M.Sc. (C.S.)- 11

VARDHAMAN MAHAVEER OPEN UNIVERSITY, KOTA

Data Communications and Networks

Course Development Committee

Chaiman

Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University Kota

Convener / Coordinator

Prof. (Dr.) D.S. Chauhan
Department of Mathematics
University of Rajasthan Jaipur

Member Secretary / Internal Coordinator

Sh. Rakesh Sharma
Assistant Professor (Computer Application)
V.M. Open University Kota

Members

1. Prof. (Dr.) Neeraj Bhargava
M.D.S. University Ajmer
2. Dr. (Mrs.) Madhavi Sinha
BITS Jaipur
3. Prof. (Ms.) Swati Chandey
IIIM Jaipur
4. Prof. (Dr.) D.P. Sharma Jaipur
5. Sh. Rajeev Shrivastava
Director (Voc. Courses)
LBS PG College Jaipur

Editing and Course Writing

Editor

Sh. Rajeev Shrivastava Jaipur
Director(Vocational Courses) LBS PG College Jaipur

Writers

1. Sh. N.K. Joshi
MIMT Kota
2. Sh. Arvind Sharma
DAV School Society Kota
3. Mrs. Sunita Chaudhary
Banasthali Vidyapith Newai
4. Mrs. Poonam Kshatriya
Banasthali Vidyapith Newai
5. MS. Anju Sharma
BITS Jaipur

Academic and Administrative Arrangement

Prof. (Dr.) Naresh Dadhich	**Prof.(Dr.) M.K. Ghadoliya**	**Sh. Yogendra Goyal**
Vice Chancellor Vardhaman Mahaveer Open University	Director Academic	In Charge Material Production & Distribution

Course Production

Sh. Yogendra Goyal
Assistant Production Officer
Vardhaman Mahaveer Open University

Production: February 2010 **ISBN No. : 13/978-81-8496-198-0**

Printed and published on behalf of Registrar, VM Open University Kota.
Printed by The Diamond Printing Press, Jaipur, 500 Copies

M.Sc. (C.S.)- 11

VARDHAMAN MAHAVEER OPEN UNIVERSITY, KOTA

Index

Data Communications and Networks

UNIT 1

TRANSMISSION TERMINOLOGY

Structure of the unit

1.0 OBJECTIVES

After completing this unit you will learn

- About Data comunication
- How Data are transmitted over network
- What various Media needed for communication

1.1 INTRODUCTION

Data communication means transfer of data from one device to another via some form of transmission medium. A data communication system must transmit data to the correct destination in an accurate and timely manner. The five components that make up a data communication system are the message, sender, receiver, medium, and protocol.

Text, numbers, images, audio, and video are different forms of information.

Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.

A network is a set of communication devices connected by media links. In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link. Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.

A network can be categorized as a local area network (LAN), a metropolitan-area network (MAN), or a wide area network (WAN).

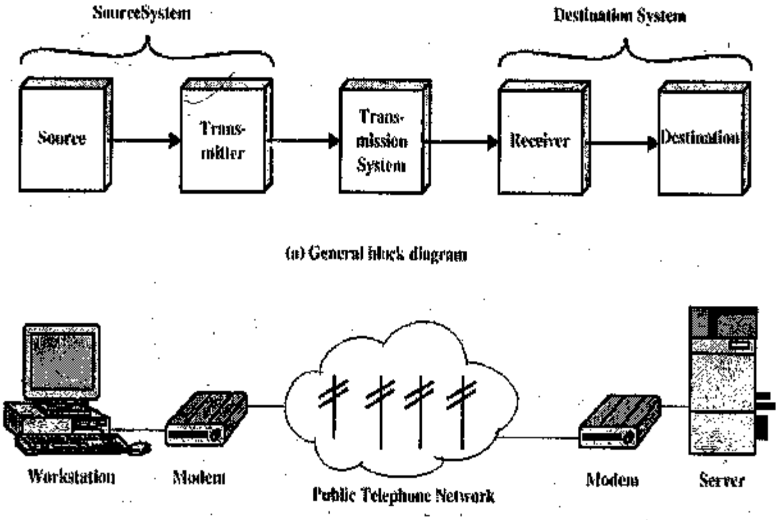
1.2 COMPONENTS OF DATA COMUNICATION

What is a Data Communications Network

It is an infrastructure that contains connection nodes and transmission pathways which allow the reliable exchange of data between connected parties

It has the following components

- **Source** - Generates data to be transmitted
- **Transmitter** - Converts data into transmittable signals
- **Transmission System** - Carries data
- **Receiver** - Converts received signal into data
- **Destination** - Takes incoming data



(a) General block diagram

(b) Example

1.3 TERMINOLOGIES

Data communication can be describe through various different terminologies.

Terminology- 1

Transmitter

Receiver

Medium

Guided medium e.g. twisted pair, optical fiber

Unguided medium e.g. air, water, vacuum

Terminology -2

Direct link - No intermediate devices

Point-to-point - Direct link Only two devices share link

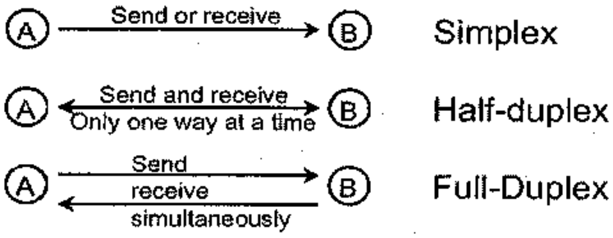
Multi-point - More than two devices share the link

Terminology - 3

Simplex - One direction e.g. Television

Half duplex - Either direction, but only one way at a time e.g. police radio

Full duplex - Both directions at the same time e.g. telephone



Shannon's Data Communciation Model

This model have Six Components –

- An **information source** generates a message
- A **transmitter** encodes the message as a signal

- The signal is transmitted over a **communications channel** — a medium that bridges the distance between the transmitter and the receiver
- A source of **noise** is usually present in the communication channel — this is a random element that modifies the encoded signal in unpredictable ways
- The **receiver** extracts a signal from the communication channel and converts it back into the form of a message
- The **destination** receives the message

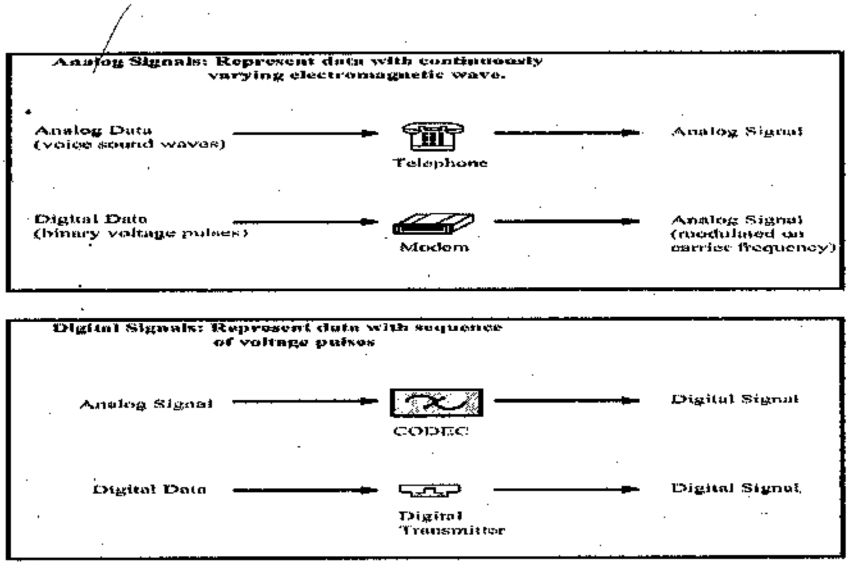
1.4 ANALOG AND DIGITAL TRANSMISSION

- Data: Entity that conveys meaning
- Signal: Electric/Electronic encoding (representation) of data
- Signaling: Act of propagating the signal along a suitable medium
- Transmission: Communication of data by the propagation and processing of signals

Analog Data and Digital Data

- Analog - Continuous values within some interval e.g. sound, video
- Digital – Discrete values e.g. text, integers

Analog and Digital Data Transmission


Analog Signals: Represent data with continuously varying electromagnetic wave.
Analog Data (voice sound waves)
Telephone
Analog Signal
Digital Data (binary voltage pulses)
Modem
Analog Signal (modulated on carrier frequency)
Digital Signals: Represent data with sequence of voltage pulses
Analog Signal
CODEC
Digital Signal
Digital Data
Digital Transmitter
Digital Signal

Above shown Diagrams are the example of Analog and Digital Transmission

Transmission techniques can be analog or digital, With analog transmission, signals are transmitted without regard to content; with digital transmission, the content of message could be interpreted to aid in faithful transmission. Important distinction is in the manner signal attenuation is handled at repeater / amplifiers. Analog - Attenuated signal is amplified and retransmitted. Digital - Data encoded in attenuated signal is recovered, a new signal is generated encoding that data, and retransmitted

Digital signals always digitally transmitted, but analog signals can be transmitted either way (assuming the signal carries digital data)

1.5 TRANSMISSION IMPAIRMENTS

Transmission impaiments can be defined as –

- signal corruption during transmission
- Attenuation

  - the strength of a signal falls off with distance
  - varies as a function of frequency
- Delay distortion
  - the velocity of propagation of a signal through a guided medium varies with frequency
- Noise
  - Thermal noise
- White noise
- Intermodulation noise
  - when two signals at different frequencies are mixed in the same medium, sum or difference of original frequencies or multiples of those frequencies can be produced, which can interfere with the intended signal
- Crosstalk
  - when there is an unwanted coupling between signal paths
- Impulse noise
  - irregular pulse or noise spikes of short duration and of high amplitude
  - external electromagnetic disturbances

Noise

- In the transmission of information errors are thought of as noise.
- The term comes from the days of radio, where the transmission errors literally resulted in a noisy radio broadcast.
- Noise is viewed as a (typically) random process.

Characteristics of Noise

- Spectral Signature
  - White noise: frequency independent
  - Pink noise: resonant peaks, noise spectrum
- Statistical Distributions – Repetitive Sampling
  - Continuous
- Gaussian
- Ricean
  - Discrete
- Poisson
  - Error Probability
  - Reference
- Mean-Square Fluctuations
  - Thermal: $<\Delta i2> = 4kT/R \text{ x } B$
  - Shot: $<\Delta i2> = 2eI \text{ x } B$
  - Multiple noises

Impedance

- Complex and Frequency Dependent
  - Stray capacitance and inductance

- Impedance Matching
  - Power delivered to the load
  - Reflection
  - Smith chart
  - Transmission line stub

Channel Properties

- Bandwidth - how much information can travel through it in a given amount of time. We often measure this in megahertz, but more intuitively we use bits/second.
- Latency, how long does it take to get from one end to another.
- Signal to noise ratio (SNR). The ratio of signal to noise expressed in decibels

1.6 TRANSMISSION MEDIA

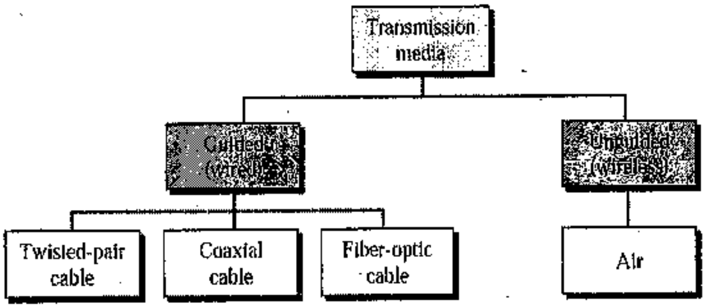
Transmission media used to provide a connection between sender and receiver to exchange information are generally grouped into two major categories namely **guided** and **unguided**.

Guided

Signals are transmitted via a physical and tangible guide between the communicating points. These include twisted pair telephone cable, optical fiber, waveguide, and coaxial cable.

Unguided

Physically, there is no direct physical connection between two points such as microwave and satellite links. Your mobile phone also uses unguided transmission medium



Wire pairs or telephone wire

Wire pairs are the most common medium in short distance such as connecting computer port to modem or telephone set to telephone exchange. The modular telephone jack installed in your house makes use of telephone wires. The wires are made of copper and coated with insulating material like PVC. The cable is highly reliable if it is protected by telephone duct. The transmitted signal relies on the movement of electronics. It is manufactured in twisted wire pairs in order to reduce crosstalk. You usually experience this effect while talking to your friends over the phone and hear a very low background voice. The bandwidth of an ordinary telephone wire is limited to 10KHz and is further limited to 3300 Hz if it is used in Public Switching Telephone Network(PSTN). Higher bandwidth will be chopped by the Switch. That is to say, even the telephone line can support up to 10 Mbps, the CODER (switch coder and decoder) will convert the analog signal into 8K (sampling rate) x 8 bits (256 levels) = 64 Kbps signal internally.

It is the cheapest transmission medium and costs around 2 dollars per meter depending on the quality, shielding and number of wires. The typical number of wires in the cable is two (Twist) or four(Quad). To support wider area, Using the Shannon's theory, the maximum transmission speed per link can be over 10Mbits per second, which of course depends on the medium bandwidth and the distance between two end points. Figure shows a few examples of wire pairs.

Local Area Network (LAN) can support transmission rates over 16 Mbps or even 100 Mbps over twisted telephone wires. This type of telephone cable is Category 5 cable, which supports this speed at a short distance. If you subscribe Interactive TV (ITV), they will replace your telephone cable by quad Category 5 cable to support voice and video.

There are two types of twisted-pair cables: unshielded twisted-pair (UTP) and shielded twisted pair (STP).

UTP using 10BaseT specification is the most popular type twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length is 100 meters (328 feet). This type of cable is used in creating standards that apply to a variety of building and wiring situations and ensure consistency of products for customers.

These standards include:

- Category 1 for traditional UTP Telephone cable which can carry voice but not data;
- Category 2 (consists of four twisted-pairs) for data transmission up to 4 Mbps;
- Category 3 (consists of four twisted-pairs with three twist per foot) for data transmission up to 10 Mbps;
- Category 4 (consists of four twisted-pairs) for data transmission up to 16 Mbps; and
- Category 5 (consists of four twisted-pair of copper wire) for data transmission up to 100 Mbps).

One potential problem with UTP is Crosstalk. Crosstalk is defined as signals from one line getting mixed with signals from another line. Shielding is used to reduce crosstalk.

STP has excellent shielding to protect transmitted data from outside interference. The connector for TP cables knows as RJ-45 connector. It look alike RJ-11 telephone connector, but there is difference between them. RJ-45 houses eight cable connections, while RJ-11 only houses four.

Coaxial cable

It is basically a **single wire** surrounded by a tube-shaped conductor of solid copper. The signal is transmitted by use of microwave rather than electronics. Because of high bandwidth (up to 350 MHZ with theoretical data rate up to 4~500 Mbps), it can support very high speed for data travelling. Coaxial cable is used for long distance communication such as Ethernet (CSMA/CD) and TV system between the antenna and TV set. Coaxial cable can be grouped into two types: broadband and baseband. In baseband transmission, digital signal like Manchester Code will be used to carry data along the channel, which relies on voltage fluctuations. In Broadband transmission, the digital data is modulated into different frequency channels separated by frequency guardbands. Because of wider bandwidth and more frequency channels, broadband transmission can support a mixture of signals such as voice and video. The cost of coaxial cable is more expensive than telephone wire. Baseband coaxial cable also allows the DC voltage to pass, which is necessary for **collision detection** in Ethernet network.

Four-wire telephone cable is regarded as **quad** with individually insulated and housed in a jacket. In Local Area Network, coaxial cable is called **Thick Wire** and Telephone Wire is **Thin Wire**. If the coaxial cable is damaged, the signal will attenuate sharply. This prevents the third party to tap information.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cable. Attenuation is the loss of signal strength which begins to occur as the signal travels further along a copper cable. The stranded, protective sleeve can absorb stray electronic signals so that they do not affect data being sent over the inner copper cable. For this reason, coaxial is a good choice for longer distances and for reliably supporting higher data rates which less sophisticated equipment. There are two types of coaxial cables Thinnet and Thicknet.

Thinnet is very flexible with about 0.25 inch thick. It is commonly used in every network installation. Thinnet can carry signal up to 185 meters (607 feet) before the signal starts to suffer from attenuation.

Thicknet is a relatively rigid cable about 0.50 inch thick. It is sometimes referred to as Standard Ethernet because it was the first cable used with poupular ethernet architecture. Thicknet can carry signal up to 500 meters (about 1,640 feet). Because of this distance ability, thicknet is usually used as a Backbone to connect several smaller thinnet-based networks.

Optical Fiber

It is a popular high bandwidth transmission medium and is used in backbone communication. Signal is transmitted by use of light through the glass fiber. It provides an electrical isolation and totally reduces electromagnetic interference or noise by surrounding equipment. Unlike telephone wire, installing and connecting the fibers requires special equipment. The transmission rate can exceed 2Gbps, nowdays around 6 ~8Gbps and is the highest transmission medium in the world. Recently, Telecom is laying fiber optic cables to provide data superhighway to support personal video services. It is expected that the future communications network will consist of one optical fiber with coaxial cable as the backbone within the building. The terminator erected around each three stories will provide a transmission bandwidth to each household at 20Mbps. At that you can use it to watch movie, shopping, a real e-commerce world.

A typical circuit that converts the digital signal to light travelling along the optical fiber. Here, the electronic signals are converted into light signals passing along the optical fiber and received by the remote. The remote then converts the light signals into electronic signals. Note that light emitting diode and photo diode are used to convert the electronics signal and accept the light signal.

Unguided transmission media

Microwave relays

It consists of transmission tower responsible for transmitting or repeating the signal for each hop (the distance is around 30 Kilometers to 50 Kilometers). The microwave uses the line of sight (the received tower can be visual by the transmitted tower) transmission. The transmission rate can be up to 250Mbps. The transmission quality however is subject to weather changes. The use of microwave is ideal for short-haul and high bandwidth applications due to no cabling cost once the transmission tower is built.

Satellite

The use of Satellite is to extend the coverage area. Signal is transmitted up and down between ground stations. The satellite is therefore used as a repeater for re-generating the signal. Here, a transmit signal is reflected by the satellite to cover a region on the earth. The characteristics are:

Microwave transmission (above 1000 MHz). It uses bandwidth between 4-6 GHZ, C-band, 12-14 GHz, Ku-band and also the 20-30 GHz
Signal requires amplification due to attenuation after travelling from the ground station to the satellite and vice versa.
Similar to microwave, the transmission quality is also subject to weather changes.
There will be a time delays between the sender and receiver and is typical 70 ms for a single hup.

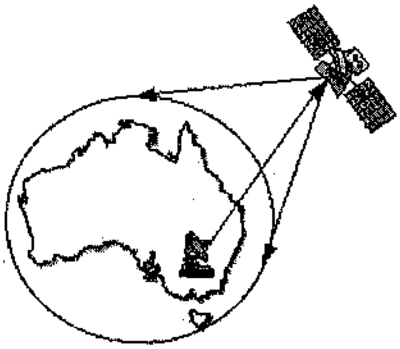
WIRELESS COMMUNICATION

If transmission lines are very useful in populated areas like cities, wireless communication is more efficient to interconnect isolated houses or towns in rural areas. The best example is Nunavut, the Canadian Inuits State, where the 25,000 inhabitants of a 200,000 km^2 area are connected via satellite communication. Of course, in these cases it is less expensive since long fibre lines and repeaters usually are not cheap. But the cost factor is not the only one that dictates the choice between transmission lines and electromagnetic radiation: in any mobile communication, transmission lines obviously cannot be used. Wireless communication is a recent but well developed way as mobile phones show. There are 2 types of media: on one hand, microwaves used for satellites, radios and mobile phones; on the other hand, infra-red ray used for remote control or HP calculators.

MICROWAVES

They cover a part of the UHF Band and all of the SHF Band; radios waves cover the other part of UHF and the VHF Band.

In terrestrial communication, antennas are used to emit and receive the microwaves. They usually are at the top of buildings to cover the wider area they can and to avoid obstacles to the propagation. Microwaves are sometimes used to replace coaxial cables or fibre optic in long-haul telecommunications because they do not need so much amplifiers and repeaters, although antennas require line-of-sight transmission. Moreover atmospheric conditions like rainfall increase losses and interferences.



In satellite microwaves, the satellite acts as a relay station between the emitting and the receiving antennas, which are usually parabolic shaped. There are 2 common configurations: point-to-point connecting two specific antennas, and point-to-multipoint where every receiver in the 'lightened' zone can capture the signal. Therefore security in a sense of confidentiality is not ensured with this medium. If satellite is already used in television distribution, it may be used by individual business users with a price as high as the complexity of the technology. Nevertheless low-cost system has appeared with VSAT (Very Small Aperture Terminal), where a number of subscribers share a satellite transmission capacity. Satellite communication allows large bandwidth (up to 100Mb/s). Eutelsat is for example able to provide an access to internet with a classical parabolic antenna at 45Mb/s. However emitting antennas are often expensive leading to the use of transmission lines in a sending way.

A complementary service could be provided by new 'satellite-plane' set up by Angel Technologies (Missouri). These jets, known as HALO (High Altitude Long Endurance), could fly at 16,700m 24H/24 since they should be automated. They could be used for high speed requiring services such as teleconferencing for a good price.

INFRARED

Point-to-point infrared is achieved using infrared light transmitters/receivers (transceivers). It may be useful to connect the buildings, which cannot be linked by electrical lines (e.g. over a street), but also in large rooms submitted to RFI and EMI. Of course, nothing must interfere with the infrared ray; it is why rain and smoke can reduce the signal. Therefore, the transmission is only available on tens of metres, even if LASER could transmit up to 2km.

1.7 SUMMARY

In this unit we have learnt about data communication basics. Types of communication, communication media, Disturbances in transmission. Has also been discussed.

1.8 UNIT END QUESTIONS

1. Define full duplex with example.
2. Differentiate between digital and analog transmission
3. what is attenuation, distortion.
4. Describe infrared and coaxial cable.

UNIT 2

DATA ENCODING & COMMUNICATION TECHNIQUES

Structure of the unit

2.0 OBJECTIVES

After completing this unit you will learn

- About Data Encoding techniques
- Various types of modulation techniques
- Error Detection Techniques

2.1 INTRODUCTION

Data must be transformed to electromagnetic signals. Data can be analog or digital before transmission. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. Analog data take on continuous values. Digital data take on discrete values. In data communications, we commonly use periodic analog signals and nonperiodic digital signals.

A signal is periodic if it consists of a continuously repeating pattern.

Each sine wave can be characterized by its amplitude, frequency, and phase. Frequency and period are inverses of each other. A time-domain graph plots amplitude as a function of time.

A frequency-domain graph plots each sine wave's peak amplitude against its frequency.

By using Fourier analysis, any composite signal can be represented as a combination of simple sine waves. The spectrum of a signal consists of the sine waves that make up the signal.

The bandwidth of a signal is the range of frequencies the signal occupies. Bandwidth is determined by finding the difference between the highest and lowest frequency components.

Bit rate (number of bits per second) and bit interval (duration of 1 bit) are terms used to describe digital signals. A digital signal is a composite signal with an infinite bandwidth.

2.2 DATA ENCODING

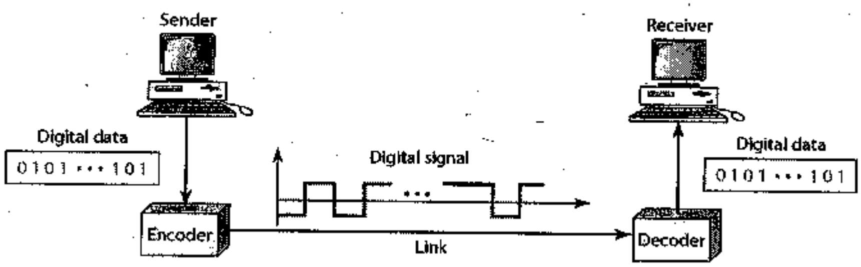
Line coding is the process of converting binary data to a digital signal. The number of different values allowed in a signal is the signal level. The number of symbols that represent data is the data level. Bit rate is a function of the pulse rate and data level.

Line coding methods must eliminate the IC component and provide a means of synchronization between the sender and the receiver. Line coding methods can be classified as unipolar, polar, or bipolar. NRZ, RZ, Manchester, and differential Manchester encoding are the most popular polar encoding methods.

AMI is a popular bipolar encoding method. Block coding can improve the performance of line coding through redundancy and error correction. Block coding involves grouping the bits, substitution, and line coding. 4B/5B, 8B/10B, and 8B/6T are common block coding methods.

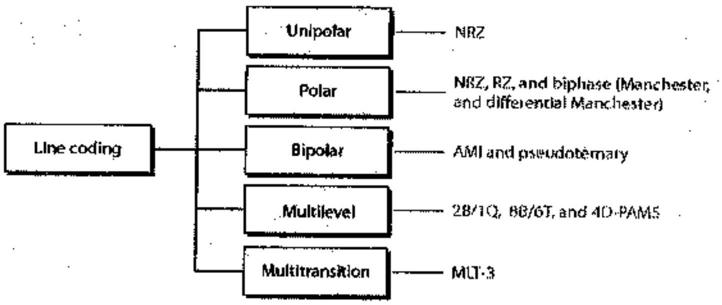
Analog-to-digital conversion relies on PCM (pulse code modulation).

PCM involves sampling, quantizing, and line coding.

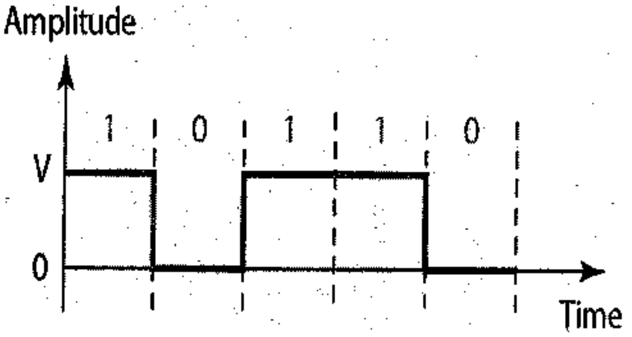


Line coding and decoding

Line coding schemes


Line coding
Unipolar
NRZ
Polar
NRZ, RZ, and biphase (Manchester, and differential Manchester)
Bipolar
AMI and pseudoternary
Multilevel
2B/1Q, 8B/6T, and 4D-PAM5
Multitransition
MLT-3

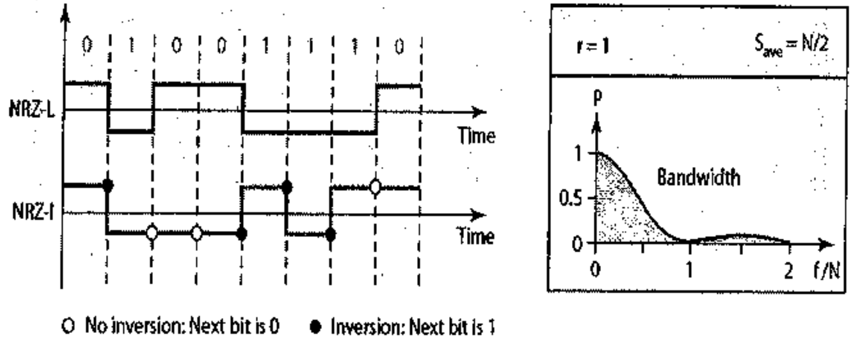
Unipolar NRZ scheme



$$\frac{1}{2}V^2 + \frac{1}{2}(0)^2 = \frac{1}{2}V^2$$

Normalized power

Polar NRZ-L and NRZ-I schemes



In NRZ-L the level of the voltage determines the value of the bit. In NRZ-I the inversion or the lack of inversion determines the value of the bit. NRZ-L and NRZ-I both have an average signal rate of N/2 Bd. NRZ-L and NRZ-I both have a DC component problem.

