-to-end link control over an 802.11-based wireless LAN.

IEEE 802.2 LLC Services

The LLC provides the following three services for a Network Layer protocol:

- Unacknowledged connectionless service
- Connection-oriented service
- Acknowledged connectionless service

These services apply to the communication between peer LLC layers--that is, one located on the source station and one located on the destination station. Typically, vendors will provide these services as options that the customer can select when purchasing the equipment.

All three LLC protocols employ the same PDU format that consists of four fields (see Figure 3.5). The Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) fields each contain 7-bit addresses that specify the destination and source stations of the peer LLCs. One bit of the DSAP indicates whether the PDU is intended for an individual or group station(s). One bit of the SSAP indicates whether it is a command or response PDU. The format of the LLC Control field is identical to that of HDLC, using extended (7-bit) sequence numbers. The Data field contains the information from higher-layer protocols that the LLC is transporting to the destination.

Figure 3.5 The LLC PDU consists of data fields that provide the LLC functionality.

The Control field has bits that indicate whether the frame is one of the following types:

- **Information** Used to carry user data.
- **Supervisory** Used for flow control and error control.
- Unnumbered Various protocol control PDUs.

Unacknowledged Connectionless Service

The *unacknowledged connectionless service* is a datagram-style service that does not involve any error-control or flow-control mechanisms. This service does not involve the establishment of a data link layer connection (such as between peer LLCs). This service supports individual, multicast, and broadcast addressing. This service simply sends and receives LLC PDUs with no

acknowledgement of delivery. Because the delivery of data is not guaranteed, a higher layer, such as TCP, must deal with reliability issues.

The unacknowledged connectionless service offers advantages in the following situations:

- If higher layers of the protocol stack provide the necessary reliability and flow-control mechanisms, then it would be inefficient to duplicate them in the LLC. In this case, the unacknowledged connectionless service would be appropriate. TCP and the ISO transport protocol, for example, already provide the mechanisms necessary for reliable delivery.
- It is not always necessary to provide feedback pertaining to successful delivery of information. The overhead of connection establishment and maintenance can be inefficient for applications involving the periodic sampling of data sources, such as monitoring sensors. The unacknowledged connectionless service would best satisfy these requirements.

Connection-Oriented Service

The *connection-oriented service* establishes a logical connection that provides flow control and error control between two stations needing to exchange data. This service does involve the establishment of a connection between peer LLCs by performing connection establishment, data transfer, and connection termination functions. The service can connect only two stations; therefore, it does not support multicast or broadcast modes. The connection-oriented service offers advantages mainly if higher layers of the protocol stack do not provide the necessary reliability and flow-control mechanisms, which is generally the case with terminal controllers.

Flow control is a protocol feature that ensures that a transmitting station does not overwhelm a receiving station with data. With flow control, each station allocates a finite amount of memory and buffer resources to store sent and received PDUs.

Networks, especially wireless networks, suffer from induced noise in the links between network stations that can cause transmission errors. If the noise is high enough in amplitude, it causes errors in digital transmission in the form of altered bits. This will lead to inaccuracy of the transmitted data, and the receiving network device may misinterpret the meaning of the information.

The noise that causes most problems with networks is usually Gaussian and impulse noise. Theoretically, the amplitude of Gaussian noise is uniform across the frequency spectrum, and it normally triggers random single-bit independent errors. Impulse noise, the most disastrous, is characterized by long quiet intervals of time followed by high amplitude bursts. This noise results from lightning and switching transients. Impulse noise is responsible for most errors in digital communication systems and generally provokes errors to occur in bursts.

- Lost PDU A PDU fails to arrive at the other end or is damaged beyond recognition.
- **Damaged PDU** A PDU has arrived, but some bits are altered.

When a frame arrives at a receiving station, the station checks whether there are any errors present by using a *Cyclic Redundancy Check (CRC)* error detection algorithm. In general, the receiving station will send back a positive or negative acknowledgement, depending on the outcome of the error detection process. In case the acknowledgement is lost in route to the sending station, the sending station will retransmit the frame after a certain period of time. This process is often referred to as *Automatic Repeat Request (ARQ)*.

Overall, ARQ is best for the correction of burst errors because this type of impairment occurs in a small percentage of frames, thus not invoking many retransmissions. Because of the feedback inherent in ARQ protocols, the transmission links must accommodate half-duplex or full-duplex transmissions. If only simplex links are available because of feasibility, then it is impossible to use the ARQ technique because the receiver would not be able to notify the transmitter of bad data frames.

The following are two approaches for retransmitting unsatisfactory blocks of data using ARQ:

• **Continuous ARQ** With this type of ARQ, often called a *sliding window protocol*, the sending station transmits frames continuously until the receiving station detects an error. The sending station is usually capable of transmitting a specific number of frames and maintains a table indicating which frames have been sent.

The system implementor can set the number of frames sent before stopping via configuration parameters of the network device. If a receiver detects a bad frame, it will send a negative acknowledgement back to the sending station requesting that the bad frame be sent again. When the transmitting station gets the signal to retransmit the frame, several subsequent frames may have already been sent (due to propagation delays between the sender and receiver); therefore, the transmitter must go back and retransmit the bad data frame.

There are a couple of ways the transmitting station can send frames again using continuous ARQ. One method is for the source to retrieve the bad frame from the transmit buffer and send it and all frames following it. This is called the *go-back-n technique*. A problem is that when n (the number of frames the transmitter sent after the

bad frame plus one) becomes large, the method becomes inefficient. This is because the retransmission of just one frame means that a large number of possibly good frames will also be resent, thus decreasing throughput.

The go-back-*n* technique is useful in applications for which receiver buffer space is limited because all that is needed is a receiver window size of one (assuming frames are to be delivered in order). When the receive node rejects a bad frame (sends a negative acknowledgment), it does not need to buffer any subsequent frames for possible reordering while it is waiting for the retransmission, because all subsequent frames will also be sent.

An alternative to the continuous go-back-*n* technique is a method that selectively retransmits only the bad frame, then resumes normal transmission at the point just before getting the notification of a bad frame. This approach is called *selective repeat*. It is obviously better than continuous go-back-*n* in terms of throughput because only the bad frame needs retransmission. With this technique, however, the receiver must be capable of storing a number of frames if they are to be processed in order. The receiver needs to buffer data that has been received after a bad frame was requested for retransmission since only the damaged frame will be sent again.

• Stop-and-wait ARQ With this method, the sending station transmits a frame, then stops and waits for some type of acknowledgment from the receiver on whether a particular frame was acceptable or not. If the receiving station sends a negative acknowledgment, the frame will be sent again. The transmitter will send the next frame only after it receives a positive acknowledgment from the receiver.

An advantage of stop-and-wait ARQ is that it does not require much buffer space at the sending or receiving station. The sending station needs to store only the current transmitted frame. However, stop-and-wait ARQ becomes inefficient as the propagation delay between source and destination becomes large. For example, data sent on satellite links normally experiences a round-trip delay of several hundred milliseconds; therefore, long block lengths are necessary to maintain a reasonably effective data rate. The trouble is that with longer frames, the probability of an error occurring in a particular block is greater. Thus, retransmission will occur often, and the resulting throughput will be lower.

Acknowledged Connectionless Service

As with the The unacknowledged connectionless service, the *acknowledged connectionless service* does not involve the establishment of a logical connection with the distant station. But the receiving stations with the acknowledged version do confirm successful delivery of datagrams. Flow and error control is handled through use of the stop-and-wait ARQ method.

The acknowledged connectionless service is useful in several applications. The connectionoriented service must maintain a table for each active connection for tracking the status of the connection. If the application calls for guaranteed delivery, but there is a large number of destinations needing to receive the data, then the connection-oriented service may be impractical because of the large number of tables required. Examples that fit this scenario include process control and automated factory environments that require a central site to communicate with a large number of processors and programmable controllers. In addition, the handling of important and time-critical alarm or emergency control signals in a factory would also fit this case. In all these examples, the sending station needs an acknowledgment to ensure successful delivery of the data; however, an urgent transmission cannot wait for a connection to be established.

LLC/MAC Layer Service Primitives

Layers within the 802 architecture communicate with each other via service primitives having the following forms:

- **Request** A layer uses this type of primitive to request that another layer perform a specific service.
- **Confirm** A layer uses this type of primitive to convey the results of a previous service request primitive.
- **Indication** A layer uses this type of primitive to indicate to another layer that a significant event has occurred. This primitive could result from a service request or from some internally generated event.
- **Response** A layer uses this type of primitive to complete a procedure initiated by an indication primitive.

These primitives are an abstract way of defining the protocol, and they do not imply a specific physical implementation method. Each layer within the 802 model uses specific primitives. The LLC layer communicates with its associated MAC layer through the following specific set of service primitives:

- **MA-UNITDATA.request** The LLC layer sends this primitive to the MAC layer to request the transfer of a data frame from a local LLC entity to a specific peer LLC entity or group of peer entities on different stations. The data frame could be an information frame containing data from a higher layer or a control frame (such as a supervisory or unnumbered frame) that the LLC generates internally to communicate with its peer LLC.
- **MA-UNITDATA.indication** The MAC layer sends this primitive to the LLC layer to transfer a data frame from the MAC layer to the LLC. This occurs only if the MAC has found that a frame it receives from the Physical layer is valid and has no errors and the destination address indicates the correct MAC address of the station.

2.5 LAN topologies and protocols

Network topologies can take a bit of time to understand when you're all new to this kind of cool stuff, but it's very important to fully understand them as they are key elements to understanding and troubleshooting networks and will help you decide what actions to take when you're faced with network problems.

This article explains the different network topologies found in today's networks. We examine Bus Topology, Ring Topology, Star Topology, Mesh Topology, Hybrid Topology and many more.

Physical and Logical Topologies

There are two types of topologies: Physical and Logical. The physical topology of a network refers to the layout of cables, computers and other peripherals. Try to imagine yourself in a room with a small network, you can see network cables coming out of every computer that is part of the network, then those cables plug into a hub or switch. What you're looking at is the physical topology of that network !

Logical topology is the method used to pass the information between the computers. In other words, looking at that same room, if you were to try to see how the network works with all the computers talking (think of the computers generating traffic and packets of data going everywhere on the network) you would be looking at the logical part of the network. The way the computers will be talking to each other and the direction of the traffic is controlled by the various protocols (like Ethernet) or, if you like, rules.

If we used token ring, then the physical topology would have to change to meet the requirements of the way the token ring protocol works (logically).

If it's all still confusing, consider this: The physical topology describes the layout of the network, just like a map shows the layout of various roads, and the logical topology describes how the data is sent accross the network or how the cars are able to travel (the direction and speed) at every road on the map.

The most common types of physical topologies, which we are going to analyse, are: Bus, Hub/Star and Ring

The Physical Bus Topology

Bus topology is fairly old news and you probably won't be seeing much of these around in any modern office or home.

With the Bus topology, all workstations are connect directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations. This works well in a small network of 2-5 computers, but as the number of computers increases so will the network traffic and this can greatly decrease the performance and available bandwidth of your network.



As you can see in the above example, all computers are attached to a continuous cable which connects them in a straight line. The arrows clearly indicate that the packet generated by Node 1 is transmitted to all computers on the network, regardless the destination of this packet.

Also, because of the way the electrical signals are transmitted over this cable, its ends must be terminated by special terminators that work as "shock absorbers", absorbing the signal so it won't reflect back to where it came from. The value of 500hms has been selected after carefully taking in consideration all the electrical characteristics of the cable used, the voltage that the signal which runs through the cables, the maximum and minimum length of the bus and a few more.

If the bus (the long yellow cable) is damaged anywhere in its path, then it will most certainly cause the network to stop working or, at the very least, cause big communication problems between the workstations.

Thinnet - 10 Base2, also known as coax cable (Black in colour) and Thicknet - 10 Base 5 (Yellow in colour) is used in these type of topologies.

2.6 Token ring (Priority), token bus and IEEE 802.4

IEEE 802.4 Token Bus : In token bus Computer network station must have possession of a token before it can transmit on the computer network. The IEEE 802.4 Committee has defined **token bus** standards as broadband computer networks, as opposed to Ethernet's baseband transmission technique. Physically, the token bus is a linear or tree-shape cable to which the stations are attached

The topology of the computer network can include groups of workstations connected by long trunk cables. Logically, the stations are organized into a ring. These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. **IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology**. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

When the logical ring is initialized, the highest numbered station may send the first frame. The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

In such a case, there is no collision as only one station possesses a token at any given time. In token bus, each station receives each frame; the station whose address is specified in the frame processes it and the other stations discard the frame.



MAC Sublayer Function

• When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.

- Token passing is done from high to low address.
- Whenever a station acquires the token, it can transmit frames for a specific amount of time.
- If a station has no data, it passes the token immediately upon receiving it.
- The token bus defines four priority classes, 0, 2, 4, and 6 for traffic, with 0 the lowest and 6 the highest.

• Each station is internally divided into four substations, one at each priority level *i.e.* 0,2,4 and 6.

• As input comes in to the MAC sublayer from above, the data are checked for priority and routed to one of the four substations.

• Thus each station maintains its own queue of frames to be transmitted.

• When a token comes into the station over the cable, it is passed internally to the priority 6 substation, which can begin transmitting its frames, if it has any.