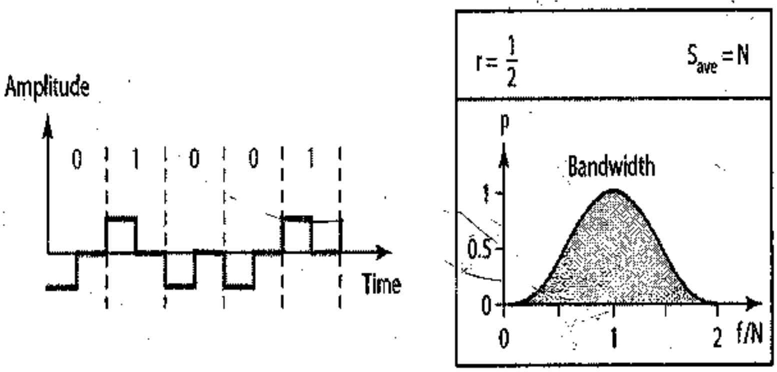
EXAMPLE

A system is using NRZ-I to transfer 10-Mbps data. What are the average signal rate and minimum bandwidth?

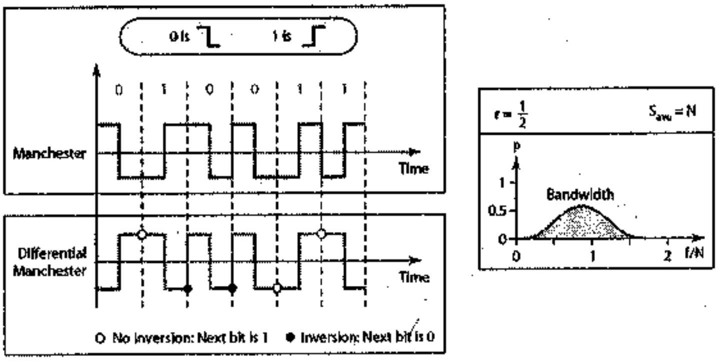
Solution

The average signal rate is S = N/2 = 500 kbaud. The minimum bandwidth for this average baud rate is Bmin = S = 500 kHz

Polar RZ scheme

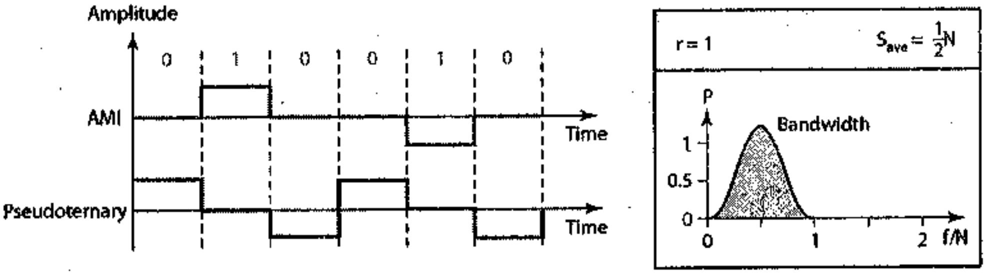


Polar biphase: Manchester and differential Manchester schemes



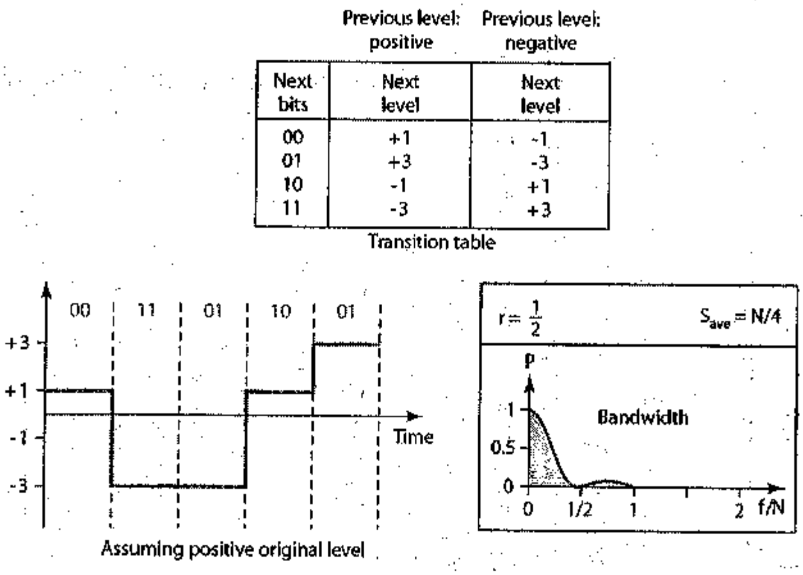
In Manchester and differential Manchester encoding, the transition at the middle of the bit is used for synchronization. The minimum bandwidth of Manchester and differential Manchester is 2 times that of NRZ. In bipolar encoding, we use three levels: positive, zero, and negative.

Bipolar schemes: AMI and pseudoternary



In mBnL scnemes, a pattern of m data elements is encoded as a pattern of n signal elements in which 2m = Ln

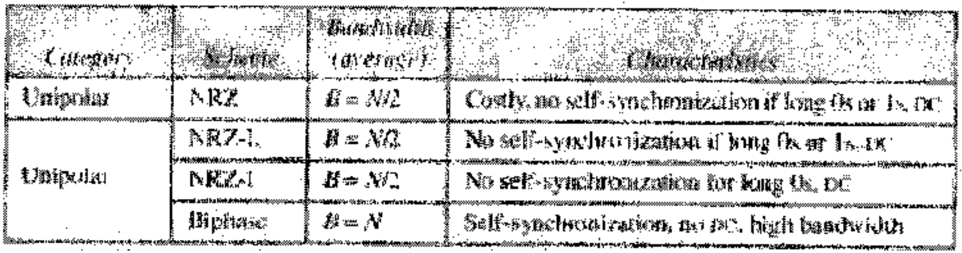
Multilevel: 2B1Q scheme



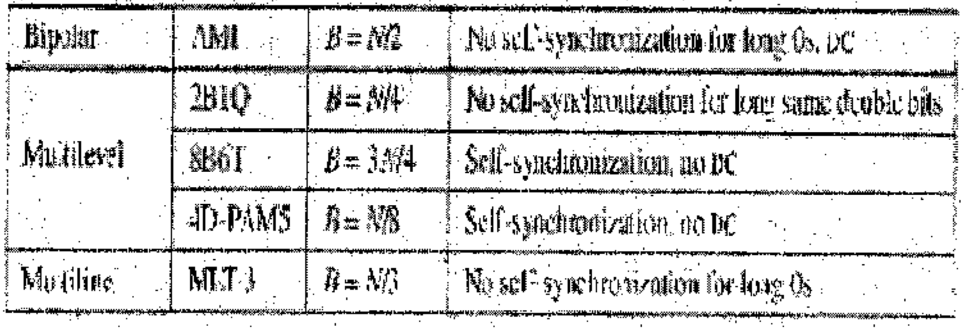
	Previous level: positive	Previous level: negative
Next bits	Next level	Next level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transition table

Summary of line coding



Category	Scheme	Bandwidth (average)	Characteristics
Unipolar	NRZ	$B = N/2$	Costly, no self-synchronization if long 0s or 1s, DC
Unipolar	NRZ-L	$B = N/2$	No self-synchronization if long 0s or 1s, DC
	NRZ-I	$B = N/2$	No self-synchronization for long 0s, DC
	Biphase	$B = N$	Self-synchronization, no DC, high bandwidth



Bipolar	AMI	$B = N/2$	No self-synchronization for long 0s, DC
Multilevel	2B1Q	$B = N/4$	No self-synchronization for long same double bits
	8B6T	$B = 3N/4$	Self-synchronization, no DC
	4D-PAM5	$B = N/8$	Self-synchronization, no DC
Multiline	MLT-3	$B = N/3$	No self-synchronization for long 0s

2.3 MODULATION

The analog signal is sampled at regular intervals and is represented by a new sequence of narrow pulses whose amplitudes are proportional to the values of the original ones (A process known as pulse amplitude modulation, PAM.)

The amplitudes of the new pulses are then quantized into the nearest integers which are represented by a series of corresponding binary digits.

The typical PCM sampling speed is 8000 times per second on voice-grade lines.

By quantizing the PAM pulse, the original signal is only approximated and may not be recovered exactly. This effect is known as quantizing error, or quantizing noise.

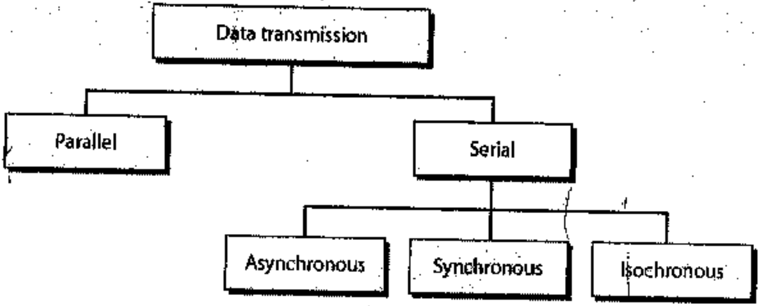
Amplitude modulation (AM) is a technique used in electronic communication, most commonly for transmitting information via a radio carrier wave. AM works by varying the strength of the transmitted signal in relation to the information being sent. For example, changes in the signal strength can be used to reflect the sounds to be reproduced by a speaker, or to specify the light intensity of television pixels. (Contrast this with frequency modulation, also commonly used for sound transmissions, in which the frequency is varied; and phase modulation, often used in remote controls, in which the phase is varied)

2.4 ASYNCHRONOUS & SYNCHRONOUS TRANSMISSION

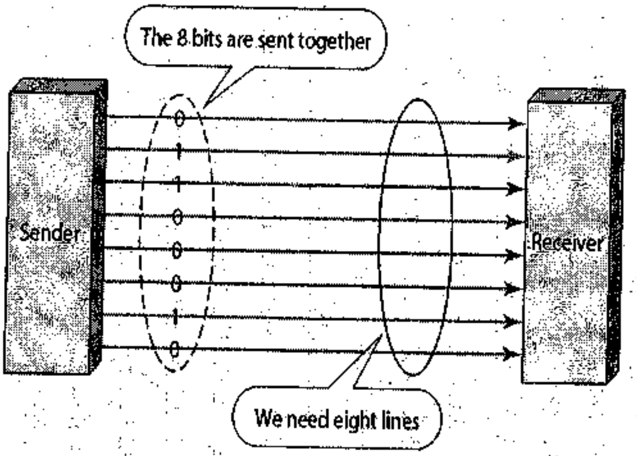
Digital transmission can be either parallel or serial in mode. In parallel transmission, a group of bits is sent simultaneously, with each bit on a separate line. In serial transmission, there is only one line and the bits are sent sequentially. Serial transmission can be either synchronous or asynchronous. In asynchronous serial transmission, each byte (group of 8 bits) is framed with a start bit and a stop bit. There may be a variable-length gap between each byte.

In synchronous serial transmission, bits are sent in a continuous stream without start and stop bits and without gaps between bytes. Regrouping the bits into meaningful bytes is the responsibility of the receiver.

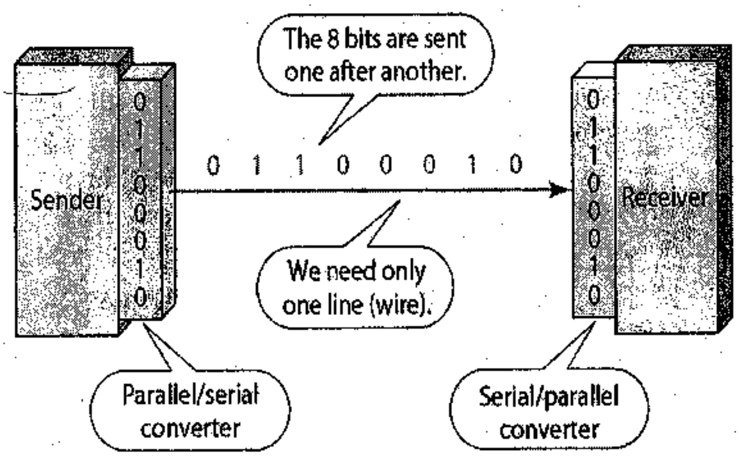
Data transmission and modes



Parallel transmission



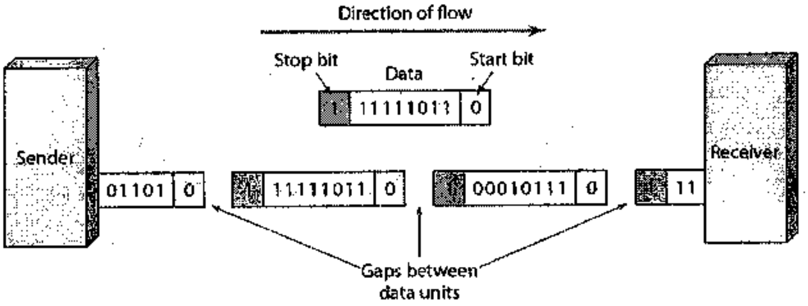
Serial transmission


The 8 bits are sent one after another.
Sender
0 1 1 0 0 0 1 0
0 1 1 0 0 0 1 0
Receiver
We need only one line (wire).
Parallel/serial converter
Serial/parallel converter

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

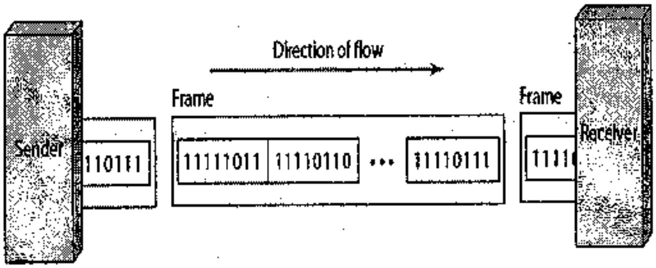
Asynchronous here means "asynchronous at the byte level," but the bits are still synchronized; their durations are the same.

Asynchronous transmission



In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.

Synchronous transmission



2.5 ERROR DETECTION TECHIQUES

Errors can be categorized as a single-bit error or a burst error. A single-bit error has one bit error per data unit. A burst error has two or more bit errors per data unit.

Redundancy is the concept of sending extra bits for use in error detection.

Additional bits added by transmitter for error detection code

Parity . Value of parity bit is such that character has even (even parity) or odd (odd parity) number of ones . Even number of bit errors goes undetected

Three common redundancy methods are parity check, cyclic redundancy check (CRC), and checksum. An extra bit (parity bit) is added to the data unit in the parity check.

The parity check can detect only an odd number of errors; it cannot detect an even number of errors. In the two-dimensional parity check, a redundant data unit follows n data units.

Cyclic Redundancy Check

CRC, a powerful redundancy checking technique, appends a sequence of redundant bits derived from binary division to the data unit.

The divisor in the CRC generator is often represented as an algebraic poly-nomial.

Errors are corrected through retransmission and by forward error correction.

For a block of k bits transmitter generates n bit sequence. Transmit k+n bits which is exactly divisible by some number. Receive divides frame by that number

If no remainder, assume no error

The Hamming code is an error correction method using redundant bits. The number of bits is a function of the length of the data bits. In the Hamming code, for a data unit of m bits, use the formula 2 r >= m +r +1 to determine r, the number of redundant bits needed.

By rearranging the order of bit transmission of the data units, the Hamming code can correct burst errors.

2.6 SUMMARY

- Data encoding is useful for error free and efficient data transmission.
- Modulation techniques are useful in case of digital transmission.
- Errors in transmission are unavoidable phenomenon. Thus, we require error correction techniques as integral part of data transmission process.

2.7 UNIT END QUESTIONS

1. Differentiate between Synchronus and asynchrous transmission.
2. What is modulation.?
3. Explain NRZ and bipolar.

UNIT - 3

MULTIPLEXING & COMMUNICATION HARDWARE

Structure of the unit

3.0 OBJECTIVES

After going through this unit, you will be in a position to:

- Define Multiplexing
- Explain Frequency Division Multiplexing(FDM)
- Describe Synchronous Time Division Multiplexing(STDM)
- Explain Statistical Time Division Multiplexing
- Define the terms : Wave Length, Modems, Multiplexers, De-multiplexers, Concentrators

3.1 INTRODUCTION

The term 'data communication' refers to the exchange of information between two or many computers/ other communicating devices using a transmission system, which may be a single transmission line or a complex computer network. The applications using data communication are financial transactions(e-commerce), travel reservations etc.

Data communication deals with the transmission of signals in a reliable and efficient manner. The information used in data communication may belong to one of the following:

- Analog data (voice, video)
- Digital data(text)

Computer network is a collection of autonomous computers or communicating devices connected together using a technology in such a way that the information can be shared or distributed effectively and efficiently. Thus, we can say, computer network and communication protocols are essential elements of data communication.

3.2 DEFINITION & NEED OF MULTIPLEXING :

We know that telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk. These multiplexing schemes will be discussed in this section. Multiplexing is the method of dividing a physical channel into many logical channels, so that simultaneously many independent signals may be transmitted in a line. The electronic device that performs this task is called *a multiplexer*.

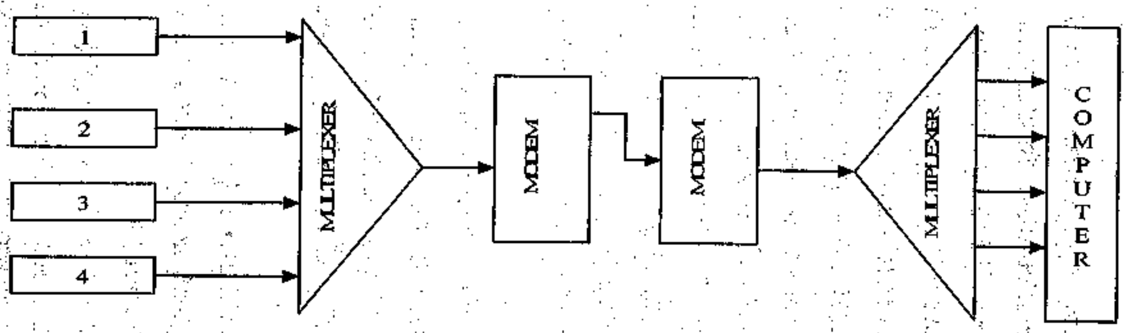
The multiplexer brings together several low speed communications lines, transforms them into one high speed together several low speed communication lines, transforms them into one high speed channel and reverses the operation at the other end.

In many applications, several terminals are connected to a computer. If each terminal is operating at 1440 bits per second over a communication line that can operate at 56,000 bits per second, then there is a very inefficient operation.

A channel is an expensive resource. Thus, multiplexing helps in its optimal utilization by simultaneously transmitting multiple signals over it.

A multiplexer puts several data communication lines or signals, helps into one data communication line or signal at the sending location.

For example: In the given figure there are 4 terminals connected to a multiplexer. The multiplexer takes the signals from the 4 terminals connected to a multiplexer. The 1 communication channel. At the receiving end, a demultiplexer takes the large signal and reconverts it into the original 4 signals. Without multiplexers, one needs 4 separate communication channels.



A Multiplexed System

There are three basic method of multiplexing channels, they are:

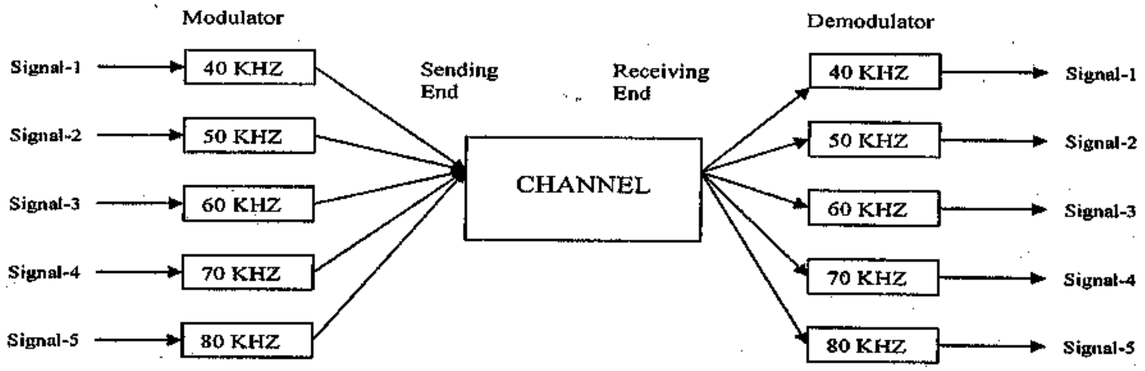
- *Time Division Multiplexing (TDM)*
- *Frequency Division Multiplexing (FDM)*
- *Space Division Multiplexing (SDM)*

3.3 FREQUENCY DIVISION MULTIPLEXING (FDM):

The bandwidth or range of a medium is always more than that of any given signal. This fact is used in frequency division multiplexing.

In FDM, the available bandwidth of a physical medium is divided into several smaller, disjoint logical bandwidths. Each of the bandwidth is used as a separate communications line.

The given figure shows process of FDM. This is represented here:



Frequency Division Multiplexing

The best example of FDM is that of radio transmission. Each radio station is assigned a frequency range within a bandwidth of radio frequencies. Several radio stations may be transmitting electromagnetic signals simultaneously over the physical channel. A radio receiver's antenna receives signals transmitted by all the stations. The tuning dial in the radio is used isolate the speed signal of the station tuned.

In FDM, the signals to be transmitted are analog signal. Thus, digital signals are converted to analog form FDM.

3.3.1 Bandwidth

Definition: The bandwidth of a signal is the width of the frequency spectrum. Thus, bandwidth refers to the range of component frequencies. Bandwidth is obtained by subtracting lowest frequency from highest frequency.

Importance of bandwith in Data Communication:

The bandwidth plays a key role in data communication.When a transmission medium has a limited bandwidth it can transfer only some range of frequencies. The higher the band width, higher is the data transmitted at the higher data rate. More the bit, rate more is significant (utilized) bandwidth.

Thus, we need a medium with wider bandwidth to transfer a signal. The two factors bit rate and bandwidth define channel capacity of the medium.

3.3.2 Wavelength

Definition: The distance between two consecutive maxima (or minima) of an electromagnetic wave is called Wavelength. It is denoted by the Greek alphabet λ (lambda). It is measured in meters.

Importance in Data Communication

Wavelength is one of the fundamental quantities in data communication. All electromagnetic waves travel at the speed of light 'C' which is equal to 3 x10^8 m/sec. This speed of light is the ultimate speed. No signal can move faster than it. The relation that governs f, λ and C (in vacuum) of a signal is given by :

$$\lambda f = C$$

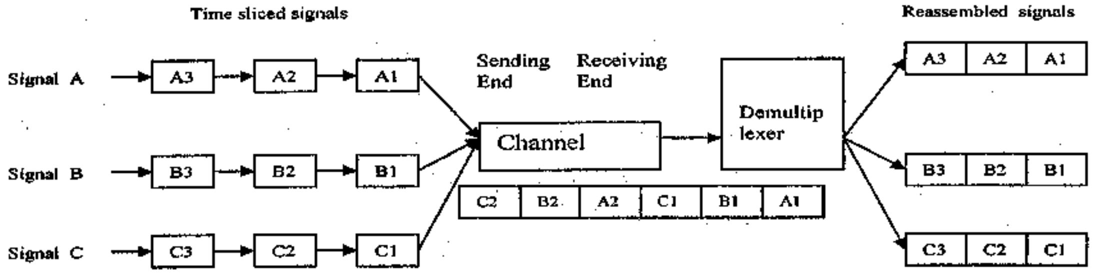
Where C is constant. Hence for λ and f are in an inverse relation. For higher frequencies λ is less , and vice-versa. Thus, 1 MHz waves have about 300 meters wavelength and 1 cm waves have a frequency of 30 GHz.

Thus, we can say wavelength plays an important role in design of various data transmission systems and devices.

3.4 TIME DIVISION MULTIPLEXING

The bit rate of a transmission medium is always more than the rate of the digital signal. This fact is utilized for time division multiplexing. In TDM, the total time available in the channel is divided between several users and each user of the channel is allotted a time interval during which he/she may transmit a message.

The channel capacity is fully utilised in TDM by interleaving a number of data streams belongs to different users into one data stream. Streams of data sent through the physical channel are de-multiplexed at the receiving end. Individual messages is reassembled at the receiving end. The process of TDM is represented in the figure below for multiplexing three different signals.



Time Division Multiplexing

TDM combines separate signals into a single high-speed transmission in which transmission time is broken into segments, each of which carries one element of one signal. The messages are broken into smaller packets and are interleaved and assigned time slots.

A header containing the address and packet number information precedes each packet. The multiplexed packets are transmitted and received by the receiving station. Appropriate packets (determined by destination address in the header) are extracted by each station as they are received and reassembled (by packet number, included in the header) into their original message. This is how full operation of TDM takes place.

TDM is used to multiplex digital or analog signals. For communication of digital data, it is more convenient to transmit data directly in digital form and thus TDM is more appropriate. Moreover, communication between computers occurs in short, fast bursts. Each burst will need the full channel bandwidth. That is available to a signal in TDM.

3.5 SYNCHRONOUS TIME DIVISION MULTIPLEXING

Synchronous Time Division Multiplexing can be discussed as :-

Synchronous Time Division Multiplexing (STDM) assigns time slots of equal length to all packets regardless whether or not anything is to be sent by each station with an assigned time slot.

For example: if message A is not included, then its allotted time would still be allocated. However, time slots for message A would not contain information.