• When it is done or when its time expires, the token is passed to the priority 4 substation, which can then transmit frames until its timer expires. After this the token is then passed internally to priority 2 substation.

• This process continues until either the priority 0 substation has sent all its frames or its time expires.

• After this the token is passed to the next station in the ring.

Frame format of Token Bus

The various fields present in the frame format are

1. **Preamble**: This. Field is at least 1 byte long. It is used for bit synchronization.

1 byte	1 byte	1 byte	2-6 byte	2-6 byte	0-8182	4 byte	1 byte
Preamble	Start Delimiter	Frame Control	Destination Address	Source Address	Data	Checksum	End Delimiter
			Frame format of	IEEE 802.4		÷.	

2. **Start Delimiter**: This one byte field marks the beginning of frame.

3. **Frame Control:** This one byte field specifies the type of frame. It distinguishes data frame from control frames. For data frames it carries frame's priority. For control frames, it specifies the frame type. The control frame types include. token passing and various ring maintenance frames, including the mechanism for letting new station enter the ring, the mechanism for allowing stations to leave the ring.

4. **Destination address**: It specifies 2 to 6 bytes destination address.

5. **Source address**: It specifies 2 to 6 bytes source address.

6. **Data**: This field may be upto 8182 bytes long when 2 bytes addresses are used & upto 8174 bytes long when 6 bytes address is used.

7. **Checksum**: This 4 byte field detects transmission errors.

8. End Delimiter: This one byte field marks the end of frame.

The various control frames used in token bus are:

Farme Control Field	Name	Meaning
00000000	Claim_token	Claim token during ring initialization
00000001	Solicit successor_1	Allow station to enter the ring
00000010	Solicit successor_2	Allow stations to enter the ring
00000011	Who_follows	Recover from lost token.
00000100	Resolve_contention	Used when multiple stations want to enter.
00001000	Token	Pass the token
00001100	Set successor	Allow station to leave the ring.

2.7 Metropolitan area networks (MANs)

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

2.8 ANSI fiber distributed data interface.

A high-speed network technology, conforming to the Open Systems Interconnection (OSI) reference model for networking and the American National Standards Institute (ANSI) standard X3T9, which runs at 100 Mbps over fiber-optic cabling; often used for network backbones in a local area network (LAN) or metropolitan area network (MAN).

How FDDI Works

Fiber Distributed Data Interface (FDDI) is usually implemented as a dual token-passing ring within a ring topology (for campus networks) or star topology (within a building). The dual ring consists of a primary and secondary ring. The primary ring carries data. The counter-rotating secondary ring can carry data in the opposite direction, but is more commonly reserved as a backup in case the primary ring goes down. This provides FDDI with the degree of fault tolerance necessary for network backbones. In the event of a failure on the primary ring, FDDI automatically reconfigures itself to use the secondary ring as shown in the illustration. Faults can be located and repaired using a fault isolation technique called beaconing. However, the secondary ring can also be configured for carrying data, extending the maximum potential bandwidth to 200 Mbps.

Stations connect to one (or both) rings using a media interface connector (MIC). Its two fiber ports can be either male or female, depending on the implementation. There are two different FDDI implementations, depending on whether stations are attached to one or both rings:

• Single-attached stations (Class B stations):

Connect to either the primary or secondary ring using M ports. Single-attached FDDI uses only the primary ring and is not as commonly deployed for network backbones as dual-attached FDDI. Single-attached stations are used primarily to connect Ethernet LANs or individual servers to FDDI backbones.

• Dual-attached stations (Class A stations):

Connect to both rings. The A port is the point at which the primary ring enters and the secondary ring leaves; the B port is the reverse. M ports provide attachment points for single-attached stations. Dual-attached FDDI uses both rings, with the secondary ring serving as a backup for the primary. Dual-attached FDDI is used primarily for network backbones that require fault tolerance. Single-attached stations can be connected to dual-attached FDDI backbones using a dual-attached device called a concentrator or multiplexer.



FDDI uses a timed token-passing technology similar to that of token ring networks as defined in the IEEE 802.5 standard. FDDI stations generate a token that controls the sequence in which

other stations will gain access to the wire. The token passes around the ring, moving from one node to the next. When a station wants to transmit information, it captures the token, transmits as many frames of information as it wants (within the specified access period), and then releases the token. This feature of transmitting multiple data frames per token capture is known as a capacity allocation scheme, in contrast to the priority mechanism used in the IEEE 802.5 token ring standard. Every node on the ring checks the frames. The recipient station then reads the information from the frames, and when the frames return to the originating station, they are stripped from the ring.

There can be up to 500 stations on a dual-ring FDDI network. The maximum circumference for an FDDI ring is 100 kilometers (or 200 kilometers for both rings combined), and there must be a repeater every 2 kilometers or less. Bridges or routers are used to connect the FDDI backbone network to Ethernet or token ring departmental LANs. For these reasons, FDDI is not often used as a wide area network (WAN) solution, but is more often implemented in campus-wide networks as a network backbone.
	Karpagam A					
	Departmen	t of Compu	iter Applica	ations		
	BCA					
	ADVANCED	NETWORK	ING (18CA	U303)		
		UNIT- I	I			
S.No	Question	Option1	Option2	Option3	Option4	Answer
1	is a set of techniques that allows the simultaneous transmission of multiple signals across a single link.	Multiple xing	Demulti plexing	Interleavi ng	Synchroni zing	Multiplexing
2	ASK stands for	Amplifie r Shift Keying	Amplitu de Shift Keying	Analog Shift Keying	Amplify Shift Keying	Amplitude Shift Keying
3	FSK stands for	Frame Shift Keying	Functio nal Shift Keying	Frequenc y Shift Keying	Final Shift Keying	Frequency Shift Keying
4	PSK stands for	Phase Shift Keying	Period Shift Keying	Performa nce Shift Keying	Page Shift Keying	Phase Shift Keying
5	QAM stands for	Quadrat ure Amplifie r Modulat ion	Quadrat ure Amplitu de Modulat ion	Quadratu re Analog Modulati on	Quadratu re Amplify Modulati on	Quadrature Amplitude Modulation
6	conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data.	Analog to anlog	Digital to digital	Analog to digital	Digital to analog	Digital to analog
7	A is a device that selects one of several analog or digital input signals and forwards the selected input into a single line.	demulti plexer	multiple xer	converter	inverter	multiplexer
8	A is a device that takes a single input line and routes it to one of several digital output lines	demulti plexer	multiple xer	converter	inverter	demultiplexer
9	The word refers to the portion of a link that carries a transmission between a given pair of lines	path	link	channel	node	channel

S.No	Question	Option1	Option2	Option3	Option4	Answer
10	FDM stands for	Frame Division Multiple xing	Functio nal Division Multiple xing	Frequenc y Division Multiplexi ng	Factor Division Multiplexi ng	Frequency Division Multiplexing
11	is a analog multiplexing technique that combines analog signal	TDM	FDM	WDM	ADM	FDM
12	WDM stands for	Work Division Multiple xing	Wavele ngth Division Multiple xing	Weight Division Multiplexi ng	Web Division Multiplexi ng	Wavelength Division Multiplexing
13	is designed to use the high-data-rate capability of fiber optic cable	TDM	FDM	WDM	ADM	WDM
14	TDM stands for	Time Division Multiple xing	Type Division Multiple xing	Test Division Multiplexi ng	Transmiss ion Division Multiplexi ng	Time Division Multiplexing
15	is a digital is a digital	TDM	FDM	WDM	ADM	TDM
16	Multiplexing is used in 	Packet switchin g	Circuit switchin g	Data switching	datagram switching	Circuit switching
17	In multiplexing, channels are separated by unused strips of bandwidth guard bands - to prevent	Synchro nization	Overlap ping	random motion of electrons	interleavi ng	Overlapping
18	Frequency difference between WDM and FDM is	very high	very low	zero	infinity	very high
19	Transmission media are actually located below the layer.	applicati on	present ation	physical	data link	physical
20	Transmission media are directly controlled by the	physical layer	data link layer	network layer	session layer	physical layer
21	Optical fibers use reflection to guide light through a	channel	metal wire	light	plastic	channel
22	Which transmission media has the highest transmission speed in a network?	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	optical fiber cable
23	is a cable made up of glass or plastics that transmits the signlas in the form of light	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	optical fiber cable

S.No	Question	Option1	Option2	Option3	Option4	Answer
24	cable consists of two insulated copper wires twisted together.	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	twisted pair cable
25	cable consists of central conductor and sheild.	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	coaxial cable
26	cable is used in backbone networks, cable Tv networks and fast ethernet networks	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	fiber optic cable
27	are used for cellular phone, satellite and wireless LAN communications	Micro Waves	Infrared Waves	Sine Waves	Radio Waves	Micro Waves
28	Which of the following is used for short range communications?	Micro Waves	Infrared Waves	Sine Waves	Radio Waves	Infrared Waves
29	Three methods of switching are	circuit switchin g, packet switchin g, and protocol switchin g	circuit switchin g, packet switchin g, and messag e switchin g	Loop switching, packet switching, and message switching	Node switching, packet switching, and message switching	circuit switching, packet switching, and message switching
30	A switched network consists of a series of interlinked nodes, called	endpoin ts	packets	switches	links	switches
31	Switching in Internet is done by using datagram approach to packet switching at the	network layer	applicati on layer	data link layer	physical layer	network layer
32	A Circuit-Switched Network is made of a set of switches connected by physical	media	links	nodes	lines	links
33	A switch in a datagram network uses a	destinat ion address	sender address	routing table	header	routing table
34	Routing processor searching for routing table is called	switch fabric	buffer	table lookup	rolling table	table lookup
35	In the resources need to be reserved during the setup phase.	circuit switchin g	packet switchin g	message switching	datagram switching	circuit switching
36	In Circuit Switching, resources needs to be reserved during the	data transfer phase	teardow n phase.	setup phase	propagati on phase	setup phase

S.No	Question	Option1	Option2	Option3	Option4	Answer
37	In there is no	circuit	packet	message	datagram	packet
	resources are alloted on	σ	σ	Switching	switching	Switching
	demand	б	б			
38	In a packet-switched	randoml	on	reserved	automatic	on demand
	network, resources are	у	demand	already	ally	
	allocated					
39	Actual communication in a	one	two	three	four	three phases
	circuit-switched network	phase	phases	phases	phases	
40	requires	oino uit	in a alvat		data ara m	oine uit
40	connection teardown are	switchin	switchin	switching	switching	switching
	three phases of	g	g	Switching	Switching	Switching
41	Circuit switching takes place	network	applicati	data link	physical	physical layer
	at the	layer	on layer	layer	layer	.,,,
42	A local telephone network is	packet	circuit	message	virtual	packet
	an example of a	switche	switche	switched	switched	switched
	network	d	d			
43	which of the following	packet	circuit	message	virtual	circuit
	network requires that all	switche	switche	switched	switched	switched
	channels in a message	d	d			
	transmission path be of the					
44	Which of the networks allow	packet	circuit	message	virtual	packet
	different speed links?	switche	switche	switched	switched	switched
		d	d			
45	Which of the networks allow	packet	circuit	message	virtual	packet
	pipelining effect?	switche	switche	switched	switched	switched
		d	d			
46	HFC stands for	High	High	Hybrid	Hybrid	High
		cable	cy Cable	Coaxial	v Cable	Cable
47	Cable TV networks started to	1940s	1950s	1960s	1970s	1940s
	distribute broadcast video					
	signals to locations in late					
48	When Cable TV is used for	11	22	33channe	44	33channels
	data transfer then	channel	channel	IS	channels	
	downstream band has	5	5			
49	DSL stands for	Digital	Data	Digital	Data	Digital
		Subscrib	Subscrib	Switched	SwitchedL	Subscriber
		er Line	er Line	Line	ine	Line
50	Distance of Symmetric	18000	12000	10000	30000	12000
	Digital Subscriber Line is					

3.1 Network Protocols : TCP , UDP, IP, ICMP, SNMP,RMON

Protocols

In information technology, a protocol (from the Greek *protocollon*, which was a leaf of paper glued to a manuscript volume, describing its contents) is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols attach layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

Standards Organization

Standards

creation

Communities

IEEE (Institute of **Electrical** and **Electronics Engineers**) IEEE's Constitution defines the purposes of the organization as "scientific and educational, directed toward the advancement of the theory and practice of Electrical, Electronics, Communications and Computer Engineering, as well as Computer Science, the allied branches of engineering and the related arts and sciences." The IEEE is incorporated under the Not-for-Profit Corporation Law of the state of New York, United States. It was formed in 1963 by the merger of the Institute of Radio Engineers (IRE, founded 1912) and the American Institute of Electrical Engineers (AIEE, founded 1884). It has more than 400,000 members in more than 160 countries, 45% outside the United States. In pursuing these goals, the IEEE serves as a major publisher of scientific journals and a conference organizer. It is also a leading developer of industrial standards (having developed over 900 active industry standards) in a broad range of disciplines, including electric power and energy, biomedical technology and health care, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotechnology. IEEE develops and participates in educational activities such as accreditation of electrical engineering programs in institutes of higher learning. IEEE is one of the leading standards-making organizations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association (IEEE-SA). IEEE standards affect a wide range of industries including: power and energy, biomedical and health care, Information Technology (IT), telecommunications, transportation, nanotechnology, information assurance, and many more. In 2005, IEEE had close to 900 active standards, with 500 standards under development. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and 802.11 Wireless IEEE Networking standard. the ANSI (American National **Standards Institute**)

Though ANSI itself does not develop standards, the Institute oversees the development and use of standards by accrediting the procedures of standards developing organizations. ANSI accreditation signifies that the procedures used by standards developing organizations meet the requirements for balance, Institute's openness, consensus, and due process. ANSI was originally formed in 1918, when five engineering societies and three government agencies founded the American Engineering Standards Committee (AESC). In 1928, the AESC became the American Standards Association (ASA). In 1966, the ASA was reorganized and became the United States of America Standards Institute (USASI). The present name was adopted in 1969. Prior to 1918, these five engineering societies:

- American Institute of Electrical Engineers (AIEE, now IEEE)
- American Society of Mechanical Engineers (ASME)
- American Society of Civil Engineers (ASCE)
- American Institute of Mining Engineers (AIME, now American Institute of Mining, Metallurgical, and Petroleum Engineers)
- American Society for Testing and Materials (now ASTM International)

ANSI also designates specific standards as American National Standards, or ANS, when the Institute determines that the standards were developed in an environment that is equitable, accessible and responsive to the requirements of various stakeholders.