STDM systems are comparatively easy to implement once the software allocates the time slots.

3.6 STATISTICAL TIME DIVISION MULTIPLEXING

Statistical Time Division Multiplexing is defined as –

Statistical Time Division Multiplexing (STATDM) does not make a fixed assignment of time slots so that any port which is idle does not receive a (full) slot. In order to identify which slot corresponds to which data stream, it is necessary to append address and contol symbols to each slot that is used. This *'overhead'* is usually small and is more than compensated for by the increased efficiency derived from not having to take up channel space with idle bits.

These systems are more complex but allow re-assigning of time slots which are not in use. STATDM networks assign time slots only when they are to be used and delete them when they are idle. The total time used for a STATDM frame varies with the amount of traffic currently being handled.

STATDM systems are most suitable for these high-density, high-traffic applications. The continuous messages are assigned time slots and interleaved as each channel on the second side becomes active and requires

These systems are more complex but allow re-assigning of time slots which are not in use. STATDM networks assign time slots only when they are to be used and delete them when they are idle. The total time used for a STATDM frame varies with the amount of traffic currently being handled.

STATDM systems are most suitable for these high-density, high-traffic applications. The continuous messages are assigned time slots and interleaved as each channel on the second side becomes active and requires communications with another channel. If a channel does not have any traffic, its time slots are deleted and reassigned to an active channel. In this way the interconnecting media achieves a higher state of utilization than with STDM systems.

TDM and STADM require a modem in order to interface with the voice line, but this may be built in. All modern STATDMs have at least one microprocessor with programmed and programmable functions of great diversity and are called "Smart" or "Intelligent MUXs."

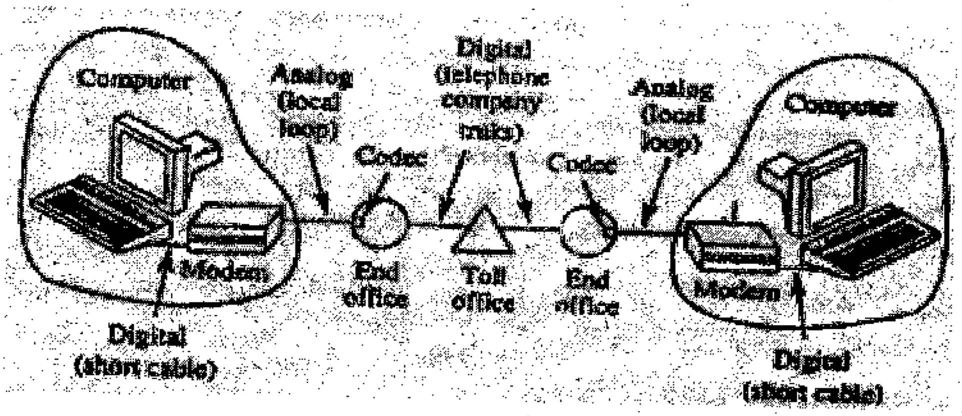
3.7 MODEMS

Modems are the devices used to convert digital signals (to be communicated over analog channels such on telephone lines) to sine wave at the sending end and back to digital signals at the receiving end. They are used to connect two distant located PCs, So that PCs can communicate with each other.

Modems convert communication signals from a form the computer can understand to a form the phone system can convey and *vice-versa.*

Modulation is the process of converting a digital signal from a computer into an analog signal the telephone system will accept. At the other end of the connection, whether it be across town or across the world, another modem interprets those analog signals and converts them back into digital form so the receiving computer can understand them. A modem can installed internally, in the computer, in which case it is called an internal modem, or it can be an external device that is connected to the computer with a serial cable.

The following figure shows the example of computer communicating *via* modems.



3.7.1 Functions & Uses of Modem:

The most familiar type of DCE (Data Conversion Equipment) is a modem. For surfing the Internet, logging on to an office computer from home, or sending news from a word processor over a phone line modem issued. Modem can be external or internal. It converts the digital signal generated by the computer into an analog signal to be carried by a phone line. It is also the device that converts the analog signals received over a phone line into digital signals usable by the computer.

The term *modem* is composite word that refers to the functions of a signal *modulator* and a signal *demodulator*. The relationship of the two functions is shown in the figure given below:

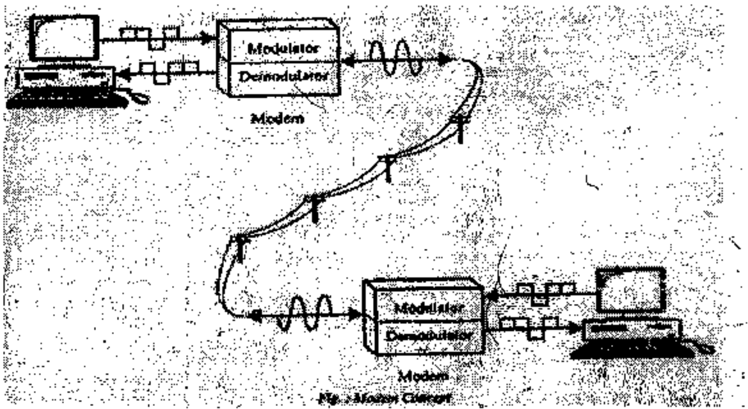


Fig. : Modem Concept

Functions of Modem

A modulator converts a digital signal into an analog signal. A demodulator converts an analog signal into a digital signal. While a demodulator resembles an analog-to digital encoder, it is not in fact an encoder of any kind. It does not sample a signal to create a digital facsimile; it merely reverses the process of modulation.

The above figure shows modems across a communication link. The two PCs at the ends are the DTEs; the modems are the DCE, The DTE creates a digital signal and relays in to the modem *via* an interface (like the EIA-232).

The modulated signal is received by the demodulation function of the second modem. The demodulator takes the ASK, FSK, PSK, or QAM signal and decodes it into a format its computer can accept. It then relays the resulting digital signal to the receiving computer *via* an interface. Each DCE is compatible with both its own DTE and with other DCEs. A modem uses the same type of encoding (such as NRZ-L), the same voltage levels to mean the same things, and the same timing conventions as its DTE. A modem is also able to talk to modems.

Modems transmit data at different speeds, measured by the number of *bits* of data they send per second (bps). Examples of modem speeds are: 256 Kbps, 512 Kbps, 2 Mbps, 8 Mbps, etc.

3.7.1 Baud Rates and bps :

Baud rate refers to the oscillations of a sound wave on which a single bit of data is carried. Bits per second (bps) is the amount of data transferred in a second. By employing special techniques that manipulate. A modem can encode data and achieve higher rate of data transfer. A modem that is modulating its sound waves at 14400 baud may actually be transmitting 38,400 bits per second.

When a computer wishes to send digital data over a dial - up line, the data must first be converted to analog form by a modem for transmission over the local loop, then converted to digital form for transmission over the long - haul trunks, then back to analog over the local loop at the receiving end, and finally back to digital form by another modem for storage in the destination computer.

3.8 MULTIPLEXERS/DE-MULTIPLEXERS

To enhance the transmission capacity of a channel and economize over all transmission cost, several signals are combined or interleaved to form a composite signal for remote transmission. The unit or device which combines several messages or channels for remote transmission is termed Multiplexer.

At destination individual message are recovered by de-multiplexing. The unit or device which performs demultiplexing is known as Demultiplexer.

The multiplexer brings together several low speed communications lines, transforms them into one high speed together several low speed communication lines, transforms them into one high speed channel and reverses the operation at the other end.

3.9 CONCENTRATOR

A concentrator refers to a device that can collect data traffic from M sources and transmit them through N facilities or trunks where M>N. Traditionally, concentrators programmed and have store and forward as well as switching capabilities. However, intelligent programmable STDMs, are now far more versatile than very expensive and bulky concentrators.

Concentrator is a multiple that combines a large number of individual data lines into a signal line. The word concentrator is used to denote a device which not only does multiplexing, but also switching and routing to several outputs ports as well as handling data compression, code conversion, errors control, protocol functions etc. Concentrator and communication processors are used interchangeably.

Also, in other words we can say that an electronic device that interfaces in a store and forward mode, with multiple low speed communication lines at a message level and then retransmits those messages to a processing site *via* one or more high speed communication line. It is based on the fact that all the users are not active simultaneously.

3.9.1 Role of Concentrator in Data Transmission

The role of concentrator and the front end processor is to relieve the central processor of the routine communication tasks of interfacing with the transmission network. The concentrator functions as a sophisticated switching node in a large data network and in addition to the multiplexing it provides, switching, network management and complete link protocol handling.

Concentrators are called upon to handle level 3 protocols such as X.25 as well as level 2 (data link control) protocols. Thus concentrator is a full-fledged network node which does switching, routing, flow control, load leveling and traffic monitoring.

Q.1. Why is multiplexing needed in data communication systems?

Q.2. What factors decode use of multiplexing?

Q.3. Explain in brief the synchronous time division multiplexing. How does it differ from the statistical time division multiplexing?

Q.4. Why modems are needed for telephone communication?

Q.5. Why the complete bandwidth of telephone lines not used for data communication?

Q.6. What is a concentrator? What role it plays in data transmission? What protocols it generally handles?

Q.7. What is the frame rate? What is the bit rate on the path?

Q.8. What is a modem? How does it work?

Q.9. What do you understand by a communication channel?

Q.10. A cable TV system has a number of commercial channels, all of them showing programs and advertisements alternatively. What type of multiplexing is it? Justify your answer.

3.10 SUMMARY

- Multiplexing is the method of dividing a physical channel into many logical channels, so that simultaneously many independent signals can be transmitted in a line.
- Multiplexing can further be classified into frequency division and time division multiplexing. Generally, in frequency division multiplexing signals are multiplexed by modulation process while in time division multiplexing by interleaving technique.
- To enhance the transmission capacity of a channel and economize over all transmission cost, several signals are combined or interleaved to form a composite signal for remote transmission. The unit or device which combines several messages or channels for remote transmission is termed Multiplexer.
- At destination individual message are recovered by de-multiplexing. The unit or device which performs demultiplexing is known as demultiplexer.

- Synchronous Time Division Multiplexing (STDM) assigns time slots of equal length to all packets regardless whether or not anything is to be sent by each station with an assigned time slot.
- Modems are the devices used to convert digital signals (to be communicated over analog channels such a telephone lines) to sine wave at the sending end and back to digital signals at the using telephone lines.
- Modems transmit data at different speeds, measured by the number of *bits* of data they send per second (bps). Examples of modem speeds are: 256 Kbps, 512 Kbps, 2 Mbps, 8 Mbps, etc.
- Baud rate refers to the oscillations of a sound wave on which a single bit of data is carried. Bits per second (bps) are the amount of data transferred in a second.
- Concentrator is a multiple that combines a large number of individual data into a signal line. The word concentrator is used to denote a device which not only does multiplexing, but which had but also switching and routing to several output ports as well as handling data compression.

3.11 GLOSSARY

- **Data Communication :** It refers to the exchange of information between two or many computers/other communicating devices using a transmission system, which may be a single transmission line or a complex computer network.
- **Multiplexing :** This is a method of dividing a physical channel into many logical channels, so that simultaneously many independent signals may be transmitted in a line.
- **FDM :** In frequency division multiplexing the available bandwidth of a physical medium is divided into several smaller, disjoint logical bandwidths. Each of the bandwidth is used as a separate communications line.
- **TDM :** Time division multiplexing combines separate signals into a single high-speed transmission in which transmission time is broken into segments, each of which carries one element of one signal.
- **STDM :** Synchronous time division multiplexing assigns time slots of equal length to all packets regardless whether or not anything is to be sent by each station with an assigned time slot.
- **Communication :** Transfer of information from one person or device to another.
- **Communication Channel :** Medium that carries the message/information sound etc. sent by sender to receiver.
- **Digital Signal :** Group of discrete electronic units transmitted in rapid succession.
- **Analog Signal :** Signal consisting of continuous electrical waves.
- **Modem :** A modem is a computer peripheral that connects a work station to other work stations *via* telephones and facilitates communications. It is short form for Modulation/Demodulation.
- **Concentrator :** It is a multiple that combines a large number of individual data into a signal line.

3.12 FURTHER READINGS

- Computer Networks; Andrew S. Tanenbaum
- An Engineering Approach to Computer Networking: S. Keshav; Pearson Education; 2002
- Data Communication & Networking: Behrouz A. Fourouzan; Tata McGrawhill
- Data Communication, Computer Networks & Open systems: F. Halsall; Addison Wesley; 1996

- Data Networks; Bertsekas and/Gallagar; PHI;1992
- Computer Networks-Protocols, Standards & Interfaces; Uyless Balck; Prentice Hall India, New Delhi.

3.13 UNIT END QUESTIONS :

Q1. What do you mean by Frequency Division Multiplexing?

Q2. Explain in brief the Synchronous Time Division Multiplexing.

Q3. Define the Time Division Multiplexing with suitable examples.

Q4. Differentiate between Internal Modem & External Modem.

Q5. Explain the following terms:

(a) Multiplexer

(b) Bandwidth

(c) Wavelength

(d) Modulation

(e) Concentrator

UNIT 4

INTRODUCTION TO COMPUTER NETWORKS

Structure of the Unit

4.0 OBJECTIVES

After this unit, you should be able to:

- Define and classify networks
- Understand goals and applications of networks
- Distinguish between different types of networks

4.1 INTRODUCTION

Earlier computers used for information gathering, processing or distributing as standalone system. Later on more than one computer were connected to each other to form computer network. In this unit we will learn about networks, goals and applications of network, different types of networks and classification of networks.

4.2 WHAT IS NETWORK?

A Network is an interconnected collection of autonomous computers. Two or more computers connected together by a communication media so that they can exchange information. In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

Different topologies to connect networks include the bus, star, Token Ring, and mesh topologies. Networks can also be characterized in terms of spatial distance as local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).

4.3 NETWORK GOALS

Goals of the networks are :

- Resource sharing - programs, data, equipment.
- High reliability - replicated files, multiple CPU.
- Saving money - small computers have much better price/performance ratio than large ones. The systems of personal computers, one per person, are built with data kept on one or more shared file server machines. Users are called clients, the whole arrangement is called the client-server model.
- Scalability - the ability to increase system performance gradually as the workload grows just by adding more processors.
- Communication medium - enables e.g. to write a report together.

Services delivered by networks to people at home:

- Access to remote information (interaction between a person and a remote database) - financial institutions, home shopping, newspapers, digital library, potential replacement of printed books by notebook computers, access to information systems (WWW).
- Person-to-person communication (21st century answer to the 19th century's telephone) - email, videoconference, newsgroups.
- Interactive entertainment - video on demand, interactive films.

Social issues of networking:

- newsgroups set up on topics that people actually care about (politics, religion, sex) - photographs, video clips
- employee rights versus employer rights - some employers have claimed the right to read and possibly censor employee messages
- school and students
- anonymous messages

4.4 APPLICATIONS OF NETWORKS

Data communication networks play important role in business, industry and entertainment. Some of the network applications in different fields are the following:-

- Teleconferencing applications include simple text conferencing, voice conferencing and video conferencing.
- Electronic mail(E-mail) is most widely used network application.
- Directory services allow lists of files to be stored in a central location to speed worldwide search operations.
- In marketing computer networks are used to collect, exchange, and analyze data relating to customer needs and product development cycles. In sales, networks are used for teleshopping, which uses computers or telephones connected to an order-processing network, and on-line reservation services for hotels, airlines, and so on.
- Applications that uses networks are credit history searches, foreign exchange and investment services, and electronic funds transfer(EFT).
- Bulletin board and data bank are examples of Network information services. A World Wide Web is a good example of information service.
- Electronic data interchange allows business information (including documents such as purchase orders and invoices) to be transferred without using paper.
- Today's cellular networks make it possible to maintain wireless phone connections even while traveling over large distance.

- Future services provided by cable television networks may include video on request, as well as the same information, financial, and communication services currently provided by the telephone companies and computer networks.

4.5 TYPES OF NETWORKS

There are two types of networks according to transmission technology:

- Point-to-point networks,
- Broadcast networks.

Point-to-point networks consist of many connections between individual pairs of machines. In these types of networks:

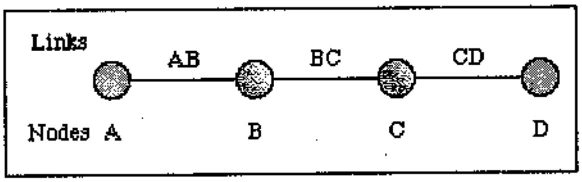
- A packet on its way from the source to the destination may go through intermediate machines.
- In general, multiple routes are possible - routing algorithms are necessary.

In general smaller, geographically localized networks tends to use broadcasting, larger networks usually are point-to-point.

4.5.1 Point-to-Point or Switched Network

Switched network is a type of network that provide switched communication system and in which users are connected with each other through the circuits, packets switching and the control devices. Example is public switch telephone network. From source to destination data transmitted through a network of intermediate switching nodes. The switching network provides a switching facility that will move the data from node to node until they reach their destination. The end devices that wish to communicate may be referred to as station. Switching devices are known as nodes. Nodes are connected to one another by transmission lines. Each station attaches to a node and the collection of nodes is referred to as a communication network.

The connection between A and D is provided using (shared) links between two other pieces of equipment, B and C.



A connection between two systems A & D formed from 3 links

Point-to-Point networks have different topologies through which routers are interconnected and have different technologies to construct communication.

4.5.1.1 Network Topology

Topology defines the physical or logical arrangement of links in a network. The physical topology of a network refers to the actual layout of the computer cables and other network devices. The logical topology of a network, on the other hand, refers to the way in which the network appears to the devices that uses it. The topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to each other. There are basic topologies possible: mesh, start, tree, bus and ring.

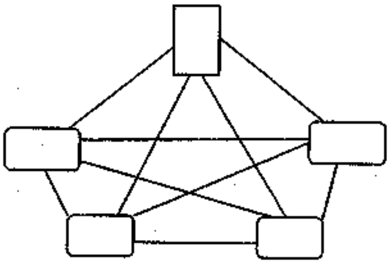
In topology two relationships are possible:-

- Peer to peer, where the devices share the link equally, example ring and mesh.
- Primary secondary, where one device controls traffic and the other must transmit through it, example star and tree.

A bus topology is equally equivalent for either.

Mesh

The *mesh* topology incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. The purpose of the mesh design is to provide a high level of redundancy. If one network cable fails, the data always has an alternative path to get to its destination.



Mesh topology.

Advantages:

- The use of dedicated links reduced the network traffic problem.
- The network can be expanded without disruption to current users.
- It is very secure and private.
- Point-to-point links make fault identification and fault isolation easy.

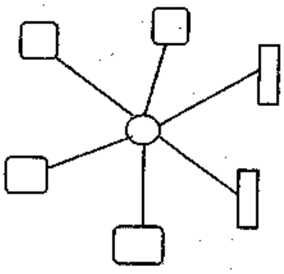
Disadvantage

- Requires more cable than the other LAN topologies.
- Installation and reconfiguration are difficult.

Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, called hub. The devices can communicate with each other with the help of hub only. Each connected device requires a single cable to be connected to the hub, creating a point-to-point connection between the device and the hub.

Using a separate cable to connect to the hub allows the network to be expanded without disruption to the network. A break in any single cable will not cause the entire network to fail. Because all devices connect to a centralized hub, this creates a single point of failure for the network. If the hub fails, any device connected to it will not be able to access the network.



Star topology.

Advantages

- Less expensive than mesh topology.
- Easy to install and configure.
- Star networks are easily expanded without disruption to the network.

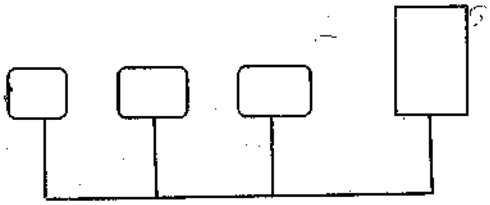
- Cable failure affects only a single user.
- Easy to troubleshoot and isolate problems.

Disadvantages

- Requires more cable than most of the other topologies.
- A central connecting device allows for a single point of failure.
- More difficult than other topologies to implement.

Bus

A bus topology is multipoint. A *bus network* uses a trunk or backbone to which all of the computers on the network connect. Systems connect to this backbone using T connectors or taps. To avoid signal reflection, a physical bus topology requires that each end of the physical bus be terminated.



Physical bus topology

Advantage

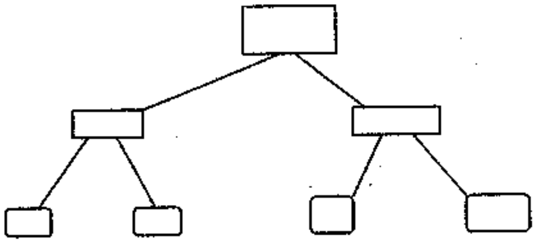
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

Tree

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices. Some of devices connected to central hub (active hub) and majority of devices connected to secondary hub(passive hub) that is connected to the central hub.



Tree Network Topology

Advantages

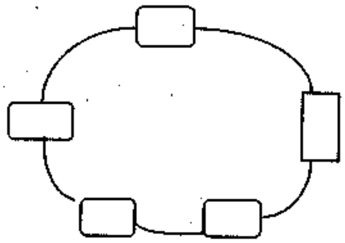
- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Ring

A **ring network** is a network topology in which each node connects to exactly two other nodes, forming a circular pathway for signals - a ring. Data travels from node to node. The *ring* topology is actually a logical ring, meaning that the data travels in circular fashion from one computer to another on the network. It is not a physical ring topology.



Logical design of the ring network.

Advantages

- Cable faults are easily located, making troubleshooting easier.
- Ring networks are moderately easy to install.

Disadvantage

- Expansion to the network can cause network disruption.
- A single break in the cable can disrupt the entire network.

Self Assessments

True/ False

1. E-mail is most widely used network application.(True)
2. In bus topology nodes are connected in ring manner.
3. Resource sharing is not an application of network.
4. E-mail is most widely used network application.

Fill in the Blanks

1. .... *networks* consist of many connections between individual pairs of machines.
2. A bus topology is ....
3. EFT stands for.................
4. A Network is an ....collection of autonomous computers.

4.5.1.2 Network Technology –

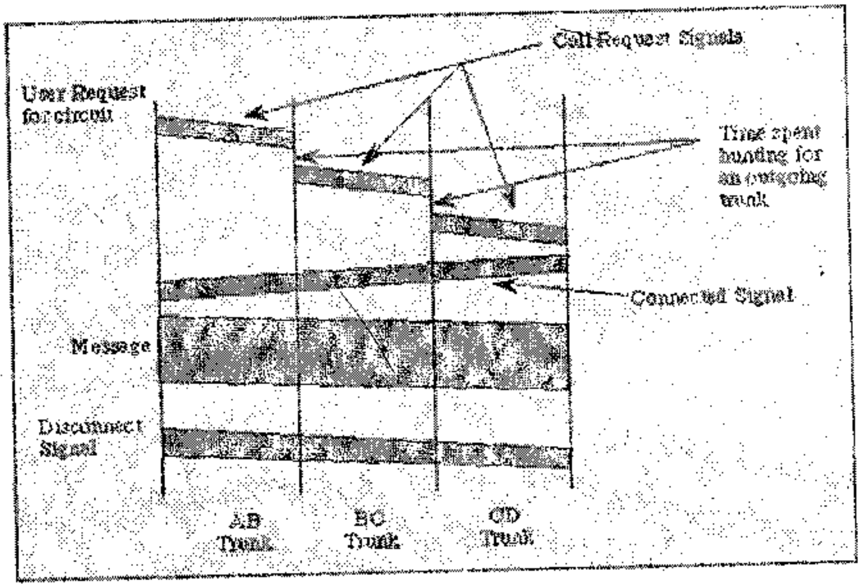
Two different technologies to construct communication are:

- Circuit Switching network
- Packet Switching network

Circuit Switching network

In circuit switching network there is a dedicated communication path between two stations. This path is a connected sequence of links between network nodes. The most ubiquitous circuit-switching network is the telephone system. Consider communication between two points A and D in a network.

Network use is initiated by a connection phase, during which a circuit is set up between source and destination, and terminated by a disconnect phase. These phases, with associated timings, are illustrated in the figure below.



A circuit switched connection between A and D

Main phases in circuit switching network are:

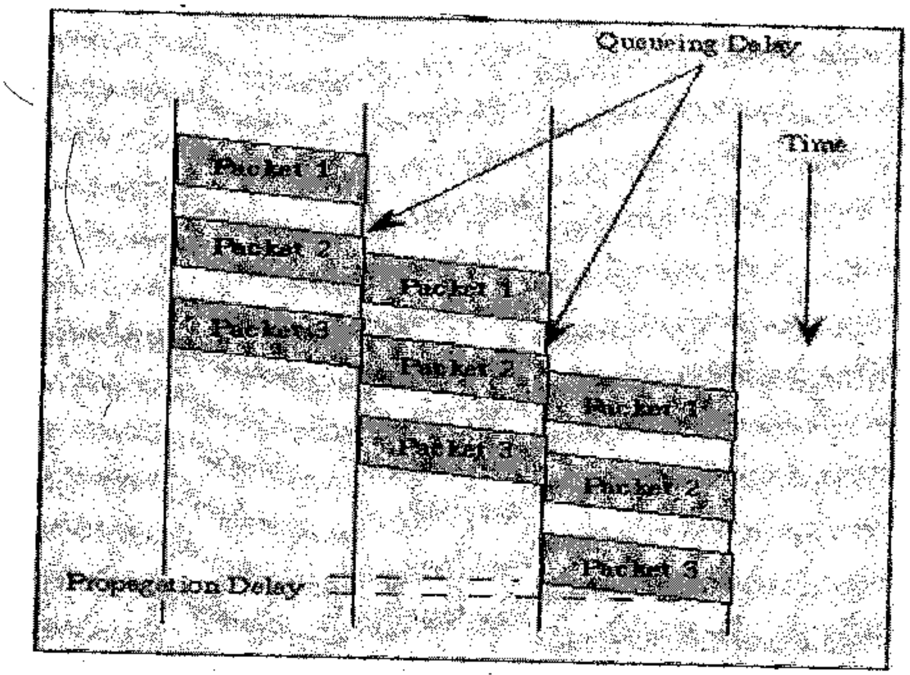
1. Circuit establishment – Before any signal transmission, an end-to-end (station to station) must be established.
2. Data transfer – Information can now be transmitted from one node through the network to other node. The data may be analog or digital depending on the nature of network.
3. Circuit disconnect – After some period of time data transfer, the connection is terminated usually by the action of one of the station.