The American National Standards process involves:

- consensus by a group that is open to representatives from all interested parties
- broad-based public review and comment on draft standards
- consideration of and response to comments
- incorporation of submitted changes that meet the same consensus requirements into a draft standard
- availability of an appeal by any participant alleging that these principles were not respected during the standards-development process.

ITU (International Telecommunications Union - formerly CCITT) The International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.

ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

ISO (International Organization for Standardization widely known as ISO, is an international standard-setting body composed of representatives from various national standards organizations. Founded on February 23, 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments

ISO, is an international standard-setting body composed of representatives from various national standards organizations the organization promulgates worldwide proprietary industrial and commercial standards.ISO's main products are the International Standards. ISO also publishes Technical Reports, Technical Specifications, Publicly Available Specifications, Technical Corrigenda, and Guides.

EIA (Electronic Industries Association)

The Electronic Industries Alliance (EIA, until 1997 Electronic Industries Association) was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangable.In 1924 the Associated Radio Manufacturers alliance was formed, which was renamed to Radio Manufacturers Association (RMA) the same year. Upcoming new electronic technologies brought new members and further name changes: Radio Television Manufacturers Association (RTMA) (1950), Radio Electronics Television Manufacturers (RETMA) (1953) and Electronics Industries Association (EIA) (1957). The last renaming took place in 1997, when EIA became Electronics Industries Alliance (EIA), reflecting the change away from a pure manufacturers association A standard defining serial communication between computers and modems e. g. was originally drafted by the radio sector as RS-232. Later it was taken over by the EIA as EIA-232. Later this standard was managed by the TIA and the name was changed to the current TIA-232. Because the EIA was accredited by ANSI to help develop standards in its areas, the standards are often described as e. g. ANSI TIA-232 (or formerly as ANSI EIA/TIA-232').

ETSI (European Telecommunications Standards Institute)

The European Telecommunications Standards Institute (ETSI) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSM cell phone system and the TETRA professional mobile radio system.Significant ETSI standardisation bodies include TISPAN (for fixed networks and Internetmachine-to-machine communications). ETSI inspired the creation of, and is a partner in 3GPP.

ETSI was created by CEPT in 1988 and is officially recognized by the European Commission and the EFTA secretariat. Based in Sophia Antipolis (France), ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics. ETSI has 740 members from 62 countries/provinces inside and outside Europe, including manufacturers, network operators, administrations, service providers, research bodies and users — in fact, all the key players in the ICT arena. convergence) and M2M (for ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSMTETRA professional mobile radio system.ETSI was created by CEPT in 1988 and is officially recognized by the European Commission and the EFTASophia Antipolis (France), ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics. Wide Consortium W₃C World Web The World Wide Web Consortium (W3C) is the main international standards organizationWorld Wide Web (abbreviated WWW or W3).

Founded and headed by Tim Berners-Lee, the consortium is made up of member organizations which maintain full-time staff for the purpose of working together in the development of standards for the World Wide Web. As of 18 February 2011, the World Wide Web Consortium (W3C) has 322 members.

W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.

W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.W3C was created to ensure compatibility and agreement among industry members in the adoption of new standards. Prior to its creation, incompatible versions of HTML were offered by different vendors, increasing the potential for inconsistency between web pages. The consortium was created to get all those vendors to agree on a set of core principles and components which would be supported by everyone.

3.2 TCP/IP : TCP/IP and internetworking

Internetworking elements:

The diagram shows elements of a typical network, including devices, media, and services, tied together by rules, that work together to send messages. We use the word *messages* as a term that encompasses web pages, e-mail, instant messages, telephone calls, and other forms of communication enabled by the Internet.



Internetworking is a very graphically oriented subject, and icons are commonly used to represent networking devices. On the left side of the diagram are shown some common devices which often originate messages that comprise our communication. These include various types of computers (a PC and laptop icon are shown), servers, and IP phones. On local area networks these devices are typically connected by LAN media (wired or wireless). The right side of the figure shows some of the most common intermediate devices, used to direct and manage messages across the network, as well as other common **internetworking** symbols. Generic symbols are shown for:

- Switch the most common device for interconnecting local area networks
- Firewall provides security to networks
- Router helps direct messages as they travel across a network
- Wireless Router a specific type of router often found in home networks
- Cloud used to summarize a group of networking devices, the details of which may be unimportant to the discussion at hand
- Serial Link one form of WAN interconnection, represented by the lightning bolt-shaped line



Common Data Network Symbols

Network Interface Card - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC.

Physical Port - A connector or outlet on a **internetworking** device where the media is connected to a host or other networking device.

Interface - Specialized ports on an **internetworking** device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to network interfaces.

For a network to function, the devices must be interconnected. Network connections can be wired or wireless. In wired connections, the medium is either copper, which carries electrical signals, or optical fiber, which carries light signals. In wireless connections, the medium is the Earth's atmosphere, or space, and the signals are microwaves. Copper medium includes cables, such as twisted pair telephone wire, coaxial cable, or most commonly, what is known as Category 5 Unshielded Twisted Pair (UTP) cable. Optical fibers, thin strands of glass or plastic

that carry light signals, are another form of **internetworking** media. Wireless media may include the home wireless connection between a wireless router and a computer with a wireless network card, the terrestrial wireless connection between two ground stations, or the communication between devices on earth and satellites. In a typical journey across the Internet, a message may travel across a variety of media.



Human beings often seek to send and receive a variety of messages using computer applications; these applications require services to be provided by the network. Some of these services include the World Wide Web, e-mail, instant messaging, and IP Telephony. Devices interconnected by medium to provide services must be governed by rules, or protocols. In the chart, some common services and a protocol most directly associated with that service are listed. Protocols are the rules that the networked devices use to communicate with each other. The industry standard in **internetworking** today is a set of protocols called TCP/IP(Transmission Control Protocol). TCP/IP is used in home and business networks, as well as being the

primary protocol of the Internet. It is TCP/IP protocols that specify the formatting, addressing and routing mechanisms that ensure our messages are delivered to the correct recipient.

The Messages

In the first step of its journey from the computer to its destination, our instant message gets converted into a format that can be transmitted on the network. All types of messages must be converted to bits, binary coded digital signals, before being sent to their destinations. This is true no matter what the original message format was: text, video, voice, or computer data. Once our instant message is converted to bits, it is ready to be sent onto the network for delivery.

The Devices

To begin to understand the robustness and complexity of the interconnected networks that make up the Internet, it is necessary to start with the basics. Take the example of sending the text message using an instant messaging program on a computer. When we think of using network services, we usually think of using a computer to access them. But, a computer is only one type of device that can send and receive messages over a network. Many other types of devices can also be connected to the network to participate in network services. Among these devices are telephones, cameras, music systems, printers and game consoles.

In addition to the computer, there are numerous other components that make it possible for our instant message to be directed across the miles of wires, underground cables, airwaves and satellite stations that might exist between the source and destination devices. One of the critical components in any size network is the router. A router joins two or more networks, like a home network and the Internet, and passes information from one network to another. Routers in a network work to ensure that the message gets to its destination in the most efficient and quickest manner.

The Medium

To send our instant message to its destination, the computer must be connected to a wired or wireless local network. Local networks can be installed in homes or businesses, where they enable computers and other devices to share information with each other and to use a common connection to the Internet.

Wireless networks allow the use of networked devices anywhere in an office or home, even outdoors. Outside the office or home, wireless networking is available in public hotspots, such as coffee shops, businesses, hotel rooms, and airports.

Many installed networks use wires to provide connectivity. Ethernet is the most common wired **internetworking** technology found today. The wires, called cables, connect the computers and

other devices that make up the networks. Wired networks are best for moving large amounts of data at high speeds, such as are required to support professional-quality multimedia.

The Services

Network services are computer programs that support the human network. Distributed on devices throughout the network, these services facilitate online communication tools such as e-mail, bulletin/discussion boards, chat rooms, and instant messaging. In the case of instant messaging, for example, an instant messaging service, provided by devices in the cloud, must be accessible to both the sender and recipient.

The Rules

Important aspects of networks that are neither devices nor media are rules, or protocols. These rules are the standards and protocols that specify how the messages are sent, how they are directed through the network, and how they are interpreted at the destination devices. For example, in the case of Jabber instant messaging, the XMPP, TCP, and IP protocols are all important sets of rules that enable our communication to occur.

The Network architecture:

Networks must support a wide range of applications and services, as well as operate over many different types of physical infrastructures. The term network architecture, in this context, refers to both the technologies that support the infrastructure and the programmed services and protocols that move the messages across that infrastructure. As the Internet, and networks in general, evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations: fault tolerance, scalability, quality of service, and security.

Fault Tolerance

The expectation that the Internet is always available to the millions of users who rely on it requires a network architecture that is designed and built to be fault tolerant. A fault tolerant network is one that limits the impact of a hardware or software failure and can recover quickly when such a failure occurs. These networks depend on redundant links, or paths, between the source and destination of a message. If one link or path fails, processes ensure that messages can be instantly routed over a different link transparent to the users on either end. Both the physical infrastructures and the logical processes that direct the messages through the network are designed to accommodate this redundancy. This is a basic premise of the architecture of current networks.



Scalability

A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users. Thousands of new users and service providers connect to the Internet each week. The ability of the network to support these new interconnections depends on a hierarchical layered design for the underlying physical infrastructure and logical architecture. The operation at each layer enables users or service providers to be inserted without causing disruption to the entire network. Technology developments are constantly increasing the message carrying capabilities and performance of the physical infrastructure components at every layer. These developments, along with new methods to identify and locate individual users within an internetwork, are enabling the Internet to keep pace with user demand.



Quality of Service (QoS)

The Internet is currently providing an acceptable level of fault tolerance and scalability for its users. But new applications available to users over internetworks create higher expectations for the quality of the delivered services. Voice and live video transmissions require a level of consistent quality and uninterrupted delivery that was not necessary for traditional computer applications. Quality of these services is measured against the quality of experiencing the same audio or video presentation in person. Traditional voice and video networks are designed to support a single type of transmission, and are therefore able to produce an acceptable level of quality. New requirements to support this quality of service over a converged **internetworking** are changing the way network architectures are designed and implemented.



Security

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The security and privacy expectations that result from the use of internetworks to exchange confidential and business critical information exceed what the current architecture can deliver. Rapid expansion in communication areas that were not served by traditional data networks is increasing the need to embed security into the network architecture. As a result, much effort is being devoted to this area of research and development. In the meantime, many tools and procedures are being implemented to combat inherent security flaws in the network architecture.



Fault Tolerant Network Architecture

The Internet, in its early inception, was the result of research funded by the United States Department of Defense (DoD). Its primary goal was to have a communications medium that could withstand the destruction of numerous sites and transmission facilities without disruption of service. It only follows that fault tolerance was the focus of the effort of the initial internetwork design work. Early network researchers looked at the existing communication networks, which were primarily for the transmission of voice traffic, to determine what could be done to improve the fault tolerance level.

Circuit Switched Connection-oriented Networks

To understand the challenge that the DoD researchers were faced with, it is necessary to look at how early telephone systems work. When a person makes a call using a traditional telephone set, the call first goes through a setup process, where all of the telephone switching locations between the person and the phone set that they are calling are identified. A temporary path, or circuit, is created through the various switching locations to use for the duration of the telephone call. If any link or device participating in the circuit fails, the call is dropped. To reconnect, a new call must be made, and a new circuit created between the source telephone set and the destination. This type of connection-oriented network is called a circuit-switched network. Early circuit switched networks did not dynamically recreate dropped circuits. In order to recover from

failure, new calls had to be initiated and new circuits built end-to-end. Many circuit switched networks give priority to maintaining existing circuit connections, at the expense of new circuit requests. In this type of connection-oriented network, once a circuit is established, even if no communication is occurring between the persons on either end of the call, the circuit remains connected and resources reserved until one of the parties disconnects the call. Since there is a finite capacity to create new circuits, it is possible to occasionally get a message that all circuits are busy and a call cannot be placed. The cost to create many alternate paths with enough capacity to support a large number of simultaneous circuits, and the technologies necessary to dynamically recreate dropped circuits in the event of a failure, led the DoD to consider other types of networks.