Packet Switching Network

A key characteristic of circuit switching networks is that resources within the network are dedicated to a particular call. Because of this, two shortcoming of circuit switching networks are:

- In a typical user/host data connection (e.g., personal computer user logged on to a database server), much of the time line is idle. Thus, with data connections, a circuit switching approach is inefficient.
- In a circuit switching network, the connection provides for retransmission at a constant data rate. This limits the utility of the network in interconnecting a variety of host computers and workstations.

With the help of packet switching we can overcome these problems. Packet Switching is a process in which data is divided into the packets before it routes to its destination and all packets are recompiled to its original shape when they reach at the destination. Most of the WAN technologies such as TCP/IP, Frame relay and the X.25 are based on the packet-switching data communication technology. Each packet contains the header in which source and destination information is contained and it transmitted through the network individually. There are two types of packet switched network one is datagram and other is virtual circuit.



Packet-Switched communication between systems A and D

(The message in this case has been broken into three parts labeled 1-3)

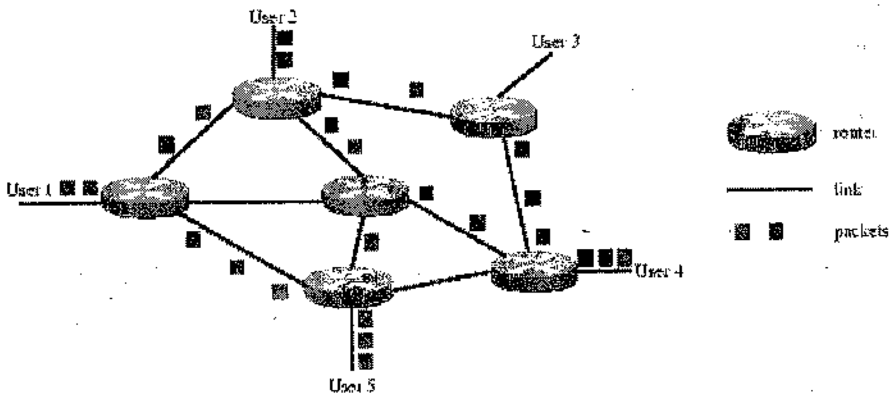
There are two important benefits from packet switching.

1. The first and most important benefit is that since packets are short, the communication links between the nodes are only allocated to transferring a single message for a short period of time while transmitting each packet. Longer messages require a series of packets to be sent, but do not require the link to be dedicated between the transmission of each packet. The implication is that packets belonging to other messages may be sent between the packets of the message being sent from A to D. This provides a much fairer sharing of the resources of each of the links.
2. Another benefit of packet switching is known as "pipelining". Pipelining is visible in the figure above. At the time packet 1 is sent from B to C, packet 2 is sent from A to B; packet 1 is sent from C to D while packet 2 is sent from B to C, and packet 3 is sent from A to B, and so forth. This simultaneous use of communications links represents a gain in efficiency, the total delay for transmission across a packet network may be considerably less than for message switching, despite the inclusion of a header in each packet rather than in each message.

Datagram Packet Networks

Datagram transmission uses a different scheme to determine the route through the network of links. Using datagram transmission, each packet is treated as a separate entity and contains a header with the full information about the intended recipient. The intermediate nodes examine the header of a packet and select an appropriate link to an intermediate node which is nearer the destination. In this system, the packets do not follow a pre-established route, and the intermediate nodes (usually known as "routers") do not require prior knowledge of the routes that will be used.

In a datagram network delivery is not guaranteed (although they are usually reliably sent). The most common datagram network is the Internet which uses the IP network protocol. One merit of the datagram approach is that not all packets need to follow the same path (route) through the network (although frequently packets do follow the same route). This removes the need to set-up and tear-down the path, reducing the processing overhead, and a need for Intermediate Systems to execute an additional protocol. Packets may also be routed around busy parts of the network when alternate paths exist. This is useful when a particular intermediate system becomes busy or overloaded with excessive volumes of packets to send. It can also provide a high degree of fault tolerance, when an individual intermediate system or communication circuit fails. As long as a route exists through the network between two end systems, they are able to communicate. Only if there is no possible way to send the packets, will the packets be discarded and not delivered.

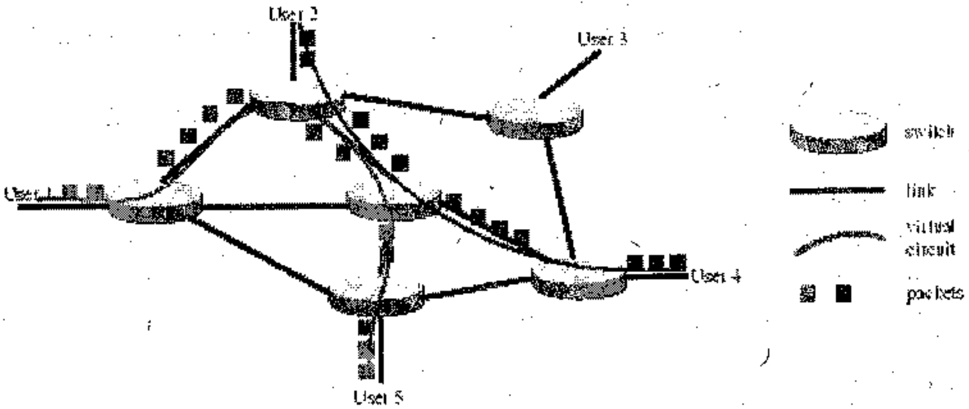


Datagram Packet Switching. Packets from a given flow are independent and a router can forward two packets from the same flow on two different links.

Virtual Circuit Packet Switching

In virtual circuit packet switching, an initial setup phase is used to set up a fixed route between the intermediate nodes for all packets which are exchanged during a session between the end nodes (analogous to the circuit-switched telephone network). At each intermediate node, an entry is made in a table to indicate the route for the connection that has been set up. Packets can then use short headers, since only identification of the virtual circuit rather than complete destination address is needed. The intermediate nodes (B,C) process each packet according to the information which was stored in the node when the connection was established.

Enhancements to provide reliability may also be provided. Delivery of packets in proper sequence and with essentially no errors is guaranteed, and congestion control to minimise queuing is common. Delays are more variable than they are with a dedicated circuit, however, since several virtual circuits may compete for the same resources. An initial connection setup phase and a disconnect phase at the end of data transfer are required (as in the circuit-switched network). The most common form of virtual circuit network were ATM and X.25, which for a while were commonly used for public packet data networks.



Virtual circuit packet switching. All packets from the same flow use the same virtual circuit.

4.5.2 Broadcast Network

Broadcast networks have a single communication channel that is shared by all the machines on the network. Short message (packets) sent by any machine are received by all the others. The sender specifies the address of receiver in the packet. When a machine receives a packet, it checks the address field. If the packet is intended for itself, it processes the packet; if the packet is intended for some other machine, it is just ignored.

Broadcasting is a mode of operation in which a packet is sent to every machine using a special code in the address field.

Multicasting is used to send a packet to a subset of the machines. Example of broadcast networks are:

Packet Radio Networks

Packet radio network is a collection of fixed or mobile nodes that communicate via radios. The network uses electromagnetic radio waves operates at *radio frequency*(RF) and its transmissions are called RF transmissions. Each host on the network attaches to an antenna, which can both send and receive RF.

Advantages

- Fast (re)deployment and set-up of network
- Ability to support mobile nodes

Disadvantage

- complications due to
- Communications medium
- Dynamic nature of the network topology
- Half duplex operation

Satellite Networks

Satellite network is a collection of satellites that are revolving around the earth. Satellite communication use microwave frequency antennas to receive radio signals from transmitting stations on the earth and to relay the signals back down to earth stations. The satellite serves as an electronic relay station. The signals received by satellite may be voice image, data transmission or television video signal.

The satellite contains a *transponder* consisting of a radio receiver and transmitter. A ground station on one side of the ocean sends a signal to the satellite, which amplifies it and transmits the amplified signal at a different angle than it arrived to another ground station on the other side of the ocean.

Advantages:

- Each satellite has a large transmission capacity.
- The cost of transmitting the signal is independent of the distance between the two earth sides.
- Provide opportunity to design a switched network without physical switches.

Disadvantages :

- Poor weather conditions may interfere with signal.
- Because of distance, delay may occur in the reception of the signal at the earth station.
- Only finite amount of frequency exist.

4.6 CLASSIFICATION OF NETWORKS

4.6.1 Local Area Networks

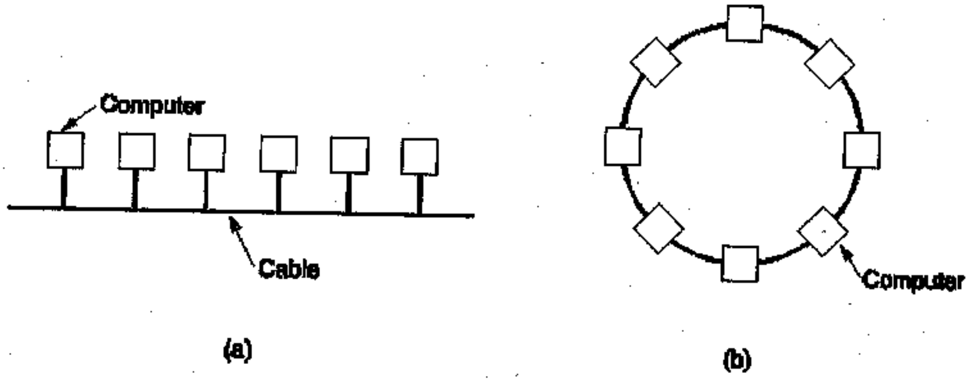
A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building.

Most LANs connect workstations and personal computers. Each *node* (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users (for example, in an FDDI network).

The following characteristics differentiate one LAN from another:

- **topology** : The geometric arrangement of devices on the network The most common LAN topologies are bus, ring and star.
- **protocols** : The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.
- **media** : Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves

Possible topologies for broadcast LANs:



Two broadcast networks. (a) Bus. (b) Ring.

- *bus* - at any instant one machine is the master of the bus allowed to transmit. Arbitration mechanism for resolving the conflicts when more than one machine want to transmit may be centralized or distributed. Example: Ethernet as a bus-based broadcast network with decentralized control operating at 10 or 100 Mbps.
- *ring* - each bit propagates around, typically it circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even be transmitted. Example: IBM token ring operating at 4 and 16 Mbps.

Broadcast networks can be, depending on how the channel is allocated, further divided into:

- Static - a typical would be a time division for the access to the channel and round-robin algorithms. It wastes channel capacity.
- Dynamic - on demand. Channel allocation could be centralized or decentralized.

LAN built using point-to-point lines is really a miniature WAN.

4.6.2 Metropolitan Area Networks

MANs (*Metropolitan Area Networks*) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers) at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network.

A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).

Some technologies used for this purpose are ATM, FDDI, and SMDS. These older technologies are in the process of being displaced by Ethernet-based MANs (e.g. Metro Ethernet) in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red laser links.

There are three important features which discriminate MANs from LANs or WANs:

1. The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.
2. A MAN (like a WAN) is not generally owned by a single organization. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a single network provider who sells the service to the users. This level of service provided to each user must therefore be negotiated with the MAN operator, and some performance guarantees are normally specified.
3. A MAN often acts as a high speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

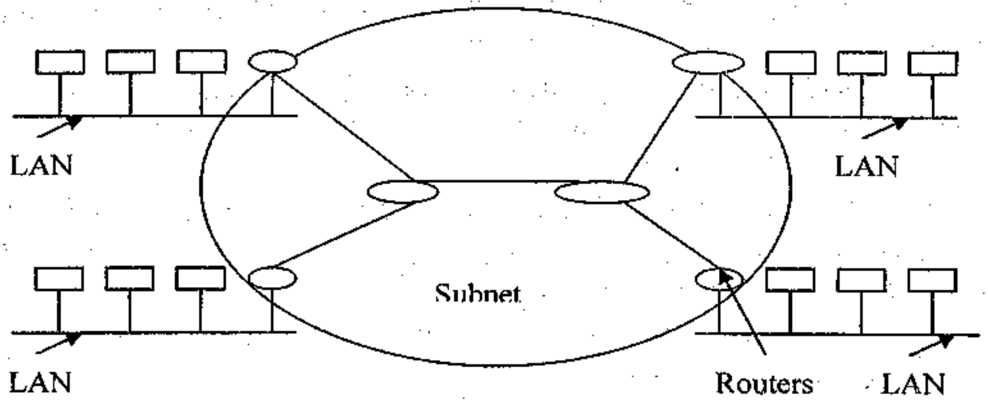
4.6.3 Wide Area Networks

A *wide area network* (WAN):

- spans a large geographical area,
- contains hosts (or end-systems) intended for running user programs,
- the hosts are connected by a *subnet* that carries messages from host to host.

The subnet usually consists of transmission lines (circuits, channels, or trunks) and switching elements. The switching elements are specialized computers used to connect two or more transmission lines. There is no standard technology used to name switching elements (e.g. packet switching nodes, intermediate systems, data switching exchanges). As a generic term we will use the word router.

Both packet switching and circuit switching technologies are used in the WAN. Packet switching allows users to share common carrier resources so that the carrier can make more efficient use of its infrastructure. Circuit Switching allows data connections to be established when needed and then terminated when communication is complete.



Relation between hosts and the subnet.

If two routers that do not share a cable wish to communicate, they must do it via other routers. When a packet is sent from one router to another via intermediate routers, the packet is received at each intermediate router, stored there until the required output line is free, and then forwarded. A subnet using this principle is called point-to-point, store-and-forward, or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets.

When the packets are small and all the same size, they are often called cells.

A second possibility for a WAN is a satellite or ground radio system. Each router has an antenna through which it can send and receive. All router can hear the output from the satellite. Satellite networks are inherently broadcast.

The world's most popular WAN is the Internet. Some segments of the Internet, like VPN-based extranets, are also WANs in themselves. Finally, many WANs are corporate or research networks that utilize leased lines.

4.6.4 Wireless Networks

The owners of mobile computers want to be connected to their home base when they are away from home. In case where wired connection is impossible (in cars, airplanes), the wireless networks are necessary.

The use of wireless networks:

- portable office - sending and receiving telephone calls, faxes, e-mails, remote login, ...
- rescue works,
- keeping in contact,
- military.

Wireless networking and *mobile computing* are often related but they are not identical. Portable computers are sometimes wired (e.g. at the traveler's stay in a hotel) and some wireless computer are not portable (e.g. in the old building without any network infrastructure).

Wireless LANs are easy to install but they have also some disadvantages: lower capacity (1-2 Mbps, higher error rate, possible interference of the transmissions from different computers).

Wireless networks come in many forms:

- antennas all over the campus to allow to communicate from under the trees,
- using a cellular (i.e. portable) telephone with a traditional analog modem,
- direct digital cellular service called CDPD (Cellular Digital Packet Data),
- different combinations of wired and wireless networking.

Self Assessments

True/ False

1. A Local Area Network (LAN) is a network that is confined to a large area.
2. Circuit switching network contains dedicated communication path.
3. Broadcast networks have a multiple communication channel.
4. Wireless networking and mobile computing are identical.

Fill in the Blanks

1. The world's most popular WAN is the ....
2. ....is sending a packet to a subset of the machines.
3. Possible topologies for LAN are..... and ......
4. A ...... is a network covering an area the size of a town or city

4.7 SUMMARY

- A network is a series of points or nodes interconnected by communication paths.
- Point-to-point networks consist of many connections between individual pairs of machines.
- Broadcast networks have a single communication channel that is shared by all the machines on the network.
- Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, tree, bus or ring topology.

- In packet switching data is divided in packets and send to router.
- A network can be categorized as a local area network(LAN), a metropolitan area network(MAN), or a wide area network(WAN).
- A Local Area Network (LAN) is a network that is confined to a relatively small area.
- A MAN is a network covering an area the size of a town or city.
- A WAN is a network covering a wide area including states, countries or the whole world,

4.8 UNIT END QUESTION

1. Discuss different types of network topologies.
2. What are different types of networks?
3. Differentiate circuit switching and packet switching?
4. Define the following: LAN, MAN and WAN .
5. Discuss how networks influence our daily life.

4.9 SOLUTION TO SAQS

	True/ False	**Fill in the Blank**
SAQ1	True False False True	Point-to-point Multipoint electronic funds transferinter connected
SAQ2	False	Internet Multicasting Bus, ring MAN

UNIT 5
COMPUTER NETWORKS

Structure of the Unit

5.0 OBJECTIVES

After this unit, you should be able to know:

- different reference model
- example of networks
- Internet Protocol Stack
- connection oriented and connection less services
- different types of data communication services

5.1 INTRODUCTION

The basics of computer were discussed in the previous unit. In this unit we will learn network reference models (OSI and TCP/IP), differentiate connection oriented and connection less services and finally discuss the examples of networks and data communication services.

5.2 LAYERED ARCHITECTURE

Most networks are organized as a series of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. But, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. Layers of same label can communicate with each other. For example, layer 2 on one machine can communicate with layer 2 on another machine. The rules and conventions used in this conversation are collectively known as the layers n protocol. A protocol is an agreement between the communication parties on how communication is to proceed. Means a protocol is a set of rules governing the format and meaning of the frame, packets, or message that are exchanged by the peer entities within a layer. Entities use protocol in order to implement their service definition.

5.3 REFERENCE MODELS

5.3.1 The OSI Reference Model

The *OSI model* is based on a proposal develop by ISO as a first step toward international standardization of the protocols used in the various layers. The model is called ISO OSI (Open Systems Interconnection) Reference Model.

Open system is a system open for communication with other systems.

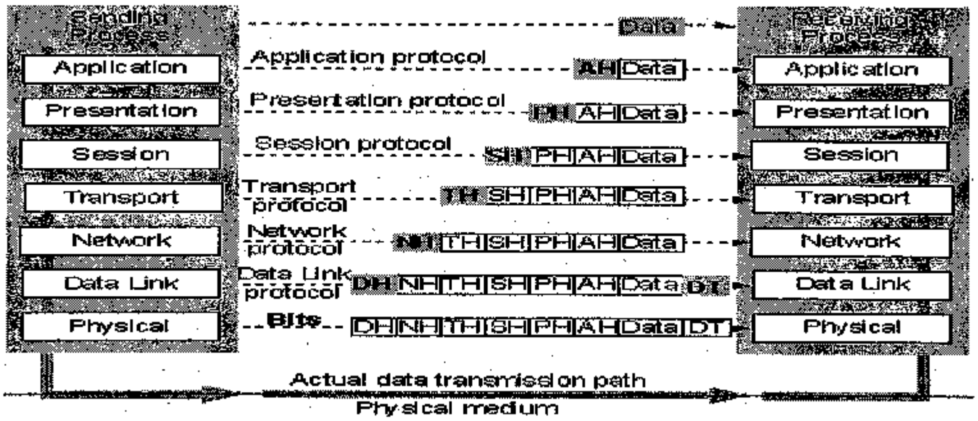
The OSI model has 7 layers (Fig. 5.1). The principles that were applied to arrive at the seven layers are as follows:

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

The OSI model is not a network architecture - it does not specify the exact services and protocols. It just tells what each layer should do.

Layer1 (The Physical Layer)- The physical layer coordinates the transmission of bit streams over the physical medium. It transmits encoded signals — either electrical or optical — over the connection. It receives data from the data link layer to send over a network, and also passes data back to the data link layer when it receives a signal.

The user of the physical layer may be sure that the given stream of bits was encoded and transmitted. User cannot be sure that the data came to the destination without error. This issue is solved in higher layers.



The OSI reference model.

Layer2 (The Data Link Layer)- The data link layer transforms the physical layer signal to a reliable link, shielding the layers above from any actual errors (transmission then appears error free). It breaks the stream of bits down into manageable units called frames.

The user of the data link layer may be sure that data were delivered without errors to the neighbor node. However, the layer is able to deliver the data just to the neighbor node.

Layer3 (The Network Layer)- The network layer is responsible for source-to-destination delivery of a packet over the network. Here, the physical addresses are used to identify hosts in the network, and the networking layer uses logical addresses (IP addresses) to send data over different networks to the specified host.

The user of the network layer may be sure that packet was delivered to the given destination. However, the delivery of the packet needs not to be in the order in which they were transmitted.

Layer 4(The Transport Layer)- The transport layer is responsible for end-to-end delivery of an entire data message. As the network layer below is responsible for sending data to the correct host, the transport layer oversees the transmission as a whole, and manages the sending and receiving of packets to ensure that a complete, error-free message is received.

The user of the transport layer may be sure that message will be delivered to the destination regardless of the state of the network. User need not worry about the technical features of the network.

Layer 5 (The Session Layer)- The session layer acts as the network's dialog controller. It establishes the interaction between two hosts over a network, and then also synchronizes the transmissions and acknowledgments between the two machines.

The user of the session layer is in similar position as the user of the transport layer but having larger possibilities.

Layer 6(The Presentation Layer)- The presentation layer deals with the syntax and semantics of the information exchanged between two systems. For instance, it encodes and decodes between bit streams that are sent over the network, and ASCII-based characters so that it can provide applications on the receiving host with usable data. Encryption and compression are also a part of the presentation layer.

Layer 7 (The Application Layer)- The application layer enables users to access and interact with the network. Interfaces for network-based applications such as email and FTP are handled here. A network virtual terminal application can also allow a user to login to a host remotely over the network and perform basic functionalities.

5.3.2 The TCP/IP Reference Model

TCP/IP reference model originates from the grandparent of all computer networks, the ARPANET and now is used in its successor, the worldwide Internet.

The name TCP/IP of the reference model is derived from two primary protocols of the corresponding network architecture.

The Internet Layer

The internet layer is the linchpin of the whole architecture. It is a connectionless internetwork layer forming a base for a packet-switching network. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination. 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. TCP/IP internet layer is very similar in functionality to the OSI network layer (Fig. 5.2).

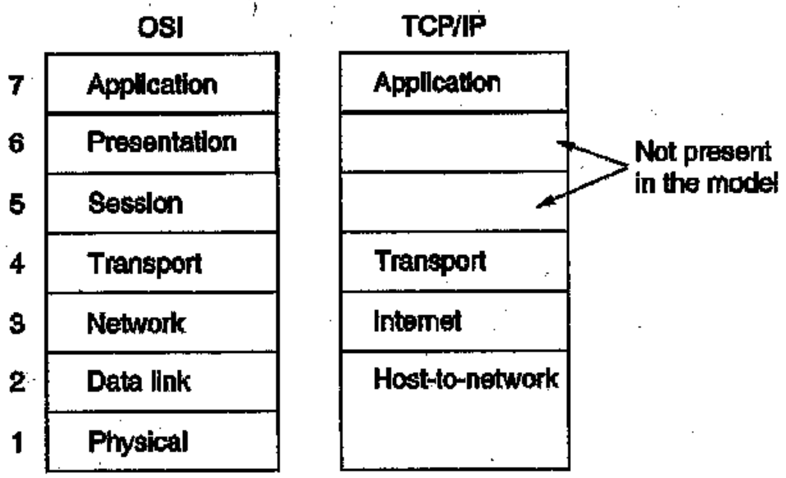


Fig. 5.2. The TCP/IP reference model.

The Transport Layer

The layer above the internet layer in the TCP/IP model is now usually called transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here:

- *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 onto the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control.
- *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.

The Application Layer

The application layer is on the top of the transport layer. It contains all the higher level protocols. Some of them are:

- Virtual terminal (TELNET) - allows a user on one machine to log into a distant machine and work there.
- File transfer protocol (FTP) - provides a way to move data efficiently from one machine to another.
- Electronic mail (SMTP) - specialized protocol for electronic mail.
- Domain name service (DNS) - for mapping host names onto their network addresses.

The Host-to-Network Layer

Below the internet layer there is a great void. 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 packet over it. This protocol is not defined and varies from host to host and network to network.

5.3.3. A Comparison of the OSI and TCP Reference Models

The OSI and the TCP/IP reference models have much in common:

- they are based on the concept of a stack of independent protocols,
- they have roughly similar functionality of layers,

- the layers up and including transport layer provide an end-to-end network-independent transport service to processes wishing to communicate.

The two models also have many differences (in addition to different protocols).

	OSI model	TCP/IP model
1.	It makes the clear distinction between its three central concepts that are services, interfaces, and protocols.	The TCP/IP model did not originally clearly distinguish between service, interface, and protocol
2.	The OSI reference model was devised before the protocols were invented. The positive aspect of this was that the model was made quite general, not biased toward one particular set of protocols.The negative aspect was that the designers did not have much experience with the subject and did not have a good idea of which functionality to put into which layer	With the TCP/IP the reverse was true: the protocols came first, and the model was just a description of the existing protocols. As a consequence, the model was not useful for describing other non-TCP/IP networks.
3	The OSI model supports both types of communication in the network layer, but only connection-oriented communication in the transport layer	The TCP/IP model has only connectionless mode in the network layer but supports both modes in the transport layer. The connectionless choice is especially important for simple request-response protocols.
4.	There are 7 layers in OSI model.	There are 4 layers in TCP/IP model.

5.4 PROTOCOL STACKS

A protocol stack is a group of protocols that all work together to allow software or hardware to perform a function. The **TCP/IP** protocol stack is a good example. It uses four layers that map to the OSI model as follows:

- **Layer 1: Network Interface** - This layer combines the Physical and Data layers and routes the data between devices on the same network. It also manages the exchange of data between the network and other devices.
- **Layer 2: Internet** - This layer corresponds to the Network layer. The **Internet Protocol** (IP) uses the IP address, consisting of a **Network Identifier** and a **Host Identifier**, to determine the address of the device it is communicating with.
- **Layer 3: Transport** - Corresponding to the OSI Transport layer, this is the part of the protocol stack where the **Transport Control Protocol** (TCP) can be found. TCP works by asking another device on the network if it is willing to accept information from the local device.
- **Layer 4: Application** - Layer 4 combines the Session, Presentation and Application layers of the OSI model. Protocols for specific functions such as e-mail (**Simple Mail Transfer Protocol, SMTP**) and file transfer (**File Transfer Protocol, FTP**) reside at this level.

As you can see, it is not necessary to develop a separate layer for each and every function outlined in the OSI Reference Model. But developers are able to ensure that a certain level of **compatibility** is maintained by following the general guidelines provided by the model.

5.5 CONNECTION-ORIENTED AND CONNECTIONLESS SERVICES

Two distinct techniques are used in data communications to transfer data. Each has its own advantages and disadvantages. They are the connection-oriented method and the connectionless method:

- **Connection-oriented** *connection-oriented* describes a means of transmitting data in which the devices at the end points use a preliminary protocol to establish an end-to-end connection before any data is sent. Requires a session connection (analogous to a phone call) be established before any data can be sent. Connection-oriented protocol service is sometimes called a "reliable" network service, because it guarantees that data will arrive in the proper sequence. Transmission Control Protocol (TCP) is a connection-oriented protocol.
- **Connectionless** In connectionless service data is sent from one end point to another without prior arrangement. Does not require a session connection between sender and receiver. The sender simply starts sending packets (called datagrams) to the destination. This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. A connectionless network provides minimal services. Connectionless protocols are usually described as stateless because the end points have no protocol-defined way to remember where they are in a "conversation" of message exchanges. Because they can keep track of a conversation, connection-oriented protocols are sometimes described as stateful.

Connection-oriented methods may be implemented in the data link layers of the protocol stack and/ or in the transport layers of the protocol stack, depending on the physical connections in place and the services required by the systems that are communicating.

Examples: TCP (Transmission Control Protocol) is a connection-oriented transport protocol, while UDP (User Datagram Protocol) is a connectionless network protocol. Both operate over IP. LANs operate as connectionless systems. The Internet is one big connectionless packet network in which all packet deliveries are handled by IP.

A WAN service that uses the connection-oriented model is frame relay. The service provider sets up PVCs (permanent virtual circuits) through the network as required or requested by the customer. ATM is another networking technology that uses the connection-oriented virtual circuit approach.

Self Assessment Questions 1

True/False.

1. The data link layer coordinates the transmission of bit streams.
2. TCP/IP reference model has 4 layers.
3. The IP address, consisting of a Network Identifier and a Host Identifier.
4. UDP is a connection-oriented transport protocol.

Fill in the Blanks.

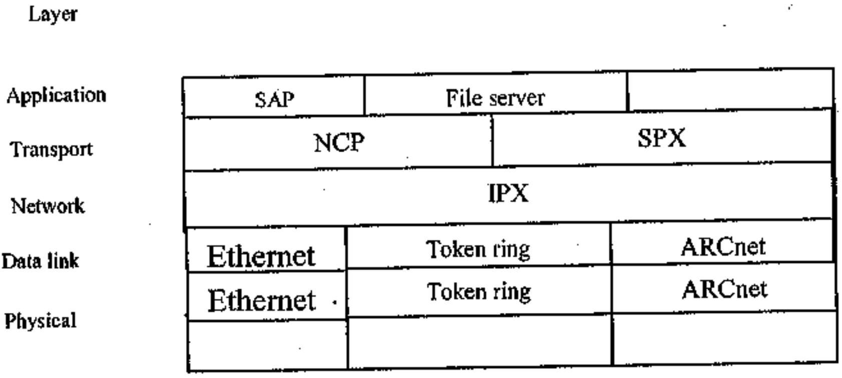
1. The .... is responsible for source-to-destination delivery of a packet over the network.
2. ....,is a system open for communication with other systems.
3. The ....is responsible for end-to-end delivery of an entire data message.
4. FTP stands for ....

5.6 EXAMPLES OF NETWORKS

5.6.1 Novell Netware

Novell Netware is a local-area network (LAN) operating system developed by Novell Corporation. NetWare is a software product that runs on a variety of different types of LANs, from Ethernets to IBM token-ring networks. It provides users and programmers with a consistent interface that is independent of the actual hardware used to transmit messages. It initially used cooperative multitasking to run various services on a PC. It provides desktop PC functionality, server services like file services, database services and other services to a collection of clients. It is based on the client-server model.

The network protocols were based on the archetypal Xerox XNS stack. It looks more like TCP/IP than like OSI.



NetWare has been superseded by Open Enterprise Server (OES). The latest version of NetWare is v6.5 Support Pack 7, which is identical to OES 2, NetWare Kernel.

The physical and data link layers can be chosen from any of the standard like Ethernet, IBM token ring and ARCnet. The network layer runs on unreliable IPX. IPX uses 10 byte address and passes packets transparently from source to destination, even if the source and destination are on different networks. For transport layer two protocols can be used, one is connection-oriented NCP(Network Core Protocol) that also provides various other services besides user data transport and second one is SPX, that only provides transport. For broadcasting it uses SAP(Service Advertising Protocol) protocol for giving its address and telling what services it offers. The packets are collected by special agent processes running on the router machines.

When the client machine is booted, it broadcast a request for the nearest server. The agent on the local router machine accepts the message and search in server's database and matches up the request with the best server. This information is sent back to client. Client can now establish an NCP connection with the server and file system and other services can be used by server with maximum packet size.

5.6.2 ARPAnet

The precursor to the Internet, ARPANET was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). Established in 1969, ARPANET served as a testbed for new networking technologies, linking many universities and research centers. ARPANET took advantage of the new idea of sending information in small units called packets that could be routed on different paths and reconstructed at their destination.

ARPA is a packet switched network, consisting of a subnet and host computer. The subnet consist of minicomputers called IMPs(Interface Message Processors) connected by transmission lines. Each IMP would be connected to at least two other IMPs for high reliability.

Each node of the network was to consist of an IMP and a host, in the same room, connected by short wire. A host could send messages of up to 8063 bits its IMP, which would then break these up into packet of at most 1008 bits and forward then independently toward the destination. Each packet was received in it's entirely before being forwarded. So the subnet was the first electronic store and forward packet switching network.

The software was split into two parts: subnet and host. The subnet software consisted of the IMP end of the host IMP connections, The IMP-IMP protocol and a source IMP to destination IMP protocol designed to improve reliability. The way that processes within the hosts communicated with one another through the network was known as the "host to host protocol". The host to host protocol was the second level protocol above the Host-IMP protocol. This protocol was implemented by the

NCP (network control program) which was part of a host's operating system. The NCP was responsible for connection establishment, connection termination and flow control. "NCP" eventually became synonymous with the host to host protocol. The NCP was the first transport layer protocol of the ARPANET.

5.6.3 Internet

The Internet is a worldwide collection of computer networks, cooperating with each other to exchange data using a common software standard. Through telephone wires and satellite links, Internet users can share information in a variety of forms.

No one is in charge of the Internet. There are organizations which develop technical aspects of this network and set standards for creating applications on it, but no governing body is in control. The Internet backbone, through which Internet traffic flows, is owned by private companies.

All computers on the Internet communicate with one another using the Transmission Control Protocol/ Internet Protocol suite, abbreviated to TCP/IP. Computers on the Internet use a client/server architecture. This means that the remote server machine provides files and services to the user's local client machine. Software can be installed on a client computer to take advantage of the latest access technology.

Components of the Internet:

E-mail: Electronic mail, or e-mail, allows computer users locally and worldwide to exchange messages. Each user of e-mail has a mailbox address to which messages are sent. Messages sent through e-mail can arrive within a matter of seconds.

Telnet: Telnet is a program that allows you to log into computers on the Internet and use online databases, library catalogs, chat services, and more. There are no graphics in Telnet sessions, just text.

FTP: FTP stands for File Transfer Protocol. This is both a program and the method used to transfer files between computers. Anonymous FTP is an option that allows users to transfer files from thousands of host computers on the Internet to their personal computer account.

E-mail Discussion Groups: One of the benefits of the Internet is the opportunity it offers to people worldwide to communicate via e-mail. The Internet is home to a large community of individuals who carry out active discussions organized around topic-oriented forums distributed by e-mail. These are administered by various types of software programs.

Usenet News: Usenet News is a global electronic bulletin board system in which millions of computer users exchange information on a vast range of topics. The major difference between Usenet News and e-mail discussion groups is the fact that Usenet messages are stored on central computers, and users must connect to these computers to read or download the messages posted to these groups.

Chat & Instant Messaging: Chat programs allow users on the Internet to communicate with each other by typing in real time. A variation of chat is the phenomenon of instant messaging. With instant messaging, a user on the Web can contact another user currently logged in and type a conversation.

World Wide Web: The World Wide Web (Web or WWW) is a system of Internet servers that supports hypertext to access several Internet protocols on a single interface. Almost every protocol type available on the Internet is accessible on the Web. This includes e-mail, FTP, Telnet, and Usenet News. In addition to these, the World Wide Web has its own protocol: HyperText Transfer Protocol, or HTTP. The World Wide Web consists of files, called pages or home pages, containing links to documents and resources throughout the Internet.

5.7 EXAMPLE DATA COMMUNICATION SERVICES

Telephone companies and other have begun to offer networking services to any organization that wishes to subscribe. The subnet is owned by the network operator providing communication service for the customer's hosts and terminals. Such a system is called a public network.

5.7.1 X.25 Networks

An X.25 network is an older packet-switched network based on Open System Interconnection (OSI) network architecture rather than on TCP/IP architecture. It is mostly used for commercial networks. It allows WAN-to-WAN or LAN connectivity at up to 2Mbps (megabits per second), but due to heavy error-checking protocols, its effective network speed is very slow.

It was developed during the1970 by CCITT to provide an interface between public packet-switched networks and their customers. X.25 is connection-oriented and supports both switched virtual circuits and permanents ones. A switched virtual circuit is created when one computer sends a packet to the network asking to make a call to a remote computer. Once established, packets can be sent over the connection, always arriving in order. X.25 provides flow control, to make sure a fast sender can't swamp a slow or busy receiver.

A permanent virtual circuit is used the same way as a switched one, but it is setup in advance by agreement between the customer and the carrier. It is analogous to a leased line. The user or network operator installs a "black box" to which these terminals can connect. The black box is called a PADC(Packer Assembler Disassembler).

Advantages

The following are some of the advantages of X.25 protocol:

- X.25 is a networking protocol, which provides highly secure and reliable data communication.
- X.25 guarantees 100% error correction and network-managed flow control.
- X.25 is a stable and a proven packet switched technology that has been around for many years.This offers the secure communication between the two end nodes.
- X.25 allows creation of multiple virtual connections over the same connection to a PSN. Each connection is called a virtual circuit (VC).
- X.25 supports the reverse charging facility, by which the cost for each call can be evaluated.

Disadvantages

The major disadvantages of X.25 that causes it to be less useful in today's protocols world are the following:

- X.25 was designed when the underlying physical link was unreliable. By contrast, contemporary
- networks provide very high levels of reliability for which other protocols are well suited, like Frame Relay and IP.
- X.25 transaction is pretty slow, a feature that makes it un-suitable for most applications. The error correction and detection mechanism of X.25 caused it to have an inherent delay.
- X.25 requires a massive buffering capability in order to support the store-and-forward mechanism of data transfer which makes it very expensive and inefficient.

5.7.2 Frame Relay

Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission.

Frame relay is a service for people who want an absolute bare-bones connection-oriented way to move bits from A to B at reasonable speed and low cost. Frame relay can be best be thought of as a virtual leased line. The customer leases a permanent virtual circuit between two points and can be send frames (i.e. packets) of up to 1600 bytes between them. It is also possible to lease permanent virtual circuits between a given site and multiple other sites, so each frame carries a 10-bit number telling which virtual circuit to use.

Frame relay provides a minimal service, primarily a way to determine the start and end of each frame, and detection of transmission errors. If a bad frame is received, the frame relay service simply discards it. It is up to the user to discover that frame is missing and take the necessary action to recover. Unlike X.25, frame relay does not provide acknowledgement or normal flow control. It does have a bit in the header, however, which one end of a connection can set to indicate to the other end that problems exist. The use of this bit is up to users.

Advantages of Frame Relay

The success of the Frame Relay protocol is based on the following two underlying factors:

- Because virtual circuits consume bandwidth only when they transport data, many virtual circuits can exist simultaneously across a given transmission line. In addition, each device can use more of the bandwidth as necessary, and thus operate at higher speeds.
- The improved reliability of communication lines and increased error-handling sophistication at end stations allows the Frame Relay protocol to discard erroneous frames and thus eliminate time-consuming error-handling processing.

These two factors make Frame Relay a desirable choice for data transmission; however, they also necessitate testing to determine that the system works properly and that data is not lost.

5.7.3 Broadband ISDN and ATM

The telephone companies are aced with fundamental problem: multiple networks. Telephone and Telex use old circuit-switched networks. Each of the new data services as frame relay uses its own packet-switched network. DQDB (MAN) is different from these, and there is also the internal telephone call management network. Maintaining all these separate networks is a major headache, and there is another network, cable television, that the telephone companies do not control and would like to.

The solution of this problem is to invent a single new network for the future that will replace all the specialized networks with a single integrated network for all kinds of information transfer. This new network will have a huge data rate compared to all existing networks and services and will make it possible to offer a large variety of new services. This big project is now under way.

The new wide area service is called *B-ISDN* (Broadband Integrated Services Digital Networks). It will offer:

- video on demand,
- live television from many sources,
- multimedia electronic mail,
- CD-quality music,
- LAN interconnection,
- high-speed data transport for science and industry,
- many other services, all over the telephone line.

The underlying technology that makes B-ISDN possible is called ATM (Asynchronous Transfer Mode) because it is not synchronous (tied to a master clock).

A great deal of work has already been done on ATM and on B-ISDN system, although there is more ahead.

The basic idea behind *ATM* is to transmit all information in small, fixed-size packet called cells. The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are data. ATM as a service is sometimes called cell relay.ATM networks are connection-oriented.

ATM networks are organized like traditional WANs, with lines and switches. The intended speeds for ATM networks are 155 Mbps and 622 Mbps, with possible gigabit speeds later. It is worth pointing out that different organizations involved in ATM have different (financial) interests (the long-distance telephone carriers and PTTs vs. computer vendors). All these competing interests do not make the ongoing standardization process any easier, faster, or more coherent. Also, politics within the organization standardizing ATM (The ATM Forum) have considerable influence on where ATM is going.

Self Assessment 2

True/False:

1. Usenet News is a global electronic bulletin board system.
2. Novell Netware is a local-area network (LAN) operating system.
3. WWW is not the service of Internet.
4. TCP is a connectionless transport protocol

Fill in the Blanks.

1. An ..... network is an older packet-switched network.
2. ATM networks are ....
3. ....is a local-area network (LAN) operating system developed by Novell Corporation.
4. Data link layer is above the .... layer.

5.8 SUMMARY

- The *OSI model* is based on a proposal develop by ISO as a first step toward international standardization of the protocols used in the various layers.
- TCP/IP reference model originates from the grandparent of all computer networks
- Protocols can be either connectionless or connection–oriented.
- Protocol stacks are typically based on the OSI model or the TCP/IP model.
- Both of model have network, transport, and application layers, but they differ on the other layers.
- Well-known networks have included Novell's NetWare, the ARPANET, the Internet etc.
- Network services included X.25 , Frame Relay, and broadband ISDN.

5.9 UNIT END QUESTIONS

1. Discuss similarities and dissimilarities between OSI reference model and TCP/IP
2. Does the Novell Netware architecture look more like X.25 or like the Internet ? Explain your answer.
3. List out main components of Internet.
4. What is protocol stack? Give a suitable example.
5. Differentiate the TCP and UDP.

5.10 SOLUTION TO SAQS

	True/False	**Fill in the blanks**
SAQ1	False True True False	Network layer Open system Transport layer File Transfer Protocol
SAQ2	True True False False	X.25 Connection-oriented Novell Netware Physical

UNIT 6
PHYSICAL LAYER

Structure of the Unit

6.0 OBJECTIVES

After this unit, you should be able to know:

- Different transmission media
- ISDN (Narrowband and Broadband) services
- ATM networks & transmission
- FDDI

6.1 INTRODUCTION

In the Previous unit we have learned network reference models (OSI and TCP/IP), differentiate connection oriented and connection less services and examples of networks and data communication services. In this unit we will discuss topics related to physical layer, which will comprise of different transmission media, Narrowband ISDN, Broadband ISDN and ATM networks.

6.2 PHYSICAL LAYER

The Physical Layer is the first level in the seven-layer OSI model of computer networking. It translates communications requests from the Data Link Layer into hardware-specific operations to effect transmission or reception of electronic signals. The Physical Layer is a fundamental layer upon which all higher level functions in a network are based.

6.3 TRANSMISSION MEDIA

The purpose of the physical layer is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission. Media are mainly grouped into:

- **Conducted or guided media** - use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver. The data signals are bound by the "cabling" system. Guided Media is also known as Bound Media. Examples are copper wire and fiber optics.
- **Wireless or unguided media**- use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals. The data signals are not bound to a cabling media and as such are often called Unbound Media. Examples are radio and laser through the air.

6.3.1 Transmission Media - Guided

There are 4 basic types of Guided Media:

- Open Wire
- Twisted Pair
- Coaxial Cables
- Optical Fibre

Open Wire

Open Wire is traditionally used to describe the electrical wire strung along power poles. There is a single wire strung between poles. No shielding or protection from noise interference is used. This media is susceptible to a large degree of noise and interference and consequently not acceptable for data transmission except for short distances under 20 ft.

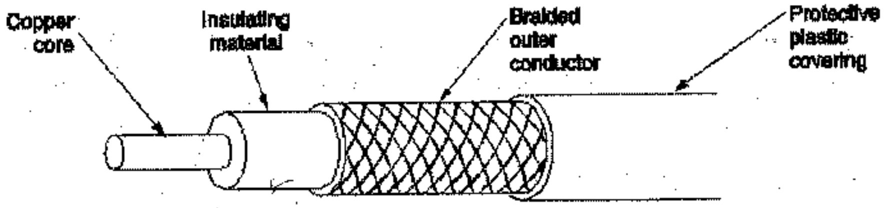
Twisted Pair

Twisted Pair wiring (Cat 3 and Cat 5) are popular methods of transferring data. They are especially prevalent in the LAN environment. The twists allow the signal to travel further than it could on a regular copper wire. The more twists per centimeter, the further the signal can travel. This is why Cat 5 wire (with more twists) is preferred over Cat 3 wire. Twisted pair wires consist of two strands of copper twisted together; the wires are unshielded, which is why Twisted Pair wire is also called Unshielded Twisted Pair (UTP).

Coaxial Cables

There are two types of coaxial cables:

- **Baseband Coaxial Cable:** Baseband coaxial cable is an insulated copper wire covered with a mesh conductor, with a coating of plastic on top of that. Coaxial cable has better shielding than twisted pairs, so it can span longer distances at higher speeds. The construction and shielding of coaxial cable give it a good communication of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable length.
- **Broadband Coaxial Cable:** The other kind of coaxial cable system uses analog transmission on standard cable television cabling. It is called broadband. In networking, the term "broadband" refers to any cable that uses analog transmission. The reason broadband cables are used is to get longer distances, but amplifiers are needed. These amplifiers transform the cable into a unidirectional cable. If two-way communication is needed, two cables will be needed (one going one way, the other goes the other way).



A coaxial cable.

Optical Fibre

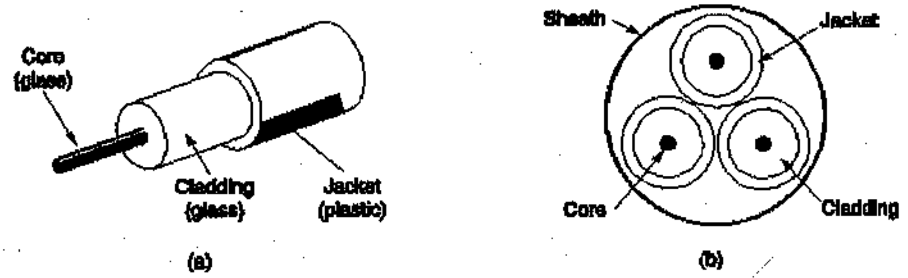
Fiber optics is one of the advances that have propelled communication technology into the future at high speeds. Communication over fiber optics requires a source (of light), a line (transmission medium = fiber), and a destination (to detect the light). The light stays within the fiber line because of the angle at which the light hits the surface of the fiber line. Instead of passing through the fiber's surface (like a window), the light bounces off of it (like a mirror). The light propagates down the fiber line because it continually reflects off the surface from the inside; the light never escapes the fiber line until the receiver detects it.

Like copper, fiber optics suffers problems when transmitting over a distance. Attenuation (a weakening of the power of a signal) occurs, as well as dispersion (the spreading out of light waves over a distance). The discovery of solitons has helped wipe out the problem of dispersion, though. A fiber cable is heavily insulated like coax, but it has several differences. The core of the cable is a glass strand, which is surrounded by a thick glass covering, which is then covered by plastic.

When compared to copper for its overall purposes, fiber wins because it is lighter, higher bandwidth, easier to install, harder to tap, and the signal stays stronger longer than in copper. The only drawback to fiber at this point in time is the lack of familiarity among the engineering community with the fiber technology compared to the copper.

Optical fibres use light to transmit data. A thin glass fibre is encased in a plastic jacket which allows the fibre to bend without breaking. A transmitter at one end uses a *light emitting diode* (LED) or *laser* to send pulses of light down the fibre which are detected at the other end by a light sensitive transistor.

Following figure illustrates a single fibre (a) and a sheath of three fibres (b). Other configurations are possible.



Single fibre and a sheath of three fibres

Optical fibres have four main advantages over copper wires.

- They use light which neither causes electrical interference nor are they susceptible to electrical interference
- They are manufactured to reflect the light inwards, so a fibre can carry a pulse of light further than a copper wire can carry a signal
- Light can encode more information that electrical signals, so they carry more information than a wire
- Light can carry a signal over a single fibre, unlike electricity which requires a pair of wires

6.3.2 Transmission Media - Unguided

Unguided Transmission Media is data signals that flow through the air. They are not guided or bound to a channel to follow. They are classified by the type of wave propagation.

Radio

A network that uses electromagnetic radio waves operates at *radio frequency* and its transmissions are called RF transmissions. Each host on the network attaches to an antenna, which can both send and receive RF.

Satellites

Radio transmissions do not bend round the surface of the earth, but RF technology combined with satellites can provide long-distance connections.

The satellite contains a *transponder* consisting of a radio receiver and transmitter. A ground station on one side of the ocean sends a signal to the satellite, which amplifies it and transmits the amplified signal at a different angle than it arrived at to another ground station on the other side of the ocean.

A single satellite contains multiple transponders (usually six to twelve) each using a different radio frequency, making it possible for multiple communications to proceed simultaneously. These satellites are often *geostationary*, i.e. they appear stationary in the sky. To achieve this, their orbit must be 22,236 miles (35,785 kilometres) high.

Microwave

Electromagnetic radiation beyond the frequency range of radio and television can be used to transport information. Microwave transmission is usually point-to-point using directional antennae with a clear path between transmitter and receiver.

Infrared

Infrared transmission is usually limited to a small area, e.g. one room, with the transmitter pointed towards the receiver. The hardware is inexpensive and does not require an antenna.

Self Assessment Questions

True/False

1. Examples of guided media are copper wire and fiber optics.
2. Infrared transmission is usually for large area.
3. Optical fibres use light to transmit data.
4. The Physical Layer is the third level in the seven-layer OSI model.

Fill in the Blanks

1. The satellite contains a .... consisting of a radio receiver and transmitter.
2. Twisted Pair wiring ......and .... are popular methods of transferring data.
3. Two types of coaxial cables are baseband and broadband
4. .... media use radio waves of different frequencies.

6.4 NARROWBAND ISDN

The objective of ISDN is to replace a major portion of the worldwide telephone system with an advanced digital system by the early part of the century. Its primary goal is the integration of voice and nonvoice services. ISDN, or Integrated Services Digital Network, can be categorized as either narrowband ISDN or broadband ISDN.

Because ISDN is so focused on 64-kbps channels, we refer to it as Narrowband ISDN, to contrast it with Broadband ISDN (ATM). Narrowband ISDN is the original implementation of this technology, which was designed to provide a standard for an integrated voice and data network over standard telephone lines. The primary advantage of this technology was that modems would not be needed to convert the signal into analog and then back into digital again.

6.4.1 ISDN Services

ISDN services offer data transmission services in addition to the normal voice services, so that information relevant to a call can be accessed at the same time as the call is answered, and it can be accessed on the same line.

Enhanced voice services:

- Telephones with multiple buttons for instant call setup to arbitrary telephone anywhere in the world.

- Telephones that display the caller's phone number, name, address, even the caller's database record.
- Call transfer and forwarding to any number worldwide and conference calls worldwide.
- Build-in mechanism for leaving messages, without using external answering machines.
- Automatic wakeup call service, without operators involvement.

New non-voice services:

- Computers with connections to any other one in the world, as telephones connections now-a-day.
- Computer-to-computer connections with multicast and broadcast mode.
- Closed user group for setting up private networks.
- **Videotex** which is interactive access to a remote database by a person at a terminal. E.g., on-line telephone book, Yellow Pages, order, payment, reservations, banking, etc.
- **Teletex** which is essentially a form of electronic mail for home and business. Telephones are turned into telephone/terminal workstations (must be cheap) for videotex, and for composing, editing, sending, receiving, archiving, and printing emails.
- **Fax** in which an image is scanned, digitized, transmitted, redrawn on a remote side. In effect, it is a distributed photocopy machine. High bandwidth is required.

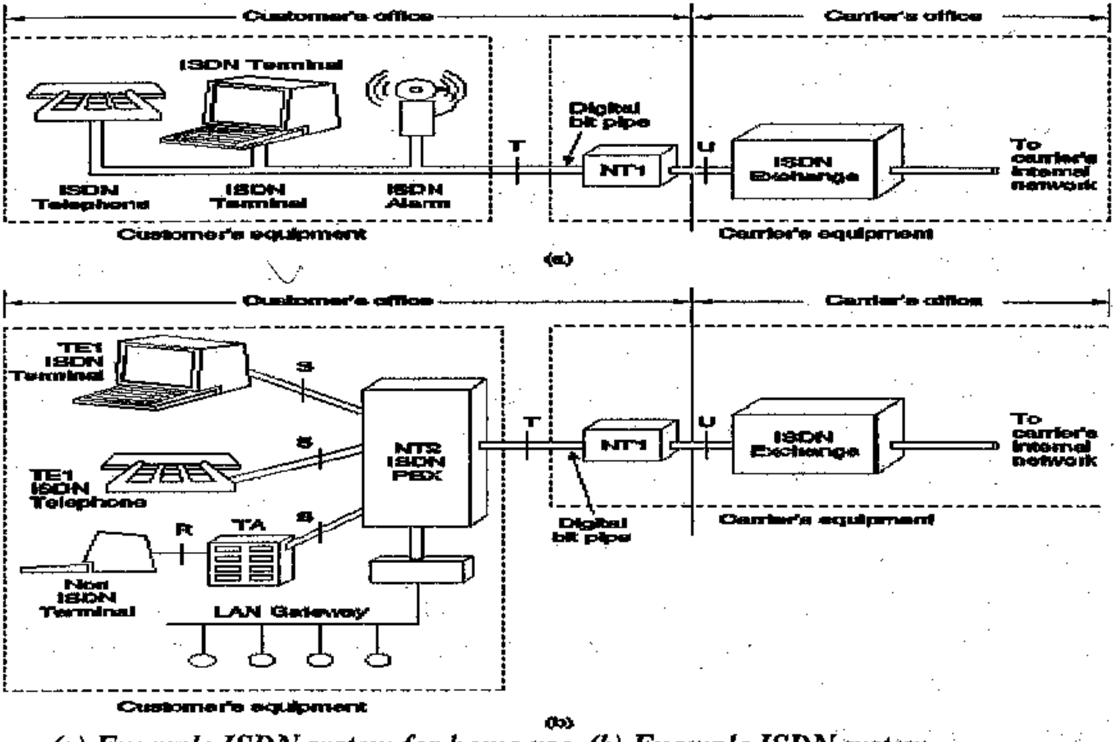
6.4.2 ISDN System Architecture

The key idea behind ISDN is the **digital bit pipe.** The ISDN's digital bit pipe does not care what kind of digital information is being sent on it—all data is treated the same way. Since businesses and homes use their communications differently, two different standards for ISDN have been developed: one for the home (low bandwidth) and one for businesses (high bandwidth).**Digital bit pipe** is:

- A conceptual pipe between the customer and the carrier through which bits flow.
- Bits may be generated by any device.
- Bits flow in both directions.
- Multiple independent channels can share one pipe by time division multiplexing.