Circuit Switching in a Telephone Network

Packet Switched Connectionless Networks

In the search for a network that could withstand the loss of a significant amount of its transmission and switching facilities, the early Internet designers reevaluated early research regarding packet switched networks. The premise for this type of networks is that a single message can be broken into multiple message blocks. Individual blocks containing addressing information indicate both their origination point and their final destination. Using this embedded information, these message blocks, called packets, can be sent through the network along various paths, and can be reassembled into the original message upon reaching their destination.

Utilizing Packets

The devices within the network itself are unaware of the content of the individual packets, only visible is the address of the final destination and the next device in the path to that destination. No reserved circuit is built between sender and receiver. Each packet is sent independently from one switching location to another. At each location, a routing decision is made as to which path to use to forward the packet towards its final destination. If a previously used path is no longer available, the routing function can dynamically choose the next best available path. Because the messages are sent in pieces, rather than as a single complete message, the few packets that may be lost in the advent of a failure can be retransmitted to the destination along a different path. In many cases, the destination device is unaware that any failure or rerouting has occurred.

Packet-switched Connectionless Networks

The DoD researchers realized that a packet switched connectionless network had the features necessary to support a resilient, fault tolerant network architecture. The need for a single, reserved circuit from end-to-end does not exist in a packet switched network. Any piece of a message can be sent through the network using any available path. Packets containing pieces of messages from different sources can travel the network at the same time. The problem of underutilized or idle circuits is eliminated -- all available resources can be used at any time to deliver packets to their final destination. By providing a method to dynamically use redundant paths, without intervention by the user, the Internet has become a fault tolerant, scalable method of communications.

Connection-oriented Networks

Although packet-switched connectionless networks met the needs of the DoD, and continue to be the primary infrastructure for today's Internet, there are some benefits to a connection-oriented system like the circuit-switched telephone system. Because resources at the various switching locations are dedicated to providing a finite number of circuits, the quality and consistency of messages transmitted across a connection-oriented network can be guaranteed. Another benefit is that the provider of the service can charge the users of the network for the period of time that the connection is active. The ability to charge users for active connections through the network is a fundamental premise of the telecommunication service industry.



During peak periods, communication may be delayed, but not denied.

A Scalable Network Architecture

The fact that the Internet is able to expand at the rate that it is, without seriously impacting the performance experienced by individual users, is a function of the design of the protocols and underlying technologies on which it is built. The Internet, which is actually a collection of interconnected private and public networks, has a hierarchical layered structure for addressing, for naming and for connectivity services. At each level or layer of the hierarchy, individual network operators maintain peering relationships with other operators at the same level. As a result, network traffic that is destined for local or regional services does not need to traverse to a central point for distribution. Common services can be duplicated in different regions, thereby keeping traffic off the higher level backbone networks.Although there is no single organization that regulates the Internet, the operators of the many individual networks that provide Internet connectivity cooperate to follow accepted standards and protocols. The adherence to standards enables the manufacturers of hardware and software to concentrate on product improvements in the areas of performance and capacity, knowing that the new products can integrate with and enhance the existing infrastructure. The current Internet architecture, while highly scalable, may not always be able to keep up with the pace of user demand. New protocols and addressing

structures are under development to meet the increasing rate at which Internet applications and services are being added.

Providing Quality of Service

Networks must provide secure, predictable, measurable, and, at times, guaranteed services. The packet-switched network architecture does not guarantee that all packets that comprise a particular message will arrive on time, in their correct in order, or even that they will arrive at all. Networks also need mechanisms to manage congested network traffic. Congestion is caused when the demand on the network resources exceeds the available capacity. If all networks had infinite resources, there would not be a need to use QoS mechanisms to ensure quality of service. Unfortunately, that is not the case. There are some constraints on network resources that cannot be avoided. Constraints include technology limitations, costs, and the local availability of highbandwidth service. Network bandwidth is the measure of the data carrying capacity of the network. When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability. The obvious fix for this situation is to increase the amount of available bandwidth. But, because of the previously stated constraints, this is not always possible. In most cases, when the volume of packets is greater than what can be transported across the network, devices queue the packets in memory until resources become available to transmit them. Queuing packets causes delay. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.

Achieving the required Quality of Service (QoS) by managing the delay and packet loss parameters on a network becomes the secret to a successful end-to-end application quality solution. Thus, ensuring QoS requires a set of techniques to manage the utilization of network resources. In order to maintain a high quality of service for applications that require it, it is necessary to prioritize which types of data packets must be delivered at the expense of other types of packets that can be delayed or dropped.

Classification

Ideally, we would like to assign a precise priority for each type of communication. Currently, this is neither practical nor possible. Therefore, we classify applications in categories based on specific quality of service requirements. To create QoS classifications of data, we use a combination of communication characteristics and the relative importance assigned to the application. We then treat all data within the same classification according to the same rules. For example, communication that is time-sensitive or important would be classified differently from communication that can wait or is of lesser importance.

Assigning priorities

The characteristics of the information being communicated also affect its management. For example, the delivery of a movie uses a relatively large amount of network resources when it is delivered continuously without interruption. Other types of service - e-mail, for example - are not nearly as demanding on the network. In one company, an administrator might decide to allocate the greatest share of the network resources to the movie, believing that this is the priority for his customers. This administrator may decide that the impact will be minimal if e-mail users have to wait a few additional seconds for their e-mail to arrive. In another company, the quality of a video stream is not as important as critical process control information that operates the manufacturing machinery.



Using Queues to Prioritize Communication

QoS mechanisms enable the establishment of queue management strategies that enforce priorities for different classifications of application data. Without properly designed and

implemented QoS mechanisms, data packets will be dropped without consideration of the application characteristics or priority. Examples of priority decisions for an organization might include:

- Time-sensitive communication increase priority for services like telephony or video distribution.
- Non time-sensitive communication decrease priority for web page retrieval or e-mail.
- High importance to organization increase priority for production control or business transaction data.
- Undesirable communication decrease priority or block unwanted activity, like peer-topeer file sharing or live entertainment.

The Quality of Service a network can offer is a vital issue, and in some situations, it is crucial. Imagine the consequences of a dropped distress call to an emergency response center, or of a lost control signal to an automated piece of heavy machinery. A key responsibility for the network managers in an organization is to establish a Quality of Service policy and ensure that the mechanisms are in place to meet that goal.

Providing

Network

Security

The network infrastructure, services, and the data contained on network attached computers are crucial personal and business assets. Compromising the integrity of these assets could have serious business and financial repercussions. Consequences of a network security breach could include:

- Network outage that prevents communications and transactions occurring, with consequent loss of business
- Misdirection and loss of personal or business funds
- Company intellectual property (research ideas, patents or designs) that is stolen and used by a competitor
- Customer contract details that become known to competitors or made public, resulting in a loss of market confidence in the business

A lack of public trust in the business's privacy, confidentiality, and integrity levels may lead to loss of sales and eventual company failure. There are two types of network security concerns that must be addressed to prevent serious consequences: network infrastructure security and content security. Securing a network infrastructure includes the physical securing of devices that provide network connectivity and preventing unauthorized access to the management software that resides on them. Content security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. When transmitting information over the Internet or other network, the content of the individual packets is not readily known to the devices and facilities through which the packets travel. Tools to provide security for the content of individual messages must be implemented on top of the underlying protocols which govern how packets are formatted, addressed and delivered. Because the reassembly and interpretation of the content is delegated to programs running on the individual source and destination systems, many of the security tools and protocols must be implemented on those systems as well.

Security measures taken in a network should:

- Prevent unauthorized disclosure or theft of information
- Prevent unauthorized modification of information
- Prevent Denial of Service

Means to achieve these goals include:

- Ensuring confidentiality
- Maintaining communication integrity
- Ensuring availability

Ensuring Confidentiality

Data privacy is maintained by allowing only the intended and authorized recipients - individuals, processes, or devices - to read the data. Having a strong system for user authentication, enforcing passwords that are difficult to guess, and requiring users to change them frequently helps restrict access to communications and to data stored on network attached devices. Where appropriate, encrypting content ensures confidentiality and minimizes unauthorized disclosure or theft of information.

Maintaining Communication Integrity

Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted - willfully or accidentally - before the intended recipient receives it. Source integrity is the assurance that the identity of the sender has been validated. Source integrity is compromised when a user or device fakes its identity and supplies incorrect information to a recipient. The use ofdigital signatures, hashing algorithms and checksum mechanisms are ways to provide source and data integrity across a network to prevent unauthorized modification of information.

Ensuring Availability

Ensuring confidentiality and integrity are irrelevant if network resources become over burdened, or not available at all. Availability means having the assurance of timely and reliable access to data services for authorized users. Resources can be unavailable during a Denial of Service (DoS) attack or due to the spread of a computer virus. Network firewall devices, along with desktop and server anti-virus software can ensure system reliability and the robustness to detect, repel, and cope with such attacks. Building fully redundant network infrastructures, with few single points of failure, can reduce the impact of these threats. The result of the implementation of measures to improve both the quality of service and the security of network communications is an increase in the complexity of the underlying network platform. As the Internet continues to expand to offer more and more new services, its future depends on new, more robust **internetworking** architectures being developed that include all four characteristics: fault tolerance, scalability, quality of service, and security.

3.3 Example of TCP/IP operations, related protocols ports and sockets.



Operation of TCP/IP

Figure 1 indicates how these protocols are configured for communications. To make clear that the total communications facility may consist of multiple networks, the constituent networks are usually referred to as *subnetworks*. Some sort of network access protocol, such as the Ethernet logic, is used to connect a computer to a subnetwork. This protocol enables the host to send data across the subnetwork to another host, or, in the case of a host on another subnetwork, to a router. IP is implemented in all of the end systems and the routers. It acts as a relay to move a

block of data from one host, through one or more routers, to another host. TCP is implemented only in the end systems; it keeps track of the blocks of data to ensure that all are delivered reliably to the appropriate application.

Figure 1 TCP/IP concepts.

For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a subnetwork must have a unique global Internet address; this allows the data to be delivered to the proper host. This address is used by IP for routing and delivery. Each application within a host must have an address that's unique within the host; this allows the host-to-host protocol (TCP) to deliver data to the proper process. These latter addresses are known as *ports*.

Let's trace a simple operation. Suppose that an application, associated with port 1 at host A, wants to send a message to another application, associated with port 2 at host B. The application at A hands the message down to TCP with instructions to send it to host B, port 12. TCP hands the message down to IP with instructions to send it to host B. Note that IP need not be told the identity of the destination port. All it needs to know is that the data is intended for host B. Next, IP hands the message down to the network access layer (such as Ethernet logic) with instructions to send it to router J (the first hop on the way to B).

To control this operation, control information as well as user data must be transmitted, as suggested in Figure 2. Let's say that the sending process generates a block of data and passes this to TCP. TCP may break this block into smaller pieces to make it more manageable. To each of these pieces, TCP appends control information known as the *TCP header*, forming a *TCP segment*. The control information is to be used by the peer TCP protocol entity at host *B*. Examples of fields that are part of this header include the following:

- **Destination port:** When the TCP entity at B receives the segment, it must know to whom the data is to be delivered.
- **Sequence number:** TCP numbers the segments that it sends to a particular destination port sequentially, so that if they arrive out of order, the TCP entity at B can reorder them.
- **Checksum:** The sending TCP includes a code that's a function of the contents of the remainder of the segment. The receiving TCP performs the same calculation and compares the result with the incoming code. A discrepancy results if there has been some error in transmission.



Figure 2 Protocol data units (PDUs) in the TCP/IP architecture.

Next, TCP hands each segment over to IP, with instructions to transmit it to B. These segments must be transmitted across one or more subnetworks and relayed through one or more intermediate routers. This operation, too, requires the use of control information. Thus, IP appends a header of control information to each segment to form an *IP datagram*. An example of an item stored in the IP header is the destination host address (in this example, B).

Finally, each IP datagram is presented to the network access layer for transmission across the first subnetwork in its journey to the destination. The network access layer appends its own header, creating a *packet* or *frame*. The packet is transmitted across the subnetwork to router J. The packet header contains the information that the subnetwork needs to transfer the data across the subnetwork. Examples of items that may be contained in this header include the following:

- **Destination subnetwork address:** The subnetwork must know to which attached device the packet is to be delivered.
- **Facilities requests:** The network access protocol might request the use of certain subnetwork facilities, such as priority.

At router J, the packet header is stripped off and the IP header examined. On the basis of the destination address information in the IP header, the IP module in the router directs the datagram out across subnetwork 2 to B. To do this, the datagram is again augmented with a network access header.

When the data is received at B, the reverse process occurs. At each layer, the corresponding header is removed, and the remainder is passed on to the next higher layer, until the original user data is delivered to the destination application.

3.4 The IP address structure

The IP address of an electronic device is its unique identifier in a network of many devices. The device can be a PC, a router, a server, or even an IP phone. This address is used to transfer data to the different devices over a network working on IP protocol system.

Each device connected to a network must have a unique IP address. Failure to do so can give rise to serious problems, as the data transfer management devices, such as, hubs, switches, and routers, would not know where to send data. This is known as IP conflict, and can even bring down an entire network in worst cases.