NT1: A network device betweem the custormer's premises and the ISDN exchange.

NT2 or **PBX (Private Branch eXechange)**: an ISDN-exchange-like device between user's equipment and NT1.



(a) Example ISDN system for home use. (b) Example ISDN system with a PBX for use in large businesses.

6.4.3 The ISDN Interface

The ISDN but pipe supports multiple channels interleaved by time division multiplexing. The different services and data rates offered by ISDN are named for letters of the alphabet (A, B, C, D, E, H) in the standards.

A- 4-kHz analog telephone channel

B- 64-kbps digital PCM channel for voice or data

C- 8-or-16 kbps digital channel

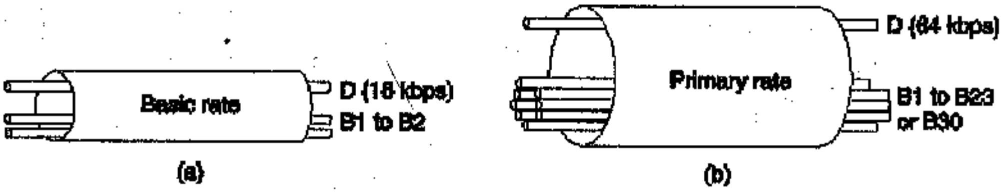
D- 16-kbps digital channel for out-of-band signaling

E- 64-kbps digital channel for internal ISDN signaling

H- 384-,1536, or 1920 –kbps digital channel

Three combinations have been standardized so far:

1. Basic rate : 2B + 1D
2. Primary rate :23 B + 1D (U.S. and Japan) or 30B +1D
3. Hybrid: 1A +1C



(a) Basic rate digital pipe. (b) Primary rate digital pipe.

6.4.4 Perspective on N-ISDN

The first ISDN services that were developed are now called Narrowband ISDN because they have a lesser data transmission rate than the newer Broadband ISDN (B-ISDN). ISDN will likely be implemented most often for fast Internet access, since other services such as video on demand will be better suited for B-ISDN.

6.5 Broadband ISDN: Broadband Integrated Services Digital Network (BISDN)

Broadband Integrated Services Digital Network (BISDN or Broadband ISDN) is designed to handle high-bandwidth applications. BISDN currently uses ATM technology over SONET-based transmission circuits to provide data rates from 155 to 622Mbps and beyond, contrast with the traditional narrowband ISDN (or N-ISDN), which is only 64 Kbps basically and up to 2 Mbps.

The designed Broadband ISDN (BISDN) services can be categorized as follows:

- Conversational services such as telephone-like services, which was also supported by N-ISDN. Also the additional bandwidth offered will allow such services as video telephony, video conferencing and high volume, high speed data transfer.
- Messaging services, which is mainly a store-and-forward type of service. Applications could include voice and video mail, as well as multi-media mail and traditional electronic mail.
- Retrieval services which provides access to (public) information stores, and information is sent to the user on demand only.
- No user control of presentation. This would be for instance, a TV broadcast, where the user can choose simply either to view or not.
- User controlled presentation. This would apply to broadcast information that the user can partially control.

The B-ISDN is designed to offer both connection oriented and connectionless services. The broadband information transfer is provided by the use of asynchronous transfer mode (ATM), in both cases, using end-to-end logical connections or virtual circuits. Broadband ISDN uses out-of-band signaling (as does N-ISDN). Instead of using a D Channel as in N-ISDN, a special virtual circuit channel can be used for signaling. However, B-ISDN was not widely deployed so far.

6.5.1 Virtual Circuit versus Circuit Switching

The basic broadband ISDN service is a compromise between pure circuit switching and pure packet switching. The actual service is connection oriented, but implemented with packet switching, not circuit switching. Connections are of two types:

- Permanent virtual circuit : Requested by the customer manually and remain in place for months or years.
- Switched virtual circuits: They set up dynamically (like telephone call) as needed and potentially torn down immediately afterward.

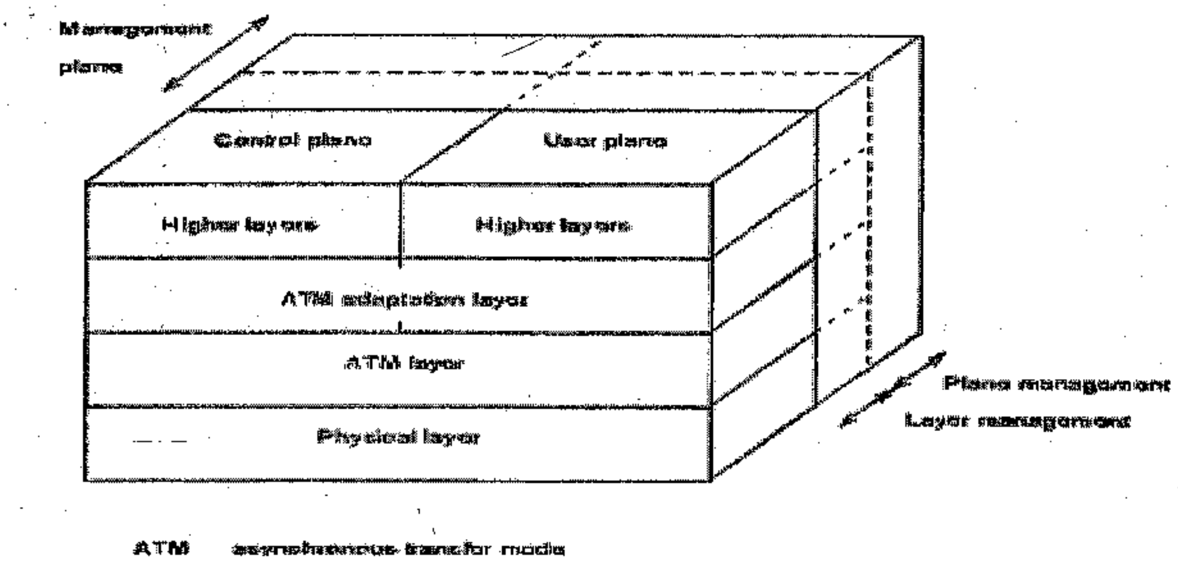
In circuit switching network, a dedicated physical path is established from source to the destination, when space division switches are used. In virtual circuit network, like ATM, the route is chosen from source to destination and all the switches (i.e. routers) along the way make table entries so they can route any packet on that virtual circuit. When a packet comes along, the switch inspects the packet's header to find which virtual circuit it belong to. Then it looks up that virtual circuit in its table to determine which communication line to send on.

Comparison of Circuit Switching and Packet Switching

Circuit Switching	**Packet switching**	
	Datagram packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Messages are not stored	Packets may be stored until delivered	Packet stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; packet transmission delay

6.5.2 Protocol Structure - B ISDN: Broadband Integrated Services Digital Network (Broadband ISDN)

Broadband ISDN protocol reference model is based on the ATM reference model



ATM reference model

ATM adaptation layer (AAL). This layer is responsible for mapping the service offered by ATM to the service expected by the higher layers. It has two sublayers.

ATM Layer. This layer is independent of the physical medium over which transmission is to take place. It has those functions: Generic flow control (GFC) function, Cell header generation and extraction, Cell multiplex and demultiplex.

Physical layer. This consists of two sublayers: Transport Convergence (TC) and Physical medium (PM)

The management plane consists of two functions to perform layer management and plane management. The plane management is not layered as the other layers are. This is because it relies needs information on all aspects of the system to provide management facilities for the systems as a whole. The layer management provides information and control facilities for the protocol entities that exists in each individual layer. This includes operation and maintenance (OAM) functions for each layer.

The control plane is responsible for the supervision of connections, including call set-up, call release and maintenance.

6.6 ATM: Asynchronous Transfer Mode Protocol

The Asynchronous Transfer Mode (ATM) composes a protocol suite which establishes a mechanism to carry all traffic on a stream of fixed 53-byte packets (cells). A fixed-size packet can ensure that the switching and multiplexing function could be carried out quickly and easily. ATM is a connection-oriented technology, i.e.; two systems on the network should inform all intermediate switches about their service requirements and traffic parameters in order to establish communication.

The ATM reference model, which has two forms - one for the user-to-network interface (UNI) and the other for the network-to-node interface (NNI), is divided into three layers: the ATM adaptation layer (AAL), the ATM layer, and the physical layer. The AAL interfaces the higher layer protocols to the ATM Layer, which relays ATM cells both from the upper layers to the ATM Layer and vice versa. When relaying information received from the higher layers, the AAL segments the data into ATM cells. When relaying information received from the ATM Layer, the AAL must reassemble the payloads into a format the higher layers can understand. This is called Segmentation and Reassembly (SAR). Different AALs are defined in supporting different types of traffic or service expected to be used on ATM networks.

The ATM layer is responsible for relaying cells from the AAL to the physical layer for transmission and from

Different AALs are defined in supporting different types of traffic or service expected to be used on ATM networks.

The ATM layer is responsible for relaying cells from the AAL to the physical layer for transmission and from the physical layer to the AAL for use at the end systems, it determines where the incoming cells should be forwarded to, resets the corresponding connection identifiers and forwards the cells to the next link, as well as buffers cells, and handles various traffic management functions such as cell loss priority marking, congestion indication, and generic flow control access. It also monitors the transmission rate and conformance to the service contract (traffic policing).

The physical layer of ATM defines the bit timing and other characteristics for encoding and decoding the data into suitable electrical/optical waveforms for transmission and reception on the specific physical media used. In addition, it also provides frame adaptation function, which includes cell delineation, header error check (HEC) generation and processing, performance monitoring, and payload rate matching of the different transport formats used at this layer. SONET , DS3, Fiber, twisted-pair are few media often used at the physical layer.

6.6.1 Transmission in ATM

ATM stands for Asynchronous Transfer Mode. This mode can be contrasted with the synchronous T1 carrier .

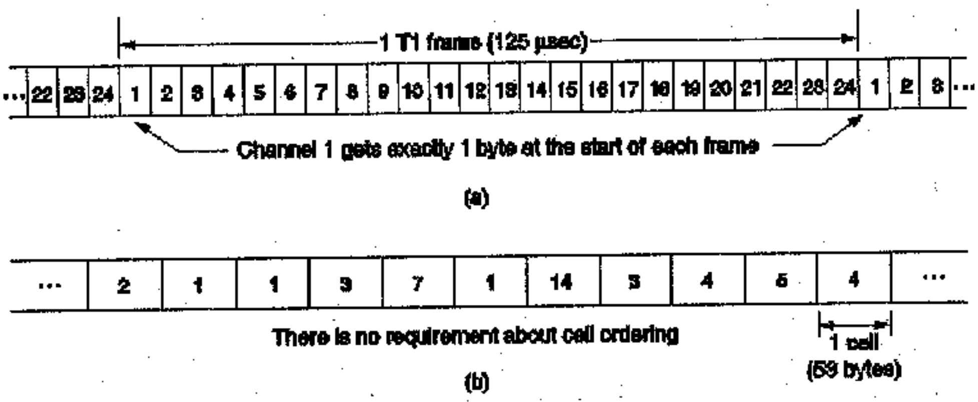


Fig. 6.7 (a) Synchronous transmission mode. (b) Asynchronous transmission mode.

T1: frames are generated precisely every 125(sec. This rate is governed by a master clock. Slot k of each frame contains 1 byte of data from the same source.

ATM: has no requirements that cells rigidly alternate among the various sources. Cells arrive randomly from different sources. The stream of cells need not be continuous. Gaps between the data are filled by special idle cells.

ATM does not standardize the format for transmitting cells. Cells are allowed to be sent individually, or they can be encased in a carrier such as T1, T3, SONET, or FDDI. For these examples, standards exist telling how cells are packed into the frames these systems provides.

In the original ATM standard, the primary rate was 155.52 Mbps, with an additional rate at four time that speed (622.08 Mbps). These rates were chosen to be compatible with SONET. ATM over T3 (44.736 Mbps) and FDDI (100 Mbps) is also foreseen.

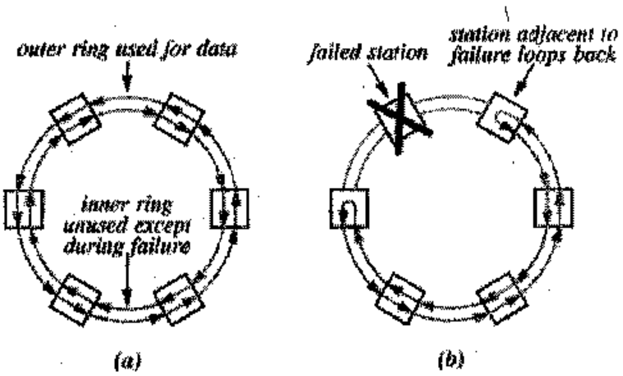
The transmission medium for ATM is normally fiber optics, but for runs under 100 m, coax or category 5 twisted pair are also acceptable. Each link goes between a computer and an ATM switch, or between two ATM switches. So, all ATM links are point-to-point. Each link is unidirectional. For full-duplex operation, two parallel links are needed.

6.7 HIGH SPEED LANS

For low speeds and short distances, 802 LANs and MAN are used, but for high speeds and longer distances LANs must be based on fiber optics or highly parallel copper networks. Fiber has high bandwidth, is thin and light weight, is not affected by electromagnet interference from heavy machinery, power surges or lightning and has excellence security. So, fast LANs often use fiber.

6.7.1 FDDI(Fiber Distributed Data Interface) –It is a high performance fiber optics token ring LAN running at 100 Mbps over distance up to 200 km with up to1000 stations connected. It has high bandwidth. Although FDDI protocol is a token ring network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus *timed token* protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. FDDI-II is the successor to FDDI, modified to handle synchronous circuit switched PCM data for voice or I SDN traffic, in addition to ordinary data.

FDDI uses multimode fibers and LEDs rather than lasers. A FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles). FDDI has a larger maximum-frame size than standard 100 Mbit/s Ethernet, allowing better throughput. FDDI protocol uses token for data transmission i.e. a station must first capture mes around again.


outer ring used for data
inner ring unused except during failure
failed station
station adjacent to failure loops back
(a)
(b)

FDDI network

Self Assessment Question 2

True/ False

1. The first ISDN services that were developed are now called Broadband ISDN.
2. Broadband ISDN protocol reference model is based on the ATM reference model.
3. FDDI protocol is a based on bus network.
4. ISDN stands for Integrated Services Digital Network

Fill in the Blank

1. The key idea behind ISDN is the.........
2. ATM stands for...........
3. FDDI protocol is a .... network.
4. Broadband ISDN protocol reference model is based on the ......reference model.

6.8 SUMMARY

- The Physical Layer is a fundamental layer upon which all higher level functions in a network are based.

- The purpose of the physical layer is to transport a raw bit stream from one machine to another.
- Transmission Medias are of two types: guided and unguided.
- ISDN, or Integrated Services Digital Network, can be categorized as either narrowband ISDN or broadband ISDN.
- ISDN is based on digital bit pipe.
- Broadband Integrated Services Digital Network (BISDN or Broadband ISDN) is designed to handle high-bandwidth applications.
- Broadband ISDN protocol reference model is based on the ATM reference model.

6.9 UNIT END QUESTIONS

1. Name the two major categories of transmission media.
2. What are the three major classes of guided media?
3. List out different ISDN services.
4. What are the main categorization of Broadband ISDN?
5. Define the ATM networks.
6. What is Digital Pipe line?

6.10 SOLUTIONS TO SAQS

	True/False	Fill in the Blanks
SAQ1	True False True False	Transponder Cat 3 , Cat 5 Baseband, Broadband Unguided
SAQ2	False True False True	digital bit pipe Asynchronous Transfer Mode token ring ATM

UNIT - 7

DATA LINK LAYER & LAN

Structure of the Unit

7.0 OBJECTIVE

After completing this unit student should be able to understand the following tasks:

- Identify the role of the Data Link layer as it describes communication from one end device to another device.
- Examine the most common Data Link layer protocol : HDLC
- Understand principles behind data link layer services:
  - o error detection, correction
  - o sharing a broadcast channel: multiple access
  - o link layer addressing
  - o reliable data transfer, flow control
  - o instantiation and implementation of various link layer technologies

7.1 INTRODUCTION

This chapter focuses on the role of the Data Link layer - examining how it divides networks into groups of hosts to manage the flow of data packets within a network. We also consider how communication between networks is facilitated. This communication between networks is called routing. Data Link Layer is responsible of transferring datagram from one node to adjacent node over a link.

Information in data packets are encoded and decoded into bits within this layer. Errors from the physical layer flow control and frame synchronization are corrected here utilizing transmission protocol knowledge and management. This layer consists of two sub layers: the Media Access Control (MAC) layer, which controls the way networked computers gain access to data and transmit it, and the Logical Link Control (LLC) layer, which controls frame synchronization, flow control and error checking.

Link Layer Services :

Framing, link access: encapsulate datagram into frame, adding header, trailer channel access if shared medium "MAC" addresses used in frame headers to identify source, destination(different from IP address!)

Reliable delivery between adjacent nodes : seldom used on low bit error link (fiber, some twisted pair); and for wireless links: high error rates

Flow Control: pacing between adjacent sending and receiving nodes

Error Detection: errors caused by signal attenuation, noise. receiver detects presence of errors: signals sender for retransmission or drops frame

Error Correction: receiver identifies and corrects bit error(s) without resorting to retransmission

Half-duplex and full-duplex : with half duplex, nodes at both ends of link can transmit, but not at same time.

7.2 SERVICES PROVIDED BY THE LINK LAYER

Framing: Units of data exchanged by the link layer are called **frames**. When transporting IP and related connectionless network-layer protocols, each frame normally encapsulates one network-layer datagram. Each frame will include a data field and a number of header (and/or trailer) fields. The frame on multiple access links usually include **physical address** fields which are different from network layer addresses.

Link access: Specifies the rules by which a frame can be transmitted onto the link.

Most interesting when the multiple hosts can access the link. Examples of multiple access links include traditional Ethernet, token ring, and wireless. The frame protocol must coordinate the transmissions of many nodes.

Reliable delivery: When a link-layer protocol includes reliable delivery, it guarantees to move each network-layer datagram across the link without error. Link-layer reliable delivery may be used for links with high error rates, such as wireless. Reliable delivery is usually considered unnecessary overhead for low bit-error links, such as fiber, coax, and twisted pair media. The bit-error rates on most of these media are very low when everything is functioning correctly.

Flow control: The link-layer protocol cat provide for flow control so that the sender will not overwhelm the receiver.

Error detection: Most link-layer protocols provide for error detection by means of error-detection bits in the frame header/trailer. This is usually more sophisticated than error detection on higher layers, and is usually implemented in hardware.

Error correction: In some cases the error detection facility is enhanced to allow for error correction.

Half-duplex and full-duplex: This apply primarily to point-to-point links. Under full-duplex, both ends of the link may transmit at the same time.

Network Interface Adaptors : An **adaptor** or **network interface card** or **NIC** is the interface between a node and the physical media. The link-layer protocol is usually implemented in hardware on the adaptor. The main components of the adaptor are the bus interface (to interface with the node) and the link interface (to interface with the physical media).

Error detection and correction techniques : The objective is to make the probability of an undetected bit-error to be small. Obviously, not all bit errors can be detected.

Parity: Parity is like a 1-bit checksum. The bits of the data field are added up mod 2, and the parity bit is this sum (or possibly the complement). This is may be used for sending 7-bit ASCII text. Then the 8th bit is used as a parity bit. However, bit errors tend to occur in bursts, and parity is not a good way to detect burst errors since if there are an even number of bit-errors in the data field, the errors will not be detected There is also 2-dimensional parity where parity is computed in two directions. The bits in successive data fields are added mod 2. 2-dimensional parity can detect and correct 1-bit errors.

Forward error correction: (FEC) refers to the ability of the receiver to both detect and correct errors. FEC is used in audio storage and playback devices, such as audio CDs. In a network setting, they allow for the receiver to correct errors without waiting for a retransmission.

Checksumming: In checksumming, the d-bit data field is considered as a sequence of k-bit integers, and these integers are added mod 2k. The checksum is either the sum or the ones-compliment of the sum. Checksumming can be easily computed in software, and so tends to be used in higher level protocols where the initial implementation was in software.

Cyclic Redundancy check (CRC): CRC codes are widely used in link-layer protocols. The bit-string can be viewed as a polynomial whose coefficients are 0 and 1, and operations can be viewed as polynomial arithmetic operations. CRC codes operate as follows: Supposed that a d-bit data field D is to be sent. The sender and the receiver agree on an r-bit pattern known as the **generator**. We will call the generator G (G is determined by the protocol.) The leftmost bit of G is assumed to be 1. The sender will append an additional r-bit CRC field to the end of the data D so that the resulting d + r bit pattern is exactly divisible by G. Division is carried out in bitwise modulo 2 arithmetic. Calculations are done in modulo 2 arithmetic without carries between bits. Addition and subtraction are both equivalent to the bitwise exclusive-or (XOR) operation.

Multiplication can be done by the grade-school algorithm—using modulo 2 arithmetic without carries. Division can be done by the grade-school long-division algorithm—using modulo 2 arithmetic without carries. Multiplying by 2k is equivalent to a left-shift by k bits. Thus, 2r _ D XORR is the d + r bit pattern sent by the sender and How is R calculated? We want to choose R so that 2r _ D XOR R is divisible by G. In other words, we want to choose R so that there exists a quotient n such that 2r _ D XOR R = nG If we add (i.e., exclusive-or) R to both sides we get: 2r _ D = nG XOR R This is of the form dividend = divsor _ quotient + remainder.

In other words, R is the remainder on division of 2r _ D by G.

Standards define G for the r values of 8, 12, 16, and 32.

The CRC standards can be shown to detect all burst errors of less than r + 1 bits and will detect any odd number of bit errors. In addition, they will detect longer burst errors with high probability (under appropriate assumptions). CRC calculations can be easily and efficiently implemented in hardware. Thus, CRC is commonly used for hardware-implemented protocols.

Introduction to multiple access protocols

There are two kinds of network links:

A **point-to-point** link connects two nodes.

A **broadcast link** can have more than 2 nodes all connected to the same channel.

It is called a *broadcast* link because a sending node broadcasts the frame, and all other nodes receive a copy. Traditional Ethernet and wireless are good examples.

Multiple access protocols:

If more than one node transmits a frame at the same time, a **collision** occurs.

Typically, when a collision occurs, none of the receiving nodes can make any sense of any of the frames transmitted. Thus, it is necessary to coordinate the transmissions to minimize or eliminate collisions. This is the job of the multiple access protocol.

There are three categories of multiple access protocols:

- Channel portioning protocols.
- Random access protocols.
- Taking-turns protocols.

Simple channel partitioning protocols.

Time Division Multiplexing (TDM).

TDM divides time into time frames which are in turn divide into time slots. If there are N nodes on the link, then each frame will be divided into N slots. Each of these slots is allocated to a node. Each node gets 1=N of the bandwidth, so the TDM is completely fair. TDM can work well if nodes need a uniform and predictable amount of bandwidth (such as a phone conversation). TDM does not work very well when the amount of bandwidth needed or desired is highly variable (such as typical computer data traffic).

Frequency Division Multiplexing (FDM).

FDM divides the channel into different frequencies. Again, each of N nodes gets a fraction 1=N of the total bandwidth. For optical fiber, this is called **Wave Division Multiplexing (WDM).** FDM has the same advantages and disadvantages as TDM.

Error Detection

When data is transmitted from one computer to another, we usually assume that it gets through correctly. But sometimes things go wrong and the data is changed accidentally. This activity uses a magic trick to show how to detect when data has been corrupted, and to correct it. The occurrence of a data bit error in a serial stream of digital data is an infrequent occurrence. Even less frequent is the experience of numerous errors within the transmission of a single message. Usually if a number of errors occur then it can be presumed that either a significant interference occurred effecting the transmission line or that there is a major failure in the communications path. Largely because of the extremely low bit-error rates in data transmissions, most error detection methods and algorithms are designed to address the detection or correction of a single bit error. However, as we shall soon see, many of these methods will also detect multiple errors. Error correction, though, will remain

a one-bit error concern. Probably the most common and oldest method of error detection is the use of **parity.** While parity is used in both asynchronous and synchronous data streams, it seems to find greater use in low-speed asynchronous transmission applications, however, its use is not exclusive to this.

Parity Error Detection

Parity works by adding an additional bit to each character word transmitted. The state of this bit is determined by a combination of factors, the first of which is the type of parity system employed. The two types are even and odd parity. The second factor is the number of logic 1 bits in the data character. In an even parity system, the parity bit is set to a low state if the number of logic 1s in the data word is even. If the count is odd, then the parity bit is set high. For an odd parity system, the state of the parity bit is reversed. For an odd count, the bit is set low, and for an even count, it is set high.

EXAMPLE

What is the state of the parity bit for both an odd and an even parity system for the

extended ASCII character B?

Solution:

The extended ASCII character B has a bit pattern of 01000010 (42 H). The number of logic 1s in that pattern is two, which is an even count. For an even parity system, the parity bit would be set low and for an odd parity system, it would be set high.