The basic structure of an IP address is like xxx.xxx.xxx, where each xxx can be any number between 0 and 255. Each of these parts is stored in 8 bits. So, the maximum number of possible combinations for each group of number is 256 (i.e. each group can have any one value from the range of 0 to 255).

Each address can be technically divided into two parts. One of these parts is the network part, which represents the class of IP address that is being used in the network. The other one is the host part, which represents the unique ID of the device in the network. Let us consider the IP address 192.168.10.14 – here 192.168.10 is the network part, and represents the network. The number 14 represents the unique ID of the device in the network.

You can find out the IP address of your PC when you are connected to a network. Here's how:

- 1. Click on Start button and then on Run.
- 2. In the box named Open, type "command" (without the quotes) and hit the Enter key.
- 3. In the window that appears, type "ipconfig" (minus the quotes) and hit Enter key.

It may take a while, depending on the type of connection your PC has. Wireless connections take longer to display the IP address.

Once the prompt displays information, you will see a line like:

IP Address : 192.168.10.14

This is the IP address of your PC in the network. The value given on the right side is a sample value. Your IP address will likely be different from this one, but the format should remain similar.

3.5 Major features of IP, IP datagram.

IP Functions

In the preceding topic I described the general operation of IP and boiled down its primary job as *internetwork datagram delivery*. I also explained the most important characteristics of how IP does this job. With that as a foundation, let's now look a bit deeper, at *how* IP "gets the job done". A good way to do this is to examine the various functions that the Internet Protocol includes.

The exact number of IP functions depends on where you "draw the line" between certain activities. For explanatory purposes, however, I view IP as having four basic functions (or more accurately, function sets):

• Addressing: In order to perform the job of delivering datagrams, IP must know where to deliver them to! For this reason, IP includes a mechanism for host addressing. Furthermore, since IP operates over internetworks, its system is designed to allow unique addressing of devices across arbitrarily large networks. It also contains a structure to facilitate the routing of datagrams to distant networks if that is required.

Since most of the other TCP/IP protocols use IP, understanding the IP addressing scheme is of vital importance to comprehending much of what goes on in TCP/IP.

- **Data Encapsulation and Formatting/Packaging:** As the TCP/IP network layer protocol, IP accepts data from the transport layer protocols UDP and TCP. It then encapsulates this data into an IP datagram using a special format prior to transmission.
- **Fragmentation and Reassembly:** IP datagrams are passed down to the data link layer for transmission on the local network. However, the maximum frame size of each physical/data-link network using IP may be different. For this reason, IP includes the ability to *fragment* IP datagrams into pieces so they can each be carried on the local network. The receiving device uses the *reassembly* function to recreate the whole IP datagram again.
- Routing / Indirect Delivery: When an IP datagram must be sent to a destination on the same local network, this can be done easily using the network's underlying LAN/WLAN/WAN protocol using what is sometimes called *direct delivery*. However, in many (if not most cases) the final destination is on a distant network not directly attached

to the source. In this situation the datagram must be delivered *indirectly*. This is accomplished by routing the datagram through intermediate devices (shockingly called *routers*). IP accomplishes this in concert with support from the other protocols including ICMP and the TCP/IP gateway/routing protocols such as RIP and BGP.

3.6 The transmission control block (TCB)

Transmission Control Protocol (TCP) keeps track of different information about each connection. TCP set up a complex data structure known as Transmission Control Block (TCB) to do this, which maintains information about the local and remote socket numbers, the send and receive buffers, security and priority values, and the current segment in the queue. The Transmission Control Block (TCB) also manages send and receive sequence numbers.

TCP Sliding Window

The working of the TCP sliding window mechanism can be explained as below.

The sending device can send all packets within the TCP window size (as specified in the TCP header) without receiving an ACK, and should start a timeout timer for each of them.

The receiving device should acknowledge each packet it received, indicating the sequence number of the last well-received packet. After receiving the ACK from the receiving device, the sending device slides the window to right side.



In this case, the sending device can send up to 5 TCP Segments without receiving an acknowledgement from the receiving device. After receiving the acknowledgement for Segment 1 from the receiving device, the sending device can slide its window one TCP Segment to the right side and the sending device can transmit segment 6 also.

If any TCP Segment lost while its journey to the destination, the receiving device cannot acknowledge the sender. Consider while transmission, all other Segments reached the destination

except Segment 3. The receiving device can acknowledge up to Segment 2. At the sending device, a timeout will occur and it will re-transmit the lost Segment 3. Now the receiving device has received all the Segments, since only Segment 3 was lost. Now the receiving device will send the ACK for Segment 5, because it has received all the Segment 5.

Acknowledgement (ACK) for Segment 5 ensures the sender the receiver has succesfully received all the Segments up to 5.

TCP uses a byte level numbering system for communication. If the sequence number for a TCP segment at any instance was 5000 and the Segment carry 500 bytes, the sequence number for the next Segment will be 5000+500+1. That means TCP segment only carries the sequence number of the first byte in the segment.

The Window size is expressed in number of bytes and is determined by the receiving device when the connection is established and can vary later. You might have noticed when transferring big files from one Windows machine to another, initially the time remaining calculation will show a large value and will come down later.



We have four catagories in above example.

1) Bytes already sent and acknowledged (upto Byte 20).

- 2) Bytes sent but not acknowledged (Bytes 21-24).
- 3) Bytes the receiver is ready to accept (Bytes 25-28).
- 4) Bytes the receiver is not ready to accept (Byte 29 onwards).

The Send Window is the sum of Bytes sent but not acknowledged and Bytes the receiver is ready to accept (Usable Window).

3.7 Route discovery protocols

To enable router discovery, the IRDP defines two kinds of ICMP messages:

- The **ICMP Router Solicitation Message** is sent from a computer host to any routers on the local area network to request that they advertise their presence on the network.
- The **ICMP Router Advertisement Message** is sent by a router on the local area network to announce its IP address as available for routing.

When a host boots up, it sends solicitation messages to IP multicast address 224.0.0.2.In response, one or more router may send advertisement messages. If there is more than one router, the host usually picks the first message it gets and adds that router to its routing table. Independently of a solicitation, a router may periodically send out advertisement messages. These messages are not considered a routing protocol, as they do not determine a routing path, just the presence of possible gateways.

	Karpagam Academy of Higher Education									
	Department of Computer Applications									
	BCA (2018-2021 Batch)									
	ADVANCED NETWORKING (18CAU303)									
	UNIT- III									
S.N	Question	Option1	Option2	Option3	Option4	Answer				
0										
1	Transmission errors are usually detected at the layer of OSI model	physical	datalink	network	transport	physical				
2	Datalink layer imposes a mechanism to avoid overwhelming the receiver	flow control	error control	access control	file transfer	flow control				
3	Error control mechanism of datalink layer is achieved through a added to the end of frame.	header	trailer	address	frames	trailer				
4	The datalink layer is responsible for moving from one hop to next	packets	frames	signals	message	frames				
5	In a single bit error,how many bits in the data unit are changed?	one	two	four	five	one				
6	In a error, only one bit in the data unit are changed.	single- bit	multi-bit	burst	syntax	single-bit				
7	In a burst error,how many bits in a data unit are changed?	less than 2	2 or more than 2	2	3	2 or more than 2				
8	In a error means that 2 or more bits in the data unit have changed.	single- bit	multi-bit	burst	syntax	burst				
9	The length of the burst error is measured from	first bit to last bit	first corrupted bit to last corrupted bit	two	three	first corrupted bit to last corrupted bit				
10	Single bit error will least occur in data transmissions	serial	parallel	synchronou s	asynchronous	serial				
11	To detect errors or correct errors,we need to send with data.	address	frames	redundant bits	packets	redundant bits				
12	is used to see if any error has occurred in the message.	error correcti on	error detection	retransmiss ion	translation	error detection				

S.N	Question	Option1	Option2	Option3	Option4	Answer
ο						
13	is used to know the exact number of bits that are corrupted and their location in tne message.	error correcti on	error detection	retransmiss ion	translation	error correction
14	In block coding, we divide our message intp blocks, each of k bits, called	datawor d	codeword	message	segment	dataword
15	In block coding,the length of the block is	k	r	k+r	k-r	k+r
16	Block coding can detect only error	single	burst	multiple	multilevel	single
17	We need redundant bits for error correction than for error detection	less	more	equal	less than or equal to	more
18	The corresponding codeword for the dataword 01 is	011	000	101	110	011
19	Coding schemes are divided into broad categories	2	3	4	5	2
20	Hamming distance between two eords x and y is represented as	f(x,y)	d(x,y)	h(x,y)	e(x,y)	d(x,y)
21	The hamming distance can easily be found if we apply the operation	XOR	OR	AND	NAND	XOR
22	The hamming distance is the smallest hamming distance between all possible pairs in a set of words	minimu m	maximum	equal	not equal	minimum
23	The hamming distance d(000,011) is	1	0	2	3	2
24	To guarantee correction of upto t errors in all cases,the minimum hamming distance in a block code must be	d(min)= 2t+1	d(min)=2t -1	d(min)=2t	d(min)=t+1	d(min)=2t+ 1
25	To guarantee correction of upto s errors in all cases,the minimum hamming distance in a block code must be	d(min)= s-1	d(min)=s+ 1	d(min)=t-1	d(min)=t+1	d(min)=s+ 1
26	A simple_parity check code is a single bit error detecting code in which n= with d(min)=2	К	K*1	K-1	K+1	K+1
27	The codeword corresponding to the dataword 1111 is	11110	11111	11101	11011	11110

S.N o	Question	Option1	Option2	Option3	Option4	Answer
28	A simple_parity check code can detect an Number of errors	odd	even	prime	natural	odd
29	The hamming code is a method of	error detectio n	error correctio n	retransmiss ion	translation	error correction
30	To make the hamming code respond to a burst error of size N,we neeed to make codewords of our frame	N+1	N-1	N	0	N
31	CRC stands for	Cyclic Redund ancy Check	Cyclic Redundan cy Count	Cyclic Redundanc y Code	Cyclic Redundancy Correction	Cyclic Redundan cy Check
32	CRC is used in network such as	WAN	LAN and WAN	LAN	MAN	LAN and WAN
33	In CRC there is no error if the remainder at the receiver is	equal to the remaind er at the sender	zero	non zero	equal to the quotient at the sender	Zero
34	At the CRC checker means that the data unit is damaged.	string of O's	string of 1's	a string of alternating 1's and 0's	a non-zero remainder	a non-zero remainder
35	is a regulation of data transmission so that the receiver buffer do not become overwhelmed	flow control	error control	access control	none of the above	flow control
36	in the datalink layer separates a message from one source ti a destination or from other message to other destinations	packets	address	framing	none of the above	framing
37	is the process of adding 1 extra byte whenever there is a flag or escape character in text	byte stuffing	redundan cy	bit_stuffing	none of the above	byte stuffing
38	is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in the data.	byte stuffing	redundan cy	bit_stuffing	none of the above	bit_stuffin g
39	in the data link layer is based on automatic repeat request,which is the retransmission of data	error control	flow control	access control	framing	error control
40	At any time an error is detected in an exchange specified frames are retransmitted and process is called	ARQ	ACK	NAK	SEL	ARQ

S.N	Question	Option1	Option2	Option3	Option4	Answer
0						
41	The datalink layer at the sender side gets data from its layer	network	physical	application	transport	network
42	ARQ stands for	acknowl edge repeat request	automatic repeat request	automatic repeat quantisatio n	automatic retransmissio n request	automatic repeat request
43	Which of the following is not a data link layer function?	framing	error control	flow control	routing	routing
44	In stop and wait ARQ ,the sequence of numbers is based on	modulo- 2- arithme tic	modulo- 12- arithmeti c	modulo-N- arithmetic	other modulo- arithmetic	modulo-2- arithmetic
45	Error correction inis done by keeping a copy of the send frames and retransmitting of the frame when time expires	stop and wait ARQ	ARQ	АСК	NAQ	stop and wait ARQ
46	In the Go_Back N protocol,the sequence numbers are modulo	2 ^m	2 ^{m-1}	2 ^{m+1}	2	2 ^m
47	Piggypacking is used to improve the efficiency of the protocols.	bidirecti onal	unidirecti onal	multidirecti onal	reversedirecti onal	bidirection al
48	The send window can slide slots when a valid acknowledgment arrive	one or more	one	two	two or more	one or more
49	The upper sublayer that is responsible for flow and error control is called control	logical	media access	A and B	all the above	logical
50	MAC stands for	Media Address Control	Media Access Control	Medium Address Control	Medium Access Control	Media Access Control
51	The MAC sublayer co- ordinates the datalink task within a specified	LAN	MAN	WAN	LAN and MAN	LAN
52	The lower sublayer that is responsible for multiple access resolution is called control	Logical	media access	A and B	all the above	media access
53	In the sliding window method or flow control several frame can be at a time	transit	received	created	deleted	transit
S.N	Question	Option1	Option2	Option3	Option4	Answer
-----	--	----------------	------------------	------------------	------------------	------------------
ο						
54	The sliding window of the sender expands to the when acknowledgement are received	left	middle	right	center	right
55	Datalink layer divided into functionality oriented sublayer.	2	3	4	5	2
56	The send window in Go_Back N maximum size can be	2 ^m	2 ^{m+1}	2	2 ^{m-1}	2m-1
57	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window is	1	2	3	4	1
58	The relationship between m and n in hamming code is	n=2m-1	n=m	n=m-1	n=2m+1	n=2m-1
59	mechanism of datalink layer is achieved through added to the trailer added to the end of frame.	ARQ	ARC	Error control	Flow control	Error control
60	Thelayer at the sender site gets data from its network layer.	physical	datalink	application	transport	datalink

Polling/Selection Protocols

4.1 Character and bit protocols

A **bit-oriented protocol** is a communications protocol that sees the transmitted data as an *opaque* stream of bits with no semantics, or meaning. Control codes are defined in terms of bit sequences instead of characters. Bit oriented protocol can transfer data frames regardless of frame contents. It can also be stated as "bit stuffing" this technique allows the data frames to contain an arbitrary number of bits and allows character codes with arbitrary number of bits per character.

Synchronous framing High-Level Data Link Control is a popular bit-oriented protocol. Synchronous framing High-Level Data Link Control may work like this:

- Each frame begins and ends with a special bit pattern 01111110, called a flag byte.
- A bit stuffing technique is used to prevent the receiver from detecting the special flag byte in user data e.g. whenever the sender's data link layer encounters 5 consecutive ones in the data, it automatically stuffs 0 into the outgoing stream.

	Circuit	Operation	Orientation	Low Bit Rate	High Bit
					Rate
Point-to-	Local circuit	End-to-End	Connection	Character	Bit Oriented
point	eg Null			Oriented Idle	Continuous
	Modem cable			RQ eg Kermit	RQ eg HDLC
	Analogue	End-to-End	Connection	Character	Bit Oriented
	PSTN using			Oriented Idle	Continuous
	Modems			RQ eg Kermit	RQ eg HDLC
					or LAP-M (V.32)
	Leased	End-to-End	Connection	Character	Bit Oriented
	Digital			Oriented Idle	Continuous
	Circuit			RQ eg Kermit	RQ eg HDLC
				or Bit	or TCP
				Oriented	
				Continuous	
				RQ eg TCP	
	Leased	End-to-End	Connectionle	Bit Oriented	Bit Oriented
	Digital		SS	Continuous	Continuous
	Circuit			RQ eg IP	RQ eg IP
Multinoint	Lessed	Doll Select	Connection	Character	Bit Oriented
winipoint	Digital	I OII-Select	Connection	Idle RO eq	Continuous
/Multidrop	Circuit			RSC RSC	RO eg HDI C
·	Circuit			bbe	subset NRM
					(Normal
					Response
					Mode)
Switched	Packet	Local	Connection	Bit Oriented	,
	Switched	Significance	(Pacnet) or		
WANs		_	connectionles	Continuous	
		DTE<>DCE	S	RQ eg HDLC	
				subset LAPB	
			(datagram)	(X.25)	
		End to end	Connectionle		Bit Oriented
			SS		Continuous
			or		RQ eg HDLC

Application Domains for Selected Data Link Protocols

			connectionles	subset LAPD	
			S	extended	
			(datagram)	(Frame	
				Relay)	
	Circuit	End-to-End	Connection	Bit Oriented	
	Switched			Continuous	
				RQ eg HDLC	
				subset LAPD	
				(ISDN)	
LAN	Bus or Ring	End-to-End	Connectionle	CSMA/CD	
			SS	as in Ethernet	

4.2 Binary synchronous control (BSC) HDLC

Binary Synchronous Communication (**BSC** or **Bisync**) is an IBM character-oriented, half-duplex link protocol, announced in 1967 after the introduction of System/360. It replaced the synchronous transmit-receive (STR) protocol used with second generation computers. The intent was that common link management rules could be used with three different character encodings for messages. Six-bit Transcode looked backwards to older systems; USASCII with 128 characters and EBCDIC with 256 characters looked forward. Transcode disappeared very quickly but the EBCDIC and USASCII dialects of Bisync continued in use.

Framing

Bisync differs from protocols that succeeded it in the complexity of message framing. Later protocols use a single framing scheme for all messages sent by the protocol. HDLC, Digital Data Communications Message Protocol (DDCMP), Point-to-Point Protocol (PPP), etc. each have different framing schemes but only one frame format exists within a specific protocol. Bisync has five different framing formats.^[citation needed]

BSC Link Control Characters

Char	EBCDIC (hexadecimal)	USASCII (hexadecimal)	Transcode (hexadecimal)	Description
SYN	32	16	3A	Synchronous idle
SOH	01	01	00	Start of heading
STX	02	02	0A	Start of text
ETB	26	17	0F	End of transmission block
ETX	03	03	2E	End of text
EOT	37	04	1E	End of transmission

Unit – 4		Computer Netwo	rks Year(PG 2017-2018 Lateral Entry)
ENQ 2D	05	2D	Enquiry
NAK 3D	15	3D	Negative acknowledgement
DLE 10	10	1F	Data link escape
ITB 1F	1F (US)	1D (US)	Intermediate block check character

ACK0 and **ACK1** (even/odd affirmative acknowledgement) are encoded as two characters— DLE '70'x, and DLE / for EBCDIC, DLE 0 and DLE 1 for USASII, DLE - and DLE T for Transcode. **WABT** (wait before transmit) was encoded as DLE ", DLE ?, or DLE W.

All frame formats begin with at least two SYN bytes. The binary form of the SYN byte has the property that no rotation of the byte is equal to the original. This allows the receiver to find the beginning of a frame by searching the received bit stream for the SYN pattern. When this is found, tentative byte synchronization has been achieved. If the next character is also a SYN, character synchronization has been achieved. The receiver then searches for a character that can start a frame. Characters outside of this set are described as "leading graphics". They are sometimes used to identify the sender of a frame. Long messages have SYN bytes inserted approximately every second to maintain synchronization. These are ignored by the receiver.

A normal block ending character (ETB or ETX) is followed by a check sum (block check character or BCC). For USASCII, this is a one character longitudinal redundancy check (LRC); for Transcode and EBCDIC, the check sum is a two character cyclic redundancy check(CRC). A data frame may contain an intermediate check sum preceded by an ITB character. This ability to include intermediate check sums in a long data frame allows a considerable improvement of the error detection probability. USASCII characters are also transmitted using *odd parity* for additional checking.

Pad characters are required following a line turn-around—NAK, EOT, ENQ, ACK0, ACK1. If the transmission ends with EOT or ETX the pad follows the BCC. This pad is either all '1' bits or alternating '0' and '1' bits. The next transmission begins with a pad character which can be either of the above or a SYN.

An optional *heading* containing control information can precede data in a frame. The content of the heading is not defined by the protocol but is defined for each specific device. The heading, if present, is preceded by an SOH (start of heading) character and followed by an STX (start of text).^[4]

Text data normally follows the heading, begun by the STX, and terminated by ETX (end of text) or ETB (end transmission block).

Normal data frames do not allow certain characters to appear in the data. These are the block ending characters: ETB, ETX and ENQ and the ITB and SYN characters. The number of unique characters that can be transmitted is therefore limited to 59 for Transcode, 123 for USASCII, or 251 for EBCDIC.

Transparent data framing provides an unrestricted alphabet of 64, 128 or 256 characters. In transparent mode block framing characters such as ETB, ETX, and SYN are preceded by a DLE character to indicate their control significance (The DLE character itself is represented by the sequence DLE DLE). This technique became known as character stuffing, by analogy with bit stuffing.

Link control

The link control protocol is similar to STR. The designers attempted to protect against simple transmission errors. The protocol requires that every message be acknowledged (ACK0/ACK1) or negatively acknowledged (NAK), so transmission of small packets has high transmission overhead. The protocol can recover from a corrupted data frame, a lost data frame, and a lost acknowledgment.

Error recovery is by retransmission of the corrupted frame. Since Bisync data packets are not serial-numbered, it's considered possible for a data frame to go missing without the receiver realizing it. Therefore, alternating ACK0s and ACK1s are deployed; if the transmitter receives the wrong ACK, it can assume a data packet (or an ACK) went missing. A potential flaw is that corruption of ACK0 into ACK1 could result in duplication of a data frame.

Error protection for ACK0 and ACK1 is weak. The Hamming distance between the two messages is only two bits.

The protocol is half-duplex (2-wire). In this environment, packets or frames of transmission are strictly unidirectional, necessitating 'turn-around' for even the simplest purposes, such as acknowledgments. Turn-around involves

- the reversal of transmission direction,
- quiescing of line echo,
- resyncing.

In a 2-wire environment, this causes a noticeable round-trip delay and reduces performance.

Some datasets support full-duplex operation, and full-duplex (4-wire) can be used in many circumstances to improve performance by eliminating the turn-around time, at the added expense of 4-wire installation and support. In typical full-duplex, data packets are transmitted along one wire pair while the acknowledgements are returned along the other.

HDLC options, HDLC frame format,

HDLC (High-level Data Link Control)

HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between network points (sometimes called nodes). In HDLC, data is organized into a unit (called a *frame*) and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in what is layer 2 of the industry communication reference model called Open Systems Interconnection (OSI). (Layer 1 is the detailed physical level that involves actually generating and receiving the electronic signals. Layer 3 is the higher level that has knowledge about the network, including access to router tables that indicate where to forward or send data. On sending, programming in layer 3 creates a frame that usually contains source and destination network addresses. HDLC (layer 2) encapsulates the layer 3 frame, adding data link control information to a new, larger frame.

Now an ISO standard, HDLC is based on IBM's SDLC protocol, which is widely used by IBM's large customer base in mainframe computer environments. In HDLC, the protocol that is essentially SDLC is known as Normal Response Mode (NRM). In Normal Response Mode, a primary station (usually at the mainframe computer) sends data to secondary stations that may be local or may be at remote locations on dedicated leased lines in what is called a multidrop or multipoint network. (This is not the network we usually think of; it's a nonpublic closed network. In this arrangement, although communication is usually half-duplex.)

Variations of HDLC are also used for the public networks that use the X.25 communications protocol and for frame relay, a protocol used in both and wide area network, public and private.

PRO+

Content

Find more PRO+ content and other member only offers, here.

• E-Zine

How to prevent network downtime in the modern enterprise

In the X.25 version of HDLC, the data frame contains a packet. (An X.25 network is one in which packets of data are moved to their destination along routes determined by network conditions as perceived by routers and reassembled in the right order at the ultimate destination.) The X.25 version of HDLC uses peer-to-peer communication with both ends able to initiate

communication on duplex links. This mode of HDLC is known as Link Access Procedure Balanced (LAPB).

The following table summarizes the HDLC variations and who uses them.

HDLC SUBSET	USES		
NRM (Normal Response Mode)	Multipoint networks that typically use SDLC		
LAP (Link Access Procedure)	Early X.25 implementations		
LAPB (Link Access Procedure, Balanced)	Current X.25 implementations		
LAPD (Link Access Procedure for the Integrated Services Digital Network D channel)	ISDN D channel and frame relay		
LAPM (Link Access Procedure for Modems)	Error-correcting modems (specified as part of V.42)		

Switching and Routing in Networks

There are a number of ways to perform switching:

Different types of switching techniques are employed to provide communication between two computers. These are: Circuit switching, message switching and packet switching.

Circuit Switching

In this technique, first the complete physical connection between two computers is established and then data are transmitted from the source computer to the destination computer. That is, when a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from sender telephone to the receiver's telephone. The important property of this switching technique is to setup an end-to-end path (connection) between computer before any data can be sent. This method involves the physical interconnection of two devices. A good example of circuit switching involves the Public phone network. A data example would be the classic A/B switch!

Message Switching

In this technique, the source computer sends data or the message to the switching office first, which stores the data in its buffer. It then looks for a free link to another switching office and then sends the data to this office. This process is continued until the data are delivered to the destination computers. Owing to its working principle, it is also known as store and forward. That is, store first (in switching office), forward later, one jump at a time.

Message Switching techniques were originally used in data communications. An example would be early "store and forward" paper tape relay systems. E-Mail delivery is another example of message switching. In voice systems, you can find Voice Mail delivery systems on the Internet. The classic "forward voice mail" capability in some voice mail systems is another example.

Packet Switching

With message switching, there is no limit on block size, in contrast, packet switching places a tight upper limit on block size. A fixed size of packet which can be transmitted across the network is specified. Another point of its difference from message switching is that data packets are stored on the disk in message switching whereas in packet switching, all the packets of fixed size are stored in main memory. This improves the performance as the access time (time taken to access a data packet) is reduced, thus, the throughput (measure of performance) of the network is improved

Packet Switching techniques switch packets of data between destinations. Traditionally, this applied to X.25 techniques, but this also applies to TCP/IP and IPX/SPX routers also. Proprietary Frame Relay switches can switch voice signals.

Cell Switching

Cell Switching is similar to packet switching, except that the switching does not necessarily occur on packet boundaries. This is ideal for an integrated environment and is found within Cell-based networks, such as ATM. Cell-switching can handle both digital voice and data signals.

The X.25 Network and Supporting Protocols

X.25 is a standard suite of protocols used for packet-switched communications over a wide area network—a WAN. A protocol is an agreed-upon set of procedures and rules. Two devices that follow the same protocols can understand each other and exchange data.

History of X.25

X.25 was originally developed in the 1970s to carry voice over analog telephone lines—dialup networks. Typical applications of X.25 included automatic teller machine networks and credit card verification networks.