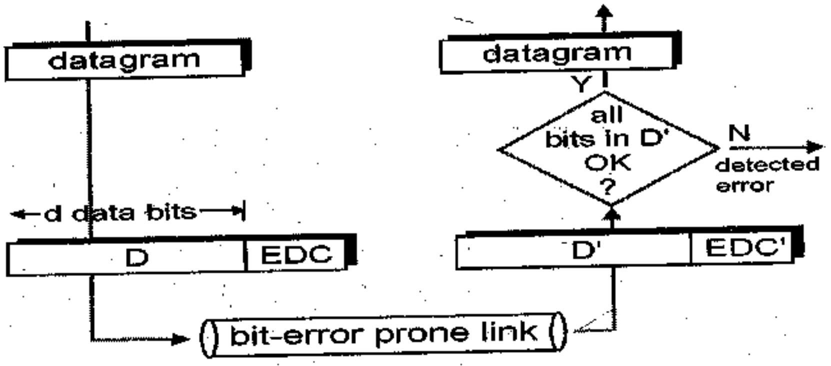
To detect data errors, each character word that is sent has a parity bit computed for it and appended after the last bit of each character is sent. At the receiving site, parity bits are recalculated for each received character. The parity bits sent with each character are compared to the parity bits the receiver computes. If their states do not match, then an error has occurred. If the states do match, then the character *may* be errorfree.

EDC= Error Detection and Correction bits (redundancy)

D = Data protected by error checking, may include header fields

- Error detection not 100% reliable!
- protocol may miss some errors, but rarely

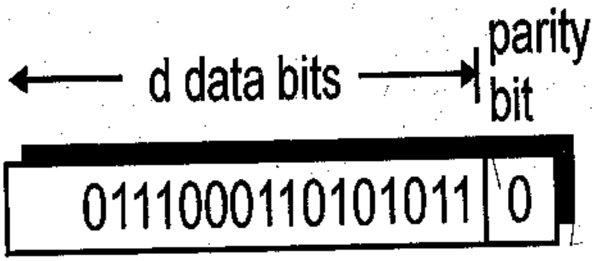
- larger EDC field yields better detection and correction

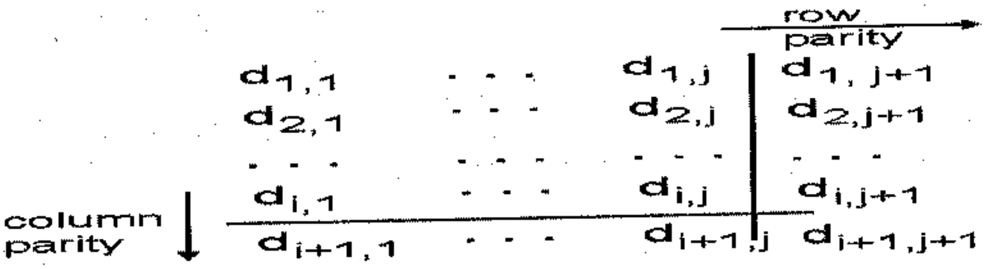


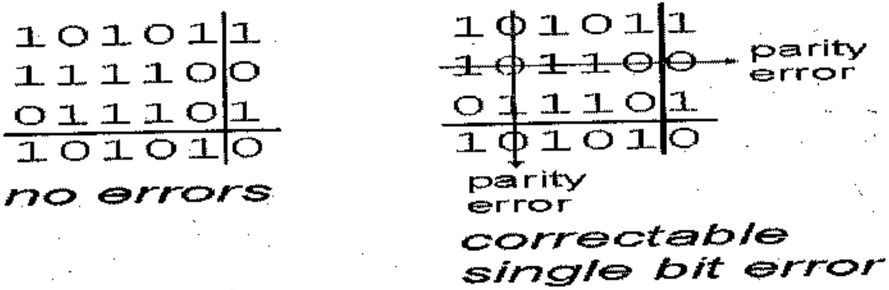
Parity Checking :

Single Bit Parity: Detect single bit errors

Two Dimensional Bit Parity: Detect and correct single bit errors




row parity
column parity
$d_{1,1}$ . . . $d_{1,j}$ $d_{1,j+1}$
$d_{2,1}$ . . . $d_{2,j}$ $d_{2,j+1}$
$d_{i,1}$ . . . $d_{i,j}$ $d_{i,j+1}$
$d_{i+1,1}$ . . . $d_{i+1,j}$ $d_{i+1,j+1}$



ARQ : To correct errors using parity, the receiving station can only request that the message containing the error be retransmitted. A system that is capable of requesting retransmission of a bad message automatically in response to detecting an error has *Automatic Request for Retransmission* or *Automatic Repeat Request (ARQ)* processing within its communications software package. ARQ was originally designed to be used with a special type of character code that used a seven-bit character size. The uniqueness of that code was that each character code contained three bits that were high and four that were low. If any character received is detected with more or less than three high bits in it, it is flagged as bad and the receive station automatically requests that the character be retransmitted.

The automatic request process has been incorporated into other error detection software such as those which respond to parity errors with any available character code. Not all systems using parity have ARQ functions included in their programs. Some use a parity error flag contained within a status register, which, when read by an application program, causes a message to be sent to a terminal to inform a user that a data error has occurred. It is then up to that user to determine if it is necessary to request the message be retransmitted. The advantage of doing this is that some errors are less critical than others and do not require taking up communication time for a retransmission of the data. For instance, an error in a plain text message may be obvious enough that the user can easily determine the correct character in the text. In that case, there is no need to have the text resent. The drawback to this method is that the display of the message must be interrupted to inform the user that an error has occurred and that it does require some action on the user's part.

Data Correction Using LRC/VRC

Parity is primarily used for detecting errors in a serial data character. A bad parity match indicates a logic error has occurred in one of the character's data bits. The use of parity called a **vertical redundancy check (VRC)** can be extended to allow single-bit error correction to take place in a received data stream. By having the ability to correct an error, a receiver would not require a message to be retransmitted, but could do the correction itself. The trade-off in using an error-correction scheme is that an additional character has to be sent with the message and additional software and/or hardware must be used to create and interpret that character. For asynchronous data transmission, that character is known as the **longitudinal redundancy check (LRC)** character.

Using a VRC/LRC system, the message is sent with each character containing the

regular even-parity bit known as the VRC bit. As with error-detection schemes, any mismatch between transmitted and received VRCs indicates that the character contains a bad data bit. In order to correct the bad bit, what is left to be done is to determine which of the character's bits is the bad one. This is where LRC comes in. It is used to create a crossmatrix type of configuration where the VRC bit denotes the row (character) and the LRC, the column (bit position) of the message's bad bit. At the sending site, each of the data bits of each character is exclusive ORed with the bits of all the other data bits. This is best illustrated by example.

Example :

Determine the states of the LRC bits for the asynchronous ASCII message "Help!"

Solution:

The first step in understanding the process is to list each of the message's characters with their ASCII code and even VRC parity bit:

LSB MSB	**VRC**	**CHARACTER**
0 0 0 1 0 0 1	0	H
1 0 1 0 0 1 1	0	e
0 0 1 1 0 1 1	0	l
0 0 0 0 1 1 1	1	p
1 0 0 0 0 1 0	0	!

Next, for each vertical column, find the LRC bit by applying the exclusive OR function. To make this process easier, you can consider the results of the exclusive OR process as being low or zero (0), if the number of ones (1) are even, and one (1) if the count is odd. For instance, in the LSB column, there are two 1's, so the LRC bit for that column is a 0. And for the rest:

LSB	MSB VRC	CHARACTER
0 0 0 1 0 0 1	0	H
1 0 1 0 0 1 1	0	e
0 0 1 1 0 1 1	0	l
0 0 0 0 1 1 1	1	p
1 0 0 0 0 1 0	0	!
0 0 0 0 1 0 0	1	LRC

When the message is transmitted, the LRC character is sent following the last character of the message. The receiver reads in the message and duplicates the process, including the LRC character in the exclusive OR process. If there were no errors, then the VRC's would all match and the resulting LRC would be 0.

Cyclic Redundancy Check One of the most frequently used error-detection methods for synchronous data transmissions is **cyclic redundancy check (CRC)** developed by IBM. This method uses a pseudo-binary-division process to create the error or CRC character, which is appended to the end of the message. The hardware circuitry that generates the CRC character at the transmitter is duplicated at the receiver. This circuitry is incorporated into the transmit and receive shift registers that send and receive the actual message. We will begin by exploring the method used to create and check the CRC character and then view the circuitry

that performs the operation. In the original specification for CRC, IBM specified a 16-bit CRC character designated as CRC-16. For CRC-16, those positions are:

16 12 5 0 ;   10001000000100001

which, as a quadratic expression, is written as:

$G(X) = X16 + X12 + X5 + 1$ note: $X0 = 1$

The process uses a constant "divisor" to perform the "division"

process, which appears in binary for CRC-16 as:

1000 1000 0001 0000 1

Again, spaces are used for clarity. In actuality, there are no spaces. Now that we have a "divisor" we need something for it to be divided into. This is the message. The process is begun by adding 16 zeros (one less than the number of bits in the "divisor") after the last bit of the message. These 16-bits will eventually be replaced by the CRC character. The "divisor" is then exclusive ORed with the seventeen most significant bits of the message. Enough additional message bits are appended to the result of the exclusive OR process to fill out 17-bit positions starting with the first logic 1 of the exclusive OR result. The process is repeated until the last bits of the message (including the added zeros) are used. The result from the last exclusive OR process becomes the CRC-character that replaces the 16-zero bits originally added to the message (leading zeros are added as needed). This process is best viewed by example, which will use a smaller CRC "divisor" to shorten the process.

Example :

Compute the CRC-4 character for the following message using a "divisor" constant

of 10011:   1100 0110 1011 01

Solution :

CRC-4 is used for illustration purposes since an example using CRC-16 looks cumbersome on paper and is difficult to follow. However, the principle is the same. Notice that the "divisor" is 5-bits, one more than the number indicated by the CRC type (CRC-4). The same was true for CRC-16, which had a 17-bit "divisor." We start the process by adding four zeros to the data stream and removing the spaces we have been using for convenience:

110001101011010000

Next, set up the problem to appear as a division problem:

10011)110001101011010000

Start the "division" process by exclusive OR the "divisor" with the first five bits of the message:

```
10011 )110001101011010000
        10011
         1011
```

Now bring "down" one bit so that the result of the exclusive OR process is filled out to the "divisor" size and repeat the process:

```
10011 )110001101011010000
        10011
        10111
        10011
          100
```

Continue with the process until all of the bits in the message plus the added four

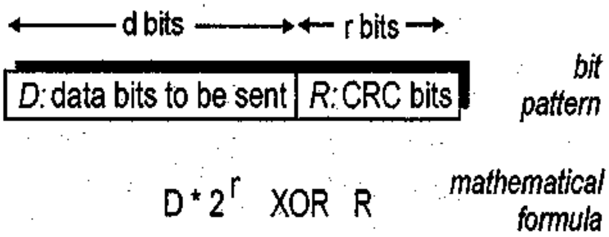
zeros are used up:

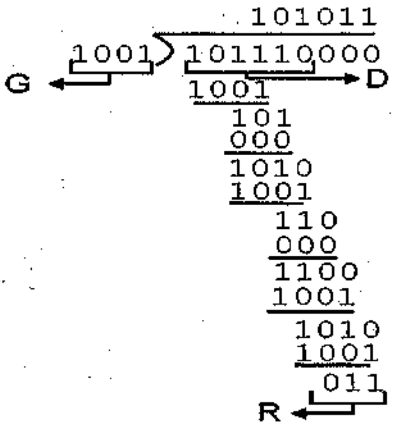
1001 = CRC character

The CRC character is appended onto the end of the message and transmitted. At the receiver, the process is repeated, except that there are no zeros added to the message. Instead, the CRC character fills up those positions. If the result of the process at the receiver produces zero then no errors occurred. If any bit or combination of bits are wrong, then the receiver will yield a non-zero result.

In short, Operation is: View data bits, D, as a binary number; choose r+1 bit pattern generator, G, goal: choose r CRC bits, R, such that <D,R> exactly divisible by G (modulo 2).

Receiver knows G, divides <D,R> by G. If non-zero remainder: error detected! can detect all burst errors less than r+1 bits widely used in practice (ATM, HDCL).





Checksum Error Detection

Another method of error detection uses a process known as **checksum** to generate an error-detection character. The character results from summing all the bytes of a message together, discarding and carry-over from the addition. Again, the process is repeated at the receiver and the two checksums are compared. A match between receiver checksum and transmitted checksum indicates good data. A mismatch indicates an error has occurred. This method, like CRC, is capable of detecting single or multiple errors in the message. The major advantage of checksum is that it is simple to implement in either hardware or software. The drawback to checksum is that, unless you use a fairly large checksum (16- or 32-bit instead of 8-bit), there are several data-bit patterns that could produce the same checksum result, thereby decreasing its effectiveness. It is possible that if enough errors occur in a message that a checksum could be produced that would be the same as a good message. This is why both checksum and CRC error-detection methods do not catch 100% of the errors that *could* occur, they both come pretty close.

Example

What is the checksum value for the extended ASCII message "Help!"?

Solution :

The checksum value is found by adding up the bytes representing the Help! characters:

01001000 H

01100101 e

01101100l

01110000 p

00100001 !

00010000 Checksum

Error detection is an acceptable method of handling data errors in lan-based networks because retransmission of most messages result in a short delay and a little extra use of bandwidth resources. Imagine a satellite orbiting around Jupiter or Saturn, transmitting critical visual data as binary stream information. The time it takes for those transmissions to reach Earth is measured in hours. During this time, the satellite has adjusted its orbit and is soaring across new territory and sending additional data. Correcting errors in these messages cannot be done by retransmission. A request for that retransmission takes as long to get to the satellite as the original message took to get to Earth. Then consider the time it would take to retransmit the message. What would the satellite do with new data, reach it while it tries to handle the retransmitting of old data? The memory needed to hold the old data in case it would need to be resent is astronomical to say the least. Instead, an error-correcting method such as the Hamming code is used so that errors can be corrected as they are detected.

ERROR CORRECTION

Hamming Code

For synchronous data streams, a error-correcting process called **Hamming code** is commonly used. This method is fairly complex from the standpoint of creating and interpreting the error bits. It is implemented in software algorithms and relies on a lot of preliminary conditions agreed upon by the sender and receiver. Error bits, called Hamming bits, are inserted into the message at random locations. It is believed that the randomness of their locations reduces the statistical odds that these

Hamming bits themselves would be in error. This is based on a mathematical assumption that because there are so many more messages bits compared to Hamming bits, that there is a greater chance for a message bit to be in error than for a Hamming bit to be wrong. Another school of thought disputes this, claiming that each and every bit in the message, including the Hamming bits, has the same chance of being corrupted as any other bit. Be that as it may, Hamming bits are inserted into the data stream randomly. The only crucial point in the selection of their locations is that both the sender and receiver are aware of where they actually are. The first step in the process is to determine how many Hamming bits (**H**) are to be inserted between the message (**M**) bits. Then their actual placement is selected. The number of bits in the message (M) are counted and used to solve the following equation to determine the number of Hamming (H) bits: $2^{H} >= ?M + H - 1$

Once the number of Hamming bits is determined, the actual placement of the bits

into the message is performed. It is important to note that despite the random nature of the Hamming bit placements, the exact same placements must be known and used by both the transmitter and the receiver. This is necessary so that the receiver can remove the Hamming bits from the message sent by the transmitter and compare them with a similar set of bits generated at the receiver.

Example :

How many Hamming bits are required when using the Hamming code with the extended ASCII synchronous message “Help!” ?

Solution:

The total number of bits in the message is:

M = 8-bits/character ??5 characters = 40 bits

This number is used in Equation 3–1 to determine the number of Hamming bits:

$2^{H} >= 40 + H + 1$

The closest value to try is 6 bits for H, since $2^{6} = 64$, which is greater than $40 + 6 + 1 = 47$. This satisfies the equation.

Once the Hamming bits are inserted into their positions within the message, their

states (high or low) need to be determined. Starting with the least significant bit (LSB) as bit 1, the binary equivalent of each message-bit position with a high (1) state is exclusive ORed with every other bit position containing a 1. The result of the exclusive OR process is the states of the Hamming bits. Once again, as with previous error detection and correction-processes, it is best to view how the Hamming code works by using an example.

Example :

Determine the states of the six Hamming bits inserted into the message “Help!” at every other bit position starting with the LSB.

Solution :

In the last example, we determined that six Hamming bits were required for the “Help!” message. For simplicity, we shall insert the Hamming bits a little less

randomly: H e l p !

01001000011001010110110001110000001H0H0H0H0H1H

Starting from the LSB on the right, the first 1 is encountered in bit position 2, the next in position 12 and so forth:

Bit Position	**Equivalent Binary**
2	0 0 0 0 1 0
12	0 0 1 1 0 0
19	0 1 0 0 1 1
20	0 1 0 1 0 0
21	0 1 0 1 0 1

25	0 1 1 0 0 1
26	0 1 1 0 1 0
28	0 1 1 1 0 0
29	0 1 1 1 0 1
31	0 1 1 1 1 1
33	1 0 0 0 0 1
36	1 0 0 1 0 0
37	1 0 0 1 0 1
42	1 0 1 0 1 0
45	1 0 1 1 0 1
H =	1 0 0 1 1 0

All these binary values are exclusive ORed together—an odd number of ones produces a 1, and an even count, a 0—to create the Hamming bits values. These values are substituted for the H-bits in the message. The entire thing is then transmitted and the process repeated at the receiver:

01001000011001010110110001110000001100000010110

If the message was received without any errors, then the Hamming-bit states produced at the receiver will match the ones sent. If an error in one bit did occur during transmission, then the difference between the transmitted Hamming bits and the receiver results will be the bit position of the bad bit. This bit is then inverted to its correct state. The limitation imposed by the Hamming code is twofold. First, it works only for single-bit errors, and secondly, if one of the Hamming bits becomes corrupted, then the receiverwill actually invert a correct bit and place an error in the message stream.

Example :

Demonstrate how the Hamming code is used to correct a single-bit error in the data stream.

Solution :

During the transmission of the message, bit 19 experiences a noise spike that causes it to be received as a 0 instead of 1. The receiver goes through the process of determining the states of the Hamming code, resulting in this calculation:

2	0 0 0 0 1 0
12	0 0 1 1 0 0
20	0 1 0 1 0 0
21	0 1 0 1 0 1
25	0 1 1 0 0 1
26	0 1 1 0 1 0
28	0 1 1 1 0 0
29	0 1 1 1 0 1
31	0 1 1 1 1 1
33	1 0 0 0 0 1
36	1 0 0 1 0 0
37	1 0 0 1 0 1
42	1 0 1 0 1 0
45	1 0 1 1 0 1
H =	1 1 0 1 0 1

Notice that bit 19 is not included in the list since it was received as a low-state instead of a high-state. Now we compare the Hamming code transmitted to this one the receiver just derived:

Transmitted code: 1 0 0 1 1 0

Receiver code: 1 1 0 1 0 1

0 1 0 0 1 1 = bit 19

There is no "black magic" mystery to why the Hamming code works. The originally transmitted codes are formulated by adding binary bits together (the exclusive OR process), ignoring carries. A similar process occurs at the receiver. If a bit has changed, then the two sums will be different and the difference between them will be the bit position number that was not added at either the transmitter or the receiver. By comparing the two Hamming codes using exclusive OR gates, the numbers are effectively being subtracted from one another (another function of the exclusive OR gate) and the difference is the bad bit position.

7.3 DLL PROTOCOLS

Data Link Layer protocols transfer data through serial data link, are categorized in two classes : Synchronous vs. Asynchronous. Another categorization is **Character-oriented**: used in case of slower data rate links (for example, modems using Kermit and X-modem) vs. **bit-oriented mode**: used in case of higher rate link involving long physical separations (for example, radio-based satellite links, circuits through private multiplexer networks use HDLC).

Data link protocols are located in the two communicating DTEs (including network equipment working as a DTE). Data Link Layer Protocols HDLC, ADCCP, LAP-B, LAP-D, SDLC, Kermit, XMODEM, BSC. X.25 packet switching networks use LAPB (link access procedure, balanced) as data link protocol based on HDLC.

ISDN (integrated service digital network) uses LAPD (link access procedure D channel) based on HDLC. In LANs, LLC (logical link control, subclass of HDLC) is used (e.g: ethernet, ring, bus.)

- Stop and Wait
  - Source transmits frame
  - Destination receives frame and replies with acknowledgement
  - Source waits for ACK before sending next frame
  - Destination can stop flow by not send ACK
  - Works well for a few large frames

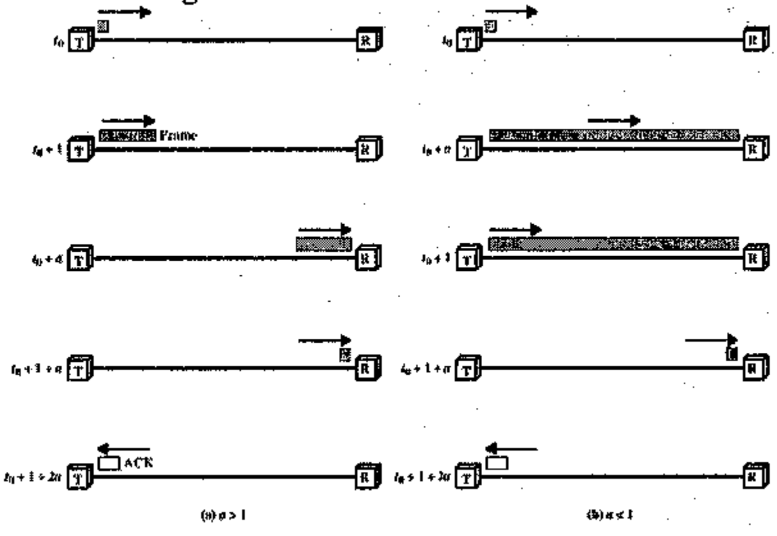


Figure 7.2 Stop-and-Wait Link Utilization (transmission time = 1; propagation time = a)

Courtesy: W.Stallings

7.3.1 Sliding Window Flow Control

The link utilization for Stop and Wait protocol is poor. The Sliding-window protocol has performs well with characteristics :

- Allow multiple frames to be in transit
- Receiver has buffer W long
- Transmitter can send up to W frames without ACK

- Each frame is numbered
- ACK includes number of next framė expected
- Sequence number bounded by size of field (k)
- Frames are numbered modulo 2k

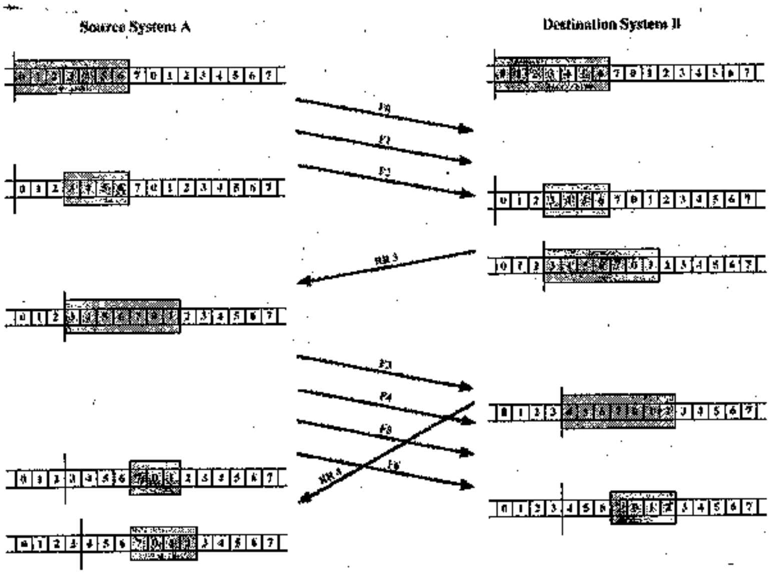


Figure 7.4 Example of a Sliding-Window Protocol

Courtesy: W.Stallings

Automatic Repeat request (ARQ)

Also known as Positive Acknowledgement with Retransmission(PAR)

- Sequence numbers
  - – going into a finite field in the header so must be cyclic
  - – how many numbers are needed?
- Stop and wait protocol
  - – Only confusion between adjacent packets since sender
  - – waits for a positive ack
  - –1 bit (2 sequence numbers) will suffice

Utilisation

Utilisation is the fraction of an available resource that is actually used. It can be calculated either in time or frequency space e.g A 2Mb/s link with 50% utilisation transmits 1Mb/s of information on average. The same link would also be occupied for 50% of the time.