X.25 also supported a variety of mainframe terminal and server applications. The 1980s were the heydays of X-25 technology when it was used by public data networks Compuserve, Tymnet, Telenet, and others. In the early 90s, many X.25 networks were replaced by Frame Relay in the U.S. Many older public networks outside the U.S. continued to use X.25 until just recently. Most networks that once required X.25 now use the less complex Internet Protocol. X-25 is still used in some ATMs and credit card verification networks.

X-25 Structure

Each X.25 packet contained up to 128 bytes of data. The X.25 network handled packet assembly at the source device, the delivery, and the reassembly at the destination. X.25 packet delivery technology included not only switching and network-layer routing but also error checking and retransmission logic should delivery failures occur. X.25 supported multiple simultaneous conversations by multiplexing packets and using virtual communication channels.

X-25 offered three basic layers of protocols:

- Physical layer
- Data link layer
- Packet layer

X-25 predates the OSI Reference Model, but the X-25 layers are analogous to the physical layer, data link layer and network layer of the standard OSI model.

With the widespread acceptance of Internet Protocol (IP) as a standard for corporate networks, X.25 applications have now migrated to cheaper solutions using IP as the network layer protocol and replacing the lower layers of X.25 with Ethernet or with new ATM hardware.

X.25 is a standard used by many older public networks specially outside the U.S.

• This was developed in *1970s* by CCITT for providing an interface between public packetswitched network and their customers.

• The packet switching networks use X.25 protocol. The X.25 recommendations were first prepared in 1976 and then revised in 1978, 1980 and 1984.

• X.25 was developed for computer connections, used for terminal/timesharing connection.

• This protocol is based on the protocols used in early packet switching networks such as ARPANET, DATAPAC, and TRANSPAC etc.

• X.25 Packet Switched networks allows remote devices to communicate with each other across high speed digital links without the expense of individual leased lines.

• A protocol X.21 which is a physical layer protocol is used to specify the physical electrical and procedural interface between the host and network.

• The problem with this standard is that it needs digital signal rather than analog signals on telephone lines.

• So not many networks support this standard. Instead RS 232 standard is defined.

• The data link layer standard has a number of variations. It is designed for error detection and corrections.

• The network layer protocol performs the addressing, flow control, delivery confirmation etc.

• It allows the user to establish virtual circuits and send packets on them. These packets are delivered to the destination reliably and in order.

• X.25 is a connection oriented service. It supports switched virtual circuits as well as the permanent circuits.

• Packet Switching is a technique whereby the network routes individual packets of HDLC data between different destinations based on addressing within each packet.

• A switched virtual circuit is established between a computer and network when the computer sends a packet to the network requesting to make a call to other computer.

• Packets can then be sent over this connection from sender to receiver.

• X.25 provides the flow control, to avoid a fast sender overriding a slow or busy receiver.

```
M.THILLAINAYAKI
```

• A permanent virtual circuit is analogous to-a leased line. It is set up in advance with a mutual agreement between the users.

• Since it is always present, no call set up is required for its use.

• In order to allow the computers which do not use the X.25 to communicate with the X.25 network a packet assembler disassembler (PAD) is used.

• PAD is required to be installed along with each computer which does not use X.25.

• X.25 defines the interface for exchange of packets between a **DTE** and switch data subnetwork node.

Three Layers of X.25:

The X.25 interface is defined at three levels:

The three levels are:

(i) Physical layer (level 1)

(ii) Data link layer (level 2)

• These three layers correspond to the three lower most layers of the ISO-OSI reference model. The physical layer takes care of the interface between a computer terminal and the link which attaches it to the packet switching node.

• The X.25 defines the interface for exchange of packets between the user's machine (DTE) and the packet switching node to which this DTE is attached which is called as DCE.

• The three layers of X.25 interface are as shown in Fig.(a).

• At the physical level X.21 physical interface is being used which is defined for circuit switched data network. At the data link level, X.25 specifies the link access procedure-B (LAP-B) protocol which is a subset of HDLC protocol.

⁽iii) Packet layer (level 3).



• At the network level $(3^{rd}$ level), X.25 defines a protocol for an access to packet data subnetwork.

• This protocol defines the format, content and procedures for exchange of control and data transfer packets. The packet layer provides an external virtual circuit service.

• Fig.(b) shows the relationship between the levels of x'25. User data is passed down to X.25 level 3.

• This data then appends the control information as a header to form a packet. This control .information is then used in the operation of the protocol.

• The entire X.25 packet formed at the packet level is then passed down to the second layer i.e. the data link layer.

• The control information is appended at the front and back of the packet forming a LAP-B frame. The control information in LAP-B frame is needed for the operation of the LAP-B protocol.

• This frame is then passed to the physical layer for transmission.



Virtual Circuit Service

• With the X25 packet layer, data are transmitted in packets over external virtual circuits, The virtual circuit service of X25 provides for two types of virtual circuits,

• The virtual circuit service of X25 provides for two types of virtual circuits i.e. "virtual call" and "permanent virtual circuit".

• A virtual call is a dynamically established virtual circuit using a call set up and call clearing procedure.

• A permanent virtual circuit is a fixed, network assigned virtual circuit. Data transfer takes place as with virtual calls, but no call set up or clearing is required.

Characteristics of X.25

In addition to the characteristics of the packet switched network, X.25 has the following characteristics:

- 1. Multiple logical channels can be set on a single physical line
- 2. Terminals of different communication speeds can communicate
- 3. The procedure for transmission controls can be changed.

Multiple Logical Channels can be set on a Single Physical Line

The terminal connected to the packet switched network can communicate with multiple terminals at the same time using a single physical line. This makes it possible to set multiple logical paths called logical channels on a single physical line. Multiple communications thus takes place through these logical channels. Based on the X.25 rules, 4096 logical channel can be set on a single physical line. To enable control of 4096 logical channels there are 16 logical channel groups. Each logical channel group is divided into 256 logical channels. These channel groups are known as LCGN (Logical Channel Group Number) and LCN (Logical Channel Number).



Terminals of Different Communication Speeds can communicate

As X.25 uses the store and forward method, therefore, the communication is possible. In other words, a terminal of 1.2 Kbits/s can communicate with a host computer at 9600 bits/s through the packet switched network. When the 'telephone network or a leased line is used, this type of communication cannot be established. In other words, in these environments, the transmission speed of the sender should be the same as that of the receiver.

The reason that communication between terminals with different communication speeds is possible is that the senders and the receivers are not physically connected. Data transmission from a 1.2 Kbits/s terminal is temporarily stored in the receiving buffer of the packet switched network and the data is then passed through the network and transmitted to the host computer at 9600 bits/s.



By using the above 2 features the network can be established. By applying a higher line speed to the host computer than the terminal and setting multiple logical channels, the number of lines at the computer can be reduced.



The Procedure for Transmission Controls can be changed

It is possible to change the procedure for transmission control. As we know that X.25 uses the store and forward method, therefore, all data must be once stored in the packet switched unit. By implementing a protocol conversion function to the packet switched unit can connect the devices with different transmission control (basic procedure and X.25 protocol). With the help of this method, any terminal that cannot handle packets cannot be connected to the packet switched network. A terminal that cannot handle packets is called an NPT (Non-packet mode terminal).

		conversion C	onversion
key board	Basic Procedure	Standard Procedure	Basic Procedure
	L	X.25 network conversion of transmission	procedure

	Karpag	am Academy	of Higher Edu	cation			
	Department of Computer Applications						
	BCA (2018-2021 Batch)						
	ADVA	NCED NETWO	RKING (18CA	U303)			
		UNIT	Γ- IV				
S.No	Question	Option1	Option2	Option3	Option4	Answer	
1	IP stands for	Internet Process	Internet Program	Internet Protocol	Internet Point	Internet Protocol	
2	LLC stands for	Logical Link Control	Local Link Control	Logical Level Control	Local Level Control	Logical Link Control	
3	Lower sub layer of data link layer is responsible for	multiple access	point to point access	error detection	flow control	multiple access	
4	Multiple-access Protocol is divided into categories	two	three	four	five	three	
5	In Carrier Sense Multiple Access (CSMA), if station senses medium before trying to use it then chance of collision can be	increased	reduced	highlighte d	removed	reduced	
6	Code Division Multiple Access (CDMA) differs from Time Division Multiple Access (TDMA) because there is no	bandwidth	link	carrier	timeshari ng	timesharin g	
7	Protocol that is used to transmit data without any schedule time is	random access	controlled access	channeliza tion	media access	random access	
8	Carrier Sense Multiple Access (CSMA) is based on medium called	listen before talk	listen before sending	sense before transmit	sense before collision	sense before transmit	
9	Random access is also called the	controlled access	channeliza tion	authentica tion	contentio n methods	contention methods	
10	Time-out period is equal to maximum possible propagation delay of	Square-trip	Round-trip	Rectangula r-trip	Triangle- trip	Round-trip	

S.No	Question	Option1	Option2	Option3	Option4	Answer
11	Field of MAC frame that alerts receiver and enables it to synchronize is known as	SFD	preamble	source address	destinatio n address	preamble
12	TCP stands for	Transmissi on Control Protocol	Transfer Control Protocol	Transition Control Protocol	Transactio n Control Protocol	Transactio n Control Protocol
13	UDP stands for	Universal Datagram Protocol	User Datagram Protocol	Universal Datagram Packet	User Datagram Packet	User Datagram Protocol
14	ISN stands for	Initial Standard Number	Initial Sequence Number	Initial Socket Number	Initial Server Number	Initial Sequence Number
15	The Client program issues a request for an	active open	passive open	passive close	active close	active open
16	Ethernet was created in	1974	1975	1976	1977	1976
17	Ethernet has gone through generations.	1	2	3	4	4
18	A is a device that operates only in both physical and data link layers of the Internet model	hub	repeater	bridge	switch	switch
19	A is a device that operates only in the physical layer of the Internet model	hub	repeater	bridge	switch	repeater
20	A is a device that operates only in the physical , data link and network layers of the Internet model	hub	router	bridge	switch	router
21	is a device that operates at all the five layers	gateway	hub	bridge	switch	gateway
22	An IPv4 address is long.	16 bits	32 bits	64 bits	128 bits	32 bits
23	How many classes in IPv4 addresses?	2	3	4	5	5
24	Packets in the IPv4 layer are called	datagrams	segments	frames	stream of bits	datagrams
25	defines a device's connection to a network.	MAC Address	IP Address	Network Address	Local address	IP Address

S.No	Question	Option1	Option2	Option3	Option4	Answer
26	Addresses in are used for multicast communication.	Class A	Class B	Class C	Class D	Class D
27	A has a table used in filtering decisions	hub	repeater	bridge	switch	bridge
28	A bridge does not change the addresses in a frame	physical	logical	network	local	logical
29	In graph theory, is a graph in which there is no loop.	decision tree	spanning tree	binary tree	b-tree	spanning tree
30	A three layer switch is a	hub	router	bridge	switch	router
31	A two layer switch is a	hub	router	bridge	switch	bridge
32	Communication at network layer in the internet is	connection less	point-to- point	connection oriented	packet- switched	connection less
33	What is the abbrevation for IPV4	Inter Protocol Versus 4	Inter Position Version 4	Internet protocol version 4	Internet Position Versus 4	Internet protocol version 4
34	IPV4 provides the term 'best-effort' means that	no error control	error control	error detection	datagram	no error control
35	Packets in the IPV4 layer are called	frames	datagroup	switching	datagram s	datagrams
36	A datagram is a variable length packet consisting ofparts.	one	six	two	three	two
37	An IPv6 address isbits long.	128	126	125	127	128
38	In classless addressing,atleast columns in a routing table.	5	6	3	4	4
39	The maximum length of datagram is	512 bytes	1024 bytes	2048 bytes	65,535 bytes	65,535 bytes
40	algorithm creates a shortest path tree from a graph.	data	dakstra	define	dijkstra	dijkstra
41	layer is responsible for process- to-process delivery.	transport	physical	application	network	transport

S.No	Question	Option1	Option2	Option3	Option4	Answer
42	Internet has decided to use universal port numbers for severs called	well- unknown port	well- known port	well- known protocol	well- unknown process	well- known port
43	IANA has divided the port numbers intoranges.	six	four	five	three	three
44	a connection, is first established between the sender and receiver.	connection -oriented	connection less	token	dialog	connection -oriented
45	UDP is called	connection -oriented	check point	token	connetion less	connetionl ess
46	UDP length = IP length - 	IP length	IP breadth	IP header's length	IP header's breadth	IP header's length
47	UDP is a suitable transport protocol for	unicasting	multicastin g	nocasting	broadcasti ng	multicastin g
48	TCP groups a number of bytes together into a packet called	segment	encapsulat ion	datagram	data binding	segment
49	The acknowledgement number is	natural	whole	integers	cumulativ e	cumulative
50	flag is used to terminate the connection.	TER	FIN	URG	PSH	FIN

5.1 Network Security

Security can be defined as state of freedom from a danger, risk or attack. Information security can be defined as the task of guarding information which is processed by a server, stored on a storage device, and transmitted over a network like Local Area Network or the public Internet. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction

Introduction to AAA

AAA stands for Authentication, Authorization and Accounting. AAA are a set of primary concepts that aid in understanding computer and network security as well as access control. These concepts are used daily to protect property, data, and systems from intentional or even unintentional damage. AAA is used to support the Confidentiality, Integrity, and Availability (CIA) security concept.

Confidentiality: The term confidentiality means that the data which is confidential should remain confidential. In other words, confidentiality means secret should stay secret.

Integrity: The term integrity means that the data being worked with is the correct data, which is not tampered or altered.

Availability: The term availability means that the data you need should always be available to you.

Authentication provides a way of identifying a user, typically requiring a Userid/Password combo before granting a session. Authentication process controls access by requiring valid user credentials. After the Authentication process is completed successfully, a user must be given authorization (permission) for carrying out tasks within the server. Authorization is the process that determines whether the user has the authority to carry out a specific task. Authorization controls access to the resources after the user has been authenticated. The last one is Accounting. Accounting keeps track of the activities the user has performed in the server.

5.2 IP Security

Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.

IPsec involves two security services:

- Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.
- Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.

There are two modes of IPsec:

- Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.
- Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

5.3 Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management.

This lesson explains Encapsulating Security Payload (ESP), Encapsulating Security Payload (ESP) Header and trailer, Encapsulating Security Payload (ESP) Header and trailer fields description.

The Encapsulating Security Payload (ESP) protocol provides all the functions of Authentication Header (Authentication, Data Integrity, and anti-replay protection). The difference here is that the Encapsulating Security Payload (ESP) provides the most critical security function, data confidentiality. The benefits of using Encapsulating Security Payload (ESP) are listed below.

1) Confidentiality of Datagrams through encryption.

2) Traffic flow confidentiality using security gateways.

3) Authentication of data origin using digital certificates.

4) Anti-replay services using sequence number mechanism.

Encapsulating Security Payload (ESP) Header



Figure 7: Encapsulating Security Payload (ESP) Header

Security Parameter Index (SPI): Security Parameter Index (SPI) field in the Encapsulating Security Payload (ESP) header along with the destination address, and the IPsec protocol are used to uniquely identify the SA that applies to this packet.

Sequence Number: The sequence number in the Encapsulating Security Payload (ESP) header provides antireplay services to Encapsulating Security Payload (ESP).

Protected Data: Protected Data field in the Encapsulating Security Payload (ESP) heade is the actual data being protected by Encapsulating Security Payload (ESP). The length of this field is variable and depends on the size of the data. The protected data field also contain any initialization vector for encryption algorithm.

Padding: Block ciphers require that plaintext be padded to a multiple of the block size. If any padding is needed, it follows immediately after the payload data in the padding field.

Pad Length: Pad Length specifies the length of the padding.

Next Header: The next header field indicates what type of data is in the payload data field.

Authentication Data: The authentication data field contains an integrity check value for the Encapsulating Security Payload (ESP) packet.

Authentication is the process which allows a sender and receiver of information to validate each other. If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple. The simplest form of authentication is the transmission of a shared password between entities wishing to authenticate each other. Today's authentication methods uses some of the below factors.

1) What you know

An example of this type of Authentication is a "Password". The simple logic here is that if you know the secret password for an account, then you must be the owner of that account. The problems associated with this type of Authentication is that the password can be stolen, someone might read it if you wrote it somewhere. If anyone came to know your password, he might tell someone else. If you have a simple dictionary password, it is easy to crack it by using password cracking software.

2)WhatyouhaveExamples of this type of Authentication are smart cards, tokens etc.The logic here is if you havethe smart card with you, you must be the owner of the account.The problems associated with

M.THILLAINAYAKI

DEPT OF CS, CA & IT KAHE

this type of authentication are you might lose the smart card, it can be stolen, or someone can duplicate the smart card etc.

3) What you are

Examples of this type of authentication are your fingerprint, handprint, retina pattern, voice, keystroke pattern etc. Problems associated with this type of authentication are that there is a chance of false positives and false negatives. Chances are there that a valid user is rejected and an invalid user is accepted. Often people are not comfortable with this type of authentication.

Access control can be a policy, a software, or a hardware device which is used to allow or deny access to a resource. Access control can be by using devices like biometric device, switches, routers, Remote Access Service (RAS), virtual private networks (VPNs), etc. Access control can also be implemented on File System level like Microsoft's New Technology File System (NTFS), GNU/Linux's ext2/ext3/ext4 etc. The following are the three main concepts of Access Control.

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

A Virtual Private Network (VPN) can be viewed as a private network which is connected through a public network. Virtual Private Networks (VPNs) are used to connect LANs together across the Internet. Using Virtual Private Network (VPN) technologies, remote users can connect to enterprise network securely over the public internet as if their computers are physically connected to the network.

Virtual Private Network (VPN) connections use either Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol/Internet Protocol security (L2TP/IPSec) over internet. Internet connections are usually cheaper than leased line, Dial-up, ISDN or similar type of connections. Since Internet is the connection medium, Virtual Private Network (VPN) can save huge telecom costs.

Point-to-Point Tunneling Protocol (PPTP)

PPTP was created by Microsoft and available since Windows NT 4.0 Routing and Remote Access Services. Point-to-Point Tunneling Protocol (PPTP) encrypts the data it encapsulates, but the header is not encrypted. Since the VPN header is not encrypted, an eavesdropper can read the VPN header but the data is somewhat secure since the contents are encrypted.

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is another VPN tunneling protocol which is used together with Internet Protocol Security (IPSec). IPSec encrypts the entire L2TP packet. A advantage of L2TP over PPTP is that eavesdroppers cannot identify that a VPN is in use, because IPSec encrypts the L2TP header information also. Hence L2TP/IPSec protocol is much more secure than Point-to-Point Tunneling Protocol (PPTP).

IPSec policies determines which IP traffic should be secured and which IP packets should be not be secured, what type of security should be appplied to the IP packets. IPSec polices contain IPSec rules and IPSec rules contain filter lists and filter actions.

There are three default IPSec policies in Windows Server 2003. We can assign only one policy at a time.

Client (Respond Only): Client (Respond Only) IPSec policy allows the computer to attempt unsecured communications first and switch to secured communications if requested.. This policy contains the default response rule, which creates dynamic IPSec filters for inbound and outbound traffic based on the requested protocol and port traffic for the communication the system is securing.

Server (Request Security): Server (Request Security) IPSec policy configured systems can request secure IP communications whenever possible but will fall back to clear-text IP communication if non IPSec-aware computers or systems not configured using a Client (Respond Only) policy request communication. Secure Server (Require Security): Systems configured with a Secure Server (Require Security) IPSec policy require secure communications. The filters for this policy require all communication from the given system to be secure, with the exception of the initial inbound communication request. Non IPSec aware devices and the devices which are not configured with Client (Respond Only) IPSec policy will not be able to communicate with a device configured with Server (Request Security) IPSec policy.

The default polices can be viewed at group policy editor. If you are working in a Windows 2003 Domain Controller, select Start > Programs > Administrative Tools > Domain Controller Security Policy.

🚡 Default Domain Controller Security Settings	
<u>File Action View Help</u>	
Security Settings Account Policies Local Policies Event Log System Services Gamma Registry Gamma File System File System Dublic Key Policies Software Restriction Policies IP Security Policies on Active Directory (omnisecu.com)	Name A Server (Request Security) Client (Respond Only) Secure Server (Require Security)

Figure 9: Domain Controller Security Policy MMC snap-in.

S.N o	Question	Option1	Option2	Option3	Option4	Answer
1	TCP is responsible for	hop-to-hop	process-to- process	host-to- host	node-to- node	process-to- process
2	FTP stands for	File Transmission Protocol	File Transfer Protocol	File Translation Protocol	File Transition Protocol	File Transfer Protocol
3	TELNET stands for	Transfer Network	Transfer Node	Terminal Network	Terminal Node	Terminal Network
4	is the Port number for Terminal Network	20	21	23	25	23
5	RPC stands for	Random Procedure Call	Remote Procedure Call	Rapid Procedure Call	Reverse Procedure Call	
6	is the port number for Remote Procedure Call	111	7	9	79	111
7	HTTP stands for	Hyper Text Transfer Protocol	Hyper Text Transmission Protocol	Hyper Text Transition Protocol	Hyper Text Translation Protocol	Hyper Text Transfer Protocol
8	is the Port number for HTTP.	7	9	79	80	80
9	TCP transmits data in mode	duplex	simplex	full duplex	half duplex	full duplex
10	In TCP, one end can stop sending data while still receiving data called	active open	passive open	half close	full close	half close
11	RTO stands for	Retransmissi on Time Out	Repair Time Out	Repeat Time Out	Retransfer Time Out	Retransmissi on Time Out

S.N	Question	Option1	Option2	Option3	Option4	Answer
12	DTT stands for	Dound Trin	Dound Transfor	Donid Trip	Dotational	Dound Trin
12		Time	Time	Time	Trip Time	Time
13	The opened, closed and shrunk activities of a window is controlled by	sender	receiver	transmitter	controller	receiver
14	The window size is determined by	maximum(rwnd, cwnd)	maximum(swnd , cwnd)	minimum(swnd, cwnd)	minimum(rwnd, cwnd)	minimum(rwnd, cwnd)
15	Which of the tool is not included for error detection and correction in TCP?	checksum	acknowledgem ent	flag	time-out	flag
16	If more than one station tries to send, there is conflict called	congestion	collision	contention	traffic	collision
17	The value of RTO is dynamic in TCP and is updated based on segme nt.	RTO	RTT	АСК	none	RTT
18	An ACK segment,if carrying data consumes no sequence number.	no	2	3	5	no
19	SCTP stands for	String Control Transmission Protocol	Stream Control Transmission Protocol	Stack Control Transmissi on Protocol	Signal Control Transmissi on Protocol	Stream Control Transmission Protocol
20	TCP is	message oriented	byte oriented	bit oriented	text oriented	byte oriented
21	UDP is	message	byte oriented	bit	text	message
	protocol	oriented		oriented	oriented	oriented

S.N	Question	Option1	Option2	Option3	Option4	Answer
0						
22	is a protocol combines the best features of TCP and UDP	SCTP	SNMP	SMTP	FTP	SCTP
23	WWW stands	Web Wide	World Wide	Wide	World	World Wide
_	for	World	Web	World Web	Wise Web	Web
24	SMTP stands for	Simple Mail Transfer Protocol	Simple Message Transfer Protocol	Single Mail Transfer Protocol	Single Message Transfer Protocol	Simple Mail Transfer Protocol
25	is a supporting program that is used by other programs such as email.	НТТР	DNS	FTP	SMTP	DNS
26	DNS stands for	Domain Name Source	Domain Name Service	Domain Name System	Domain Name Sender	Domain Name System
27	In a name space, a name is assigned to an address.	Flat	Hierarchical	Fully Qualified	Partially Qualified	Flat
28	In a name space, ech name is made of several parts	Flat	Hierarchical	Fully Qualified	Partially Qualified	Hierarchical
29	If a label is terminated by a null string, it is called name space	Flat	Hierarchical	Fully Qualified	Partially Qualified	Fully Qualified
30	If a label is not terminated by a null string, it is called name space	Flat	Hierarchical	Fully Qualified	Partially Qualified	Partially Qualified

S.N	Question	Option1	Option2	Option3	Option4	Answer
31	A full domain name is sequence of labels seperated by	colons	Semicolons	dots	commas	dots
32	URL stands for	Uniform Resource Location	Uniform Resource Locator	Uniform Remote Location	Uniform Remote Locator	Uniform Resource Locator
33	The URL defines things.	two	three	four	five	four
34	The is the client/server program used to retrieve the document.	protocol	host	port	path	protocol
35	The is the computer on which the inforation is located.	protocol	host	port	path	host
36	The documents in WWW can be grouped into categories	two	three	four	five	three
37	is fixed content document that is created and stored in a server	static document	dynamic document	active document	passive document	static document
38	is created by a web server whenever the browser requests the document	static document	dynamic document	active document	passive document	dynamic document
39	For many applications, a program or script to be run at the client side is called	static document	dynamic document	active document	passive document	active document

S.N	Question	Option1	Option2	Option3	Option4	Answer
ο						
40	is a language is used for creating web page.	Pascal	С	C++	HTML	HTML
41	HTML stands for	Hyper Text Markup Language	Hyper Text Model Language	Hyper Transmissi on Markup Language	Hyper Transmissi on Model Language	Hyper Text Markup Language
42	CGI stands for	Computer Gateway Interface	Common Gateway Interface	Computer Gateway Informatio n	Common Gateway Informatio n	Common Gateway Interface
43	Which of the following tag is used for underline the text	<l></l>		<u>></u>	<i></i>	<u></u>
44	documents are sometimes referred to as server site dynamic documents.	static documents	dynamic documents	active documents	passive documents	dynamic documents
45	Which of the following tag is used to make the text Italic	<l></l>		<u>></u>	< >	< >
46	HTTP is a protocol.	application layer	presentation layer	physical layer	transport layer	application layer
47	In the network HTTP resources are located by	unique resource locator	uniform resource identifier	unique resource identifier	uniform resource locator	uniform resource identifier
48	HTTP client requests by establishing a connection to a particular port on the server.	user datagram protocol	transmission control protocol	broader gateway protocol	Internet Protocol	transmission control protocol
49	FTP server listens for connection on port number	20	21	23	25	21

S.N o	Question	Option1	Option2	Option3	Option4	Answer
50	The communication protocol used by Internet is	FTP	TELNET	НТТР	TCP/IP	TCP/IP