ARQ Bandwidth Utilisation

- Protocols discussed so far only have 1 frame in transit
  - – with bandwidth B, delay T and N bits /frame
  - – transmission time T+N/B
  - – round trip time 2T+N/B (ack <<N bits)
  - – effective bandwidth is N/(2T+N/B)=B/(1+2TB/N)
  - – good utilisauon ıı N >> 2BT

– or N >> possible number of bits on the line

- Need more frames in transit

7.3.2. DLL in HDLC

HDLC Specifications :

1. **Type of stations**

   Primary station (P): controls the operation of the link (command)

   Secondary station (S): operates under the control of the P (response)

   Combined station (C): combines the features of P and S (response, command)

2. **Link configurations**

   Unbalanced configuration

   - P-to-P, Multipoint/Multidrop (1 master connected with many slaves)

   - one P and one or more S

   - full-duplex, half-duplex

   Balanced configuration

   - P-to-P

   - two C (combined station)

   - full-duplex, half-duplex

3. **Data transfer modes**

   Normal Responsed Mode (NRM)

   - unbalanced configuration

   - P may initiate data transfer to a S

   - S may only transmit data in response to a poll from the P multidrop line, point-to-point

   Asynchronous Balanced Mode (ABM)

   - balanced configuration

   - either C may initiate t on without permission from the other

   - full-duplex P-to-P

   Asynchronous Response Mode (ARM)

   - unbalanced configuration

   - S may initiate transmission without explicit permission of the P

   - P retains responsibility for the line, initialization, error recovery, and logical disconnection

4. **Classes of frames**

   Unnumbered frames

   - Link setup and disconnection

   - Unnumbered: no ACK info (no sequence #s)

   -Set SNRM/SARM/SABM: set logical link between primary and secondary and inform secondary of the mode of operation

   -UA: ACK to other frames in this class

   - DISC: Primary clears logical link

   Information frames (I-frame)

- Carry information / data

- May carry ACK info piggybacked (ABM, ARM)

Supervisory frames

- Error and flow control

- Contain send / receive sequence numbers

- RR (Receiver Ready) and RNR (Receiver Not Ready)

- Used in NRM and ABM

- Secondary willing/unwilling to accept I-frame

- Secondary ACK

- REJ (Reject) and SREJ (Selective Reject)

-Used in ABM

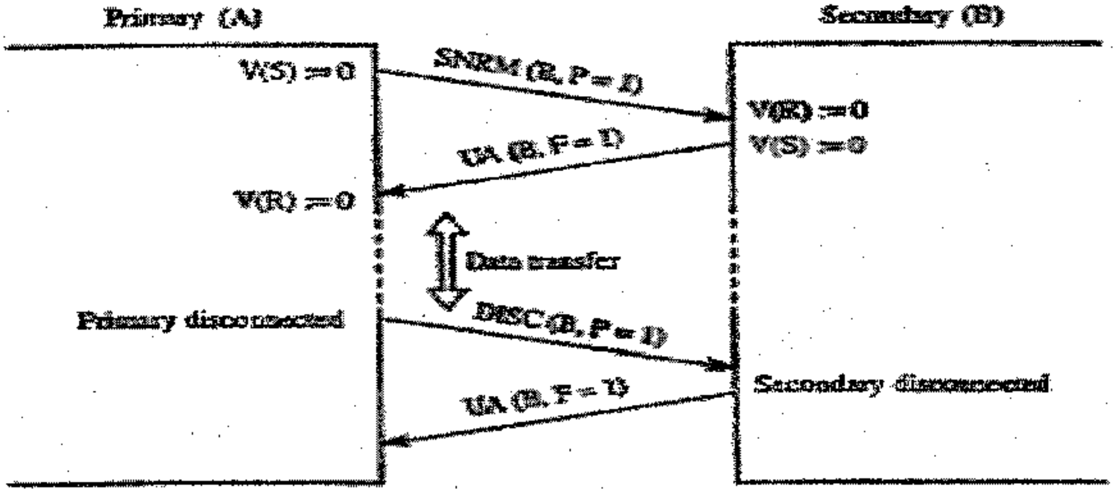
- Indicate out of sequence I-frame received

- Rej: Go Back N, SREJ: Selective Repeat

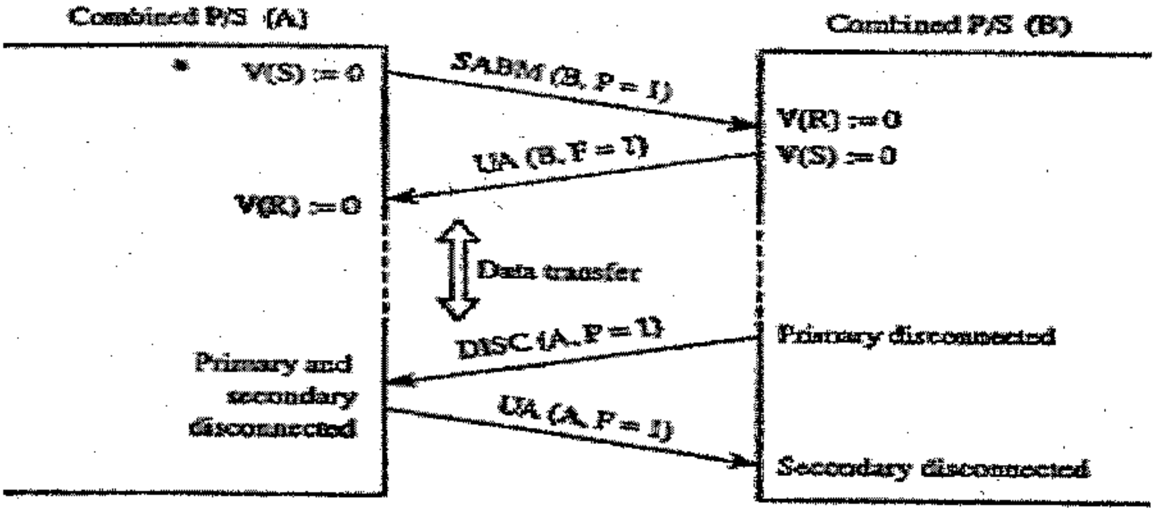
Link Management

-Exchange of unnumbered frames to setup/take down logical connection and Ack

- NRM: Multidrop link



ABM : Point-to-Point



7.4 INTERNET & ATM

What is ATM?

Asynchronous Transfer Mode (ATM) is a technology designed for the high-speed transfer of voice, video, and data through public and private networks using cell relay technology. ATM is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard. Ongoing work on ATM standards is being done primarily by the ATM Forum, which was jointly founded by Cisco Systems, NET/ADAPTIVE, Northern Telecom, and Sprint in 1991. A cell switching and multiplexing technology, ATM combines the benefits of circuit switching (constant transmission delay, guaranteed capacity) with those of packet switching (flexibility, efficiency for intermittent traffic). To achieve these benefits, ATM uses the following features:

- Fixed-size cells, permitting more efficient switching in hardware than is possible with variable-length packets
- Connection-oriented service, permitting routing of cells through the ATM network over virtual connections using simple connection identifiers
- Asynchronous multiplexing, permitting efficient use of bandwidth and interleaving of data of varying priority and size The principal characteristics of ATM are as follows:
  - ?The ATM standard defines a full suite of communication protocols, from an application-level API all the way down through the physical layer.
  - ?The ATM service models include constant bit rate (CBR) service, variable bit rate (VBR) service, available bit rate (ABR) service, and unspecified bit rate (UBR) service.
  - ?ATM uses packet switching with fixed-length packets of 53 bytes. In ATM jargon, these packets are called **cells.** Each cell has five bytes of header and 48 bytes of "payload." The fixed-length cells and simple headers have facilitated highspeed switching.
  - ?ATM uses virtual circuits. In ATM jargon, virtual circuits are called **virtual channels.** The ATM header includes a field for the virtual channel number, which is called the **virtual channel identifier (VCI)** in ATM jargon. Packet switches use the VCI to forward cells toward their destinations.
  - ?ATM provides no retransmissions on a link-by-link basis. If a switch detects an error in an ATM cell header, it attempts to correct the error using error-correcting codes. If it cannot correct the error, it drops the cell rather than request a retransmission from the preceding switch.
  - ?ATM provides congestion control only within the ATM ABR service class. ATM switches themselves do provide feedback to a sending end system to help it regulate its transmission rate in times of network congestion.
  - ?ATM can run over just about any physical layer. It often runs over fiber optics using the SONET standard at speeds of 155.52 Mbps, 622 Mbps, and higher. The ATM protocol stack consists of three layers: the ATM physical layer, the ATM layer, and the ATM adaptation layer (AAL):
  - ?The **ATM physical layer** deals with voltages, bit timings, and framing on the physical medium.
  - ?The **ATM layer** is the core of the ATM standard. It defines the structure of the ATM cell.
  - ?The **ATM adaptation layer** (AAL) is roughly analogous to the transport layer in the Internet protocol stack. ATM includes several different types of AALs to support different types of services.

Currently, ATM is most commonly used as a link-layer technology within localized regions of the Internet. A special AAL type, AAL5, has been developed to allow TCP/IP to interface with ATM. At the IP-to-

ATM interface, AAL5 prepares IP datagrams for ATM transport; at the ATM-to-IP interface, AAL5 reassembles ATM cells into IP datagrams. Figure 7.4 shows the protocol stack for the regions of the Internet that use ATM. Note that in this configuration, the three ATM layers have been squeezed into the lower two layers of the Internet protocol stack. In particular, the Internet's network layer views ATM as a link-layer protocol. A nice tutorial on ATM, reflecting its original goals, is given in [LeBoudec 1992].

Application layer (HTTP, FTP, SMTP, etc.)
Transport layer (TCP, UDP)
Network layer(IP)
AAL5
ATM layer
ATM physical layer

Internet-over-ATM protocol stack

7.5 MULTIPLE ACCESS PROTOCOLS

At the highest level of the classification we distinguish between conflict-free and contention protocols. **Conflict-free protocols** are those ensuring a transmission, whenever made, is a successful one, that is, will not be interfered by another transmission. **Contention transmission** occurs when single shared broadcast channel is used by multiple users. For broadcast networks, data link layer is divided into medium access control and logical link control sublayers: LLC deals with point-to-point connection issues, and MAC deals with how to access shared medium.

At next level there are three broad classes:

Channel Partitioning : the method is to divide channel into smaller "pieces" (time slots, frequency, code) allocate piece to node for exclusive use

Random Access : here channel not divided, allow collisions "recover" from collisions

Taking turns : In this technique Nodes take turns, but nodes with more to send can take longer turns

Conflict-free transmission can be achieved by allocating the channel to the users either statically or dynamically. The channel resources can be viewed, for this purpose, from a time, frequency, or mixed time-frequency standpoint. Hence, the channel can be divided by giving the entire frequency range (bandwidth) to a single user for a fraction of the time as done in Time Division Multiple Access (TDMA), or giving a fraction of the frequency range to every user all of the time as done in Frequency Division Multiple Access (FDMA), or providing every user a portion of the bandwidth for a fraction of the time as done in spreadspectrum based systems such as Code Division Multiple Access (CDMA). Contention schemes differ in principle from conflict-free schemes since a transmitting user is not guaranteed to be successful. The protocol must prescribe a way to resolve conflicts once they occur so all messages are eventually transmitted successfully. The resolution process does consume resources and is one of the major differences among the various contention protocols. If the probability of interference is small, such as might be the case with bursty users, taking the chance of having to resolve the interference compensates for the resources that have to be expanded to ensure freedom of conflicts. Moreover, in most conflict-free protocols, idle users do consume a portion of the channel resources; this portion becomes major when the number of potential users in the system is very large to the extent that conflict-free schemes are impractical. In contention schemes idle users do not transmit and thus do not consume any portion of the channel resources. When contention-based multiple access protocols are used, the necessity arises to resolve the conflicts, whenever they occur. As in the conflict-free case, here too, both static and dynamic resolutions exist. Static resolution means that the actual behavior is not influenced by the dynamics of the system. A static resolution can be based, for example, on user ID's or any other fixed priority assignment, meaning that whenever a conflict arises the first user to finally transmit a message will be the one with, say, the smallest ID (this is done in some tree-resolution protocols). A static resolution can also be probabilistic, meaning that the transmission schedule for the interfering users is chosen from a fixed distribution that is independent of the actual number of interfering users, as is done in Alohatype protocols and the various versions of Carrier Sense Multiple Access (CSMA) protocols. Dynamic resolution, namely taking advantage and tracking system changes is also possible in contention-based protocols. For example, resolution can be based on time of arrival giving highest (or lowest) priority to the oldest message in the system. Alternatively resolution can be probabilistic but such that the statistics change dynamically according to the extent of the interference. Estimating the multiplicity of the interfering packets, and the exponential back-off scheme of the Ethernet standard fall into this category.

7.5.1 CHANNEL PARTITIONING PROTOCOLS

Conflict-free protocols are designed to ensure that a transmission, whenever made, is not interfered by any other transmission and is therefore successful. This is achieved by allocating the channel to the users without any overlap between the portions of the channel allocated to different users. An important advantage of conflict-free access protocols is the ability to ensure fairness among users and the ability to control the packet delay—a feature that may be essential in real-time applications. The two most well known protocols in channel partitioning class are the Frequency Division Multiple Access (FDMA) in which a fraction of the frequency bandwidth is allocated to every user all the time, and the Time Division Multiple Access (TDMA) in which the entire bandwidth is used by each user for a fraction of the time. For both the FDMA and the TDMA protocols no overhead, in the form of control messages, is incurred. However, due to the static and fixed assignment, parts of the channel might be idle even though some users have data to transmit. Dynamic channel allocation

protocols attempt to overcome this drawback by changing the channel allocation based on the current demands of the users.

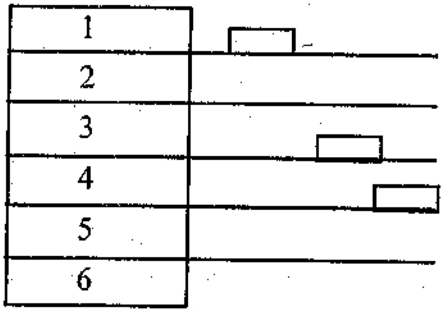
Frequency division multiple access (FDMA)

Characteristics :

channel spectrum divided into frequency bands

each station assigned fixed frequency band

unuse transmission time in frequency bands go idle example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle frequency bands



With Frequency Division Multiple Access (FDMA) the entire available frequency band is divided into bands each of which serves a single user. Every user is therefore equipped with a transmitter for a given, predetermined, frequency band, and a receiver for each band (which can be implemented as a single receiver for the entire range with a bank of bandpass filters for the individual bands). The main advantage of FDMA is its simplicity—it does not require any coordination or

synchronization among the users since each can use its own frequency band without interference. This, however, is also the cause of waste especially when the load is momentarily uneven, since when one user is idle his share of the bandwidth cannot be used by other users. It should be noted that if the users have uneven long term demands, it is possible to divide the frequency range unevenly, i.e., proportional to the demands. FDMA is also not flexible; adding a new user to the network requires equipment modification (such as additional filters) in every other user. For more details the reader may consult any of the many texts treating FDMA that have been published, e.g., by Stallings [Sta85] or the one by Martin [Mar78].

Time division multiple access (TDMA)

Characteristics :

- -access to channel in "rounds"
- - each station gets fixed length slot (length = pkt trans time) in each round unused slots go idle

example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle

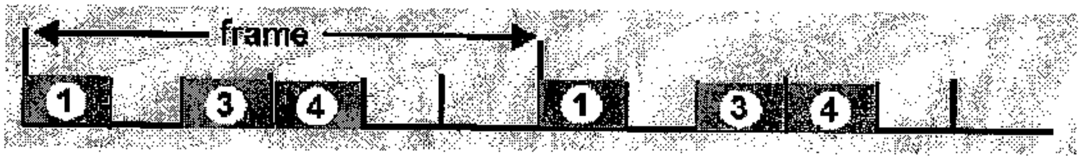


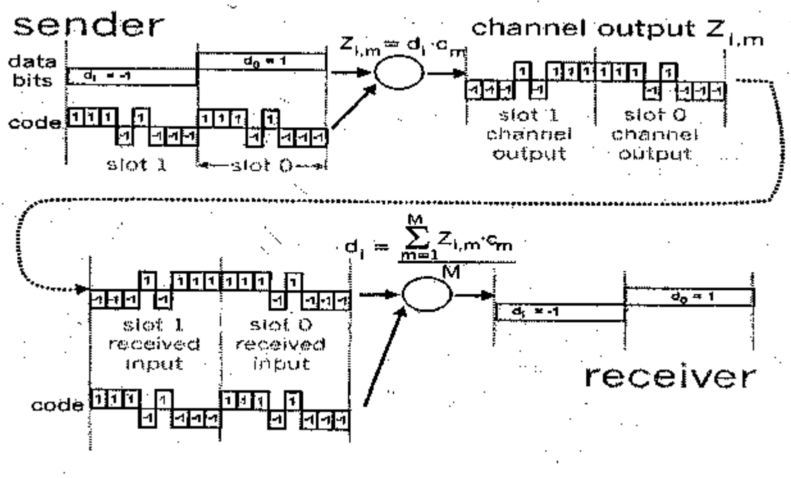
Figure 7.5

In the time division multiple access (TDMA) scheme the time axis is divided into time slots, preassigned to the different users. Every user is allowed to transmit freely during the slot assigned to it, that is, during the assigned slot the entire system resources are devoted to that user. The slot assignments follow a predetermined pattern that repeats itself periodically; each such period is called a *cycle* or a *frame*. In the most basic TDMA scheme every user has exactly one slot in every frame (see Figure 7.5). More general TDMA schemes in which several slots are assigned to one user within a frame, referred to as generalized TDMA. Note that for proper operation of a TDMA scheme, the users must be synchronized so that each one knows exactly when and for how long he can transmit.

Code Division Multiple Access (CDMA)

In this technique unique "code" is assigned to each user; i.e., code set partitioning which is used to encode the original message before transmitting, and decode back at receiving end. This is used mostly in wireless broadcast channels (cellular, satellite, etc. All users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data. Threfore, encoded signal = (original data) X (chipping sequence); decoding: inner-product of encoded signal and chipping

Sequence. This allows multiple users to "coexist" and transmit simultaneously with minimal interference (if the codes are "orthogonal"). There are two classes of signature sequences that are widely used in CDMA systems - Orthogonal Codes, Pseudo Noise Sequences (PN Sequences). Two codes are said to be orthogonal if their correlation is zero, i.e no interference between the two users.



Each user is assigned a unique signature sequence (or code), denoted by (c1,c2,...,cM). Its component is called a chip. Each bit, di, is encoded by multiplying the bit by the signature sequence: $Z_{i,m} = d_i c_m$

For eg. Data bit d1 = –1;

Signature sequence (c1,c2,...,c8) = (+1,+1,+1,–1,+1,–1,–1,–1)

Encoder Output(Z1,1,Z1,2,...,Z1,8) = (–1,–1,–1,+1,–1,+1,+1,+1)

Note that the chip rate is much higher than the data rate. Consider example.

Suppose the original data signal occupies a bandwidth of W. What is the bandwidth of the encoded signal? The bandwidth expands by a factor of M. M is called spreading factor or processing gain

Without interfering users, the receiver would receive the encoded bits, Zi,m , and recover the original data bit, di, by computing:

$$d_i = \frac{1}{M} ?_{m=1}^{M} \quad Z_{i,m}. c_m$$

7.5.2 RANDOM ACCESS PROTOCOLS

When node has packet to send transmit at full channel data rate R. There is no apriori coordination among nodes. When two or more nodes are transmitting simultaneously, then there is "collision". Random access MAC protocol specifies: how to detect collisions, how to recover from collisions (e.g., via delayed retransmissions). Examples of random access MAC protocols: slotted ALOHA, Pure ALOHA, CSMA, CSMA/CD, CSMA/CA

Aloha protocols

The Aloha family of protocols is probably the richest family of multiple access protocols. Its popularity is due first of all to seniority, as it is the first random access technique introduced. Second, many of these protocols are so simple that their implementation is straightforward. Many local area networks of today implement some sophisticated variants of this family's protocols. With the conflict-free protocols that were discussed in Chapter 2, every scheduled transmission is guaranteed to succeed. The Aloha family of protocols belongs to the contention-type or random retransmission protocols in which the success of a transmission is not guaranteed in advance. The reason is that whenever two or more users are transmitting on the shared channel simultaneously, a collision occurs and the data cannot be received correctly. This being the case, packets may have to be transmitted and retransmitted until eventually they are correctly received. Transmission scheduling is therefore the focal concern of contention-type protocols.

Because of the great popularity of Aloha protocols, analyses have been carried out for a very large number of variations. The variations present different protocols for transmission and retransmission schedules as well as adaptation to different circumstances and channel features.

PURE (Unslotted) ALOHA

The *pure Aloha* protocol is *the* basic protocol in the family of the Aloha protocols. It considers a single-hop system with an infinite population generating packets of equal length *T* according to a Poisson process with rate ??packets/sec. The most simpler technique, no synchronization is required within the stations to start the transmission. When frame first arrives, it is transmitted immediately. The channel is error-free without capture: whenever a transmission of a packet does not interfere with any other packet transmission, the transmitted packet is received correctly while if two or more packet transmissions overlap in time, a collision is caused and none of the colliding packets is received correctly and they have to be retransmitted. Collision probability increases: frame sent at t0 collides with other frames sent in [t0-1,t0+1]

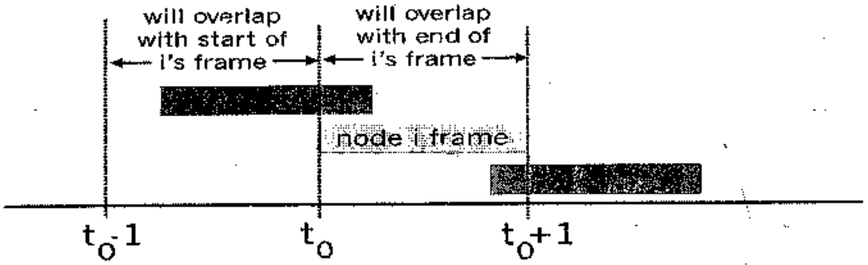

will overlap with start of i's frame
will overlap with end of i's frame
node i frame
$t_o - 1$
t_o
$t_o + 1$

Figure 7.6

The users whose packets collide with one another are called the *colliding users*. At the end of every transmission each user knows whether its transmission was successful or a collision took place. It states that a newly generated packet is transmitted immediately hoping for no interference by others. Should the transmission be unsuccessful, every colliding user, independently of the others, schedules its retransmission to a random time in the future. This randomness is required to ensure that the same set of packets does not continue to collide indefinitely. A simple example of the operation of the protocol is depicted in Figure 7.6. Since the population is infinite each packet can be considered as if it belongs to a different user. Hence, each newly arrived packet can be assigned to an idle user i.e., one that does not have a packet to retransmit. This allows us to interchange the roles of users and packets and consider only the points in time when packet transmission attempts are made. Observing the channel over time we define a point process consisting of scheduling points, i.e., the points in which packets are scheduled for transmission. The scheduling points include both the generation times of new packets and the retransmission times of previously collided packets. Let the rate of the scheduling points be g packets/sec. The parameter g is referred to as the *offered load* to the channel. Clearly, since not all packets are successful on their first attempted transmission, $g>?$. The exact characterization of the scheduling points process is extremely complicated. To overcome this complexity it is assumed that this process is a Poisson process (with rate g, of course). This assumption can, however, be a good approximation at best (as has indeed been shown by simulation). The reason is that a Poisson process implies independence between events in nonoverlapping intervals, which cannot be the case here because of the

dependence between the interval containing the original transmission and the interval containing a retransmission of the same packet. It can be shown, however, that if the retransmission schedule is chosen uniformly from an arbitrarily large interval then the number of scheduling points in any interval approaches a Poisson distribution. The Poisson assumption is used because it makes the analysis of Aloha-type systems tractable and predicts successfully their maximal throughput.

Pure Aloha is a single-hop system. Hence, the throughput is the fraction of time the channel carries useful information, namely noncolliding packets. The channel capacity is the highest value of arrival rate ??for which the rate of departure (throughput) equals the total arrival rate. Consider a packet (new or old) scheduled for transmission at some time t. This packet will be successful if no other packet is scheduled for transmission in the interval $(t-T,t+T)$ (this period of $2T$ is called the *vulnerable* period). The probability of this happening, that is, the probability of success, is that no packet is scheduled in an interval of length $2T$ and since scheduling is Poisson we have Now, packets are scheduled at a rate of g per second of which only a fraction *Psuc* are successful. Thus, the rate of successfully transmitted packets is *gPsuc*. When a packet is successful the channel carries useful information for a period of T seconds; in any other case it carries no useful information at all. Using the definition that the throughput is the fraction of time that useful information is carried on the channel we get which gives the channel throughput as a function of the offered load. Defining to be the *normalized offered load* to the channel, i.e., the rate (per packet transmission time) packets are transmitted on the channel, which is typical to many Aloha type protocols. At $G=1/2$, S takes on its maximal value of. This value is referred to as the capacity of the pure Aloha channel.

Pure Aloha efficiency

Probability P(success by given node) = P(node transmits) .

Probability P(no other node transmits in [p0-1,p0] .

P(no other node transmits in [p0-1,p0] = p . (1-p)**N-1** . (1-p)**N-1**

= p . (1-p)**2(N-1)**

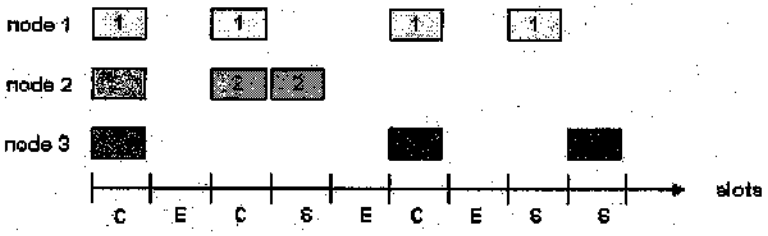
… choosing optimum p and then letting n -> infty ...

= 1/(2e) = .18

SLOTTED ALOHA

The *slotted Aloha* variation of the Aloha protocol is simply that of pure Aloha with a slotted channel. With few Assumptions : (1) all frames same size; (2) time is divided into equal size slots; (3) time to transmit 1 frame nodes start to transmit frames only at beginning of slots, i.e. when node obtains fresh frame, it transmits in next slot

; (4) nodes are synchronized and if 2 or more nodes transmit in a slot, all nodes detect collision. In other words, a slot will be successful if and only if exactly one packet was scheduled for transmission sometime during the previous slot. If collision, node retransmits frame in each subsequent slot with prob. p until success



The slot size equals *T*—the duration of packet transmission. Users are restricted to start transmission of packets only at slot boundaries. Thus, the vulnerable period is reduced to a single slot. The throughput is therefore the fraction of slots (or probability) in which a single packet is scheduled for transmission. Because the process composed of newly generated and retransmitted packets is Poisson we conclude that *S=gTe–gT*

or using the definition of the normalized offered load *G = gT*

S=Ge–G

This relation is very similar to that of pure Aloha, except of increased throughput. Channel capacity is 1 ??*e* ??0.36 and is achieved at *G=1*.

Pros : single active node can continuously transmit at full rate of channel highly decentralized: only slots in nodes need to be in sync, simple

Cons : collisions, wasting slots, idle slots, nodes may be able to detect collision in less than time to transmit packet, clock synchronization

Slotted Aloha efficiency :

Suppose N nodes with many frames to send, each transmits in slot with probability p

prob that node 1 has success in a slot = p(1-p)**N-1**

prob that any node has a success = Np(1-p)**N-1**

For max efficiency with N nodes, find p* that maximizes Np(1-p)**N-1**

For many nodes, take limit of Np*(1-p*)**N-1** as N goes to infinity, gives 1/e = .37

Efficiency is the long-run fraction of successful slots when there are many nodes, each with many frames to send.

At best: channel used for useful transmissions 37% of time!

CSMA(Carrier Sense with multiple access): listen before transmit:

Before sending the frame a station listens the medium, if channel is sensed idle, then station transmits entire packet. If collision occurs station has to retransmit it again. If channel is sensed busy, defer transmission until channel becomes free.

P-Persistent CSMA: (for slotted channels) retry immediately with probability p when channel becomes idle (may cause instability)

Non-persistant CSMA: (for nonslotted channels) retry after random interval human analogy: don't interrupt others!

Collisions can occur as propagation delay means two nodes may not hear each other' transmission and hence collision. A collision means that entire packet transmission time has been wasted, and calls for retransmission until success.

The role of distance and propagation delay is important in determining collision probability

CSMA/CD: This technique is time-sensitive as compared to CSMA. Here collisions detected within short time, hence colliding transmissions are aborted, reducing channel wastage. The collision detection is easy in wired LANs i.e.: measure signal strengths, compare transmitted, received signals; but difficult in wireless LANs: receiver shut off while transmitting. The human analogy compared with this is the polite conversationalist.

Nodes in an Ethernet LAN are interconnected by a broadcast channel, so that when

an adapter transmits a frame, all the adapters on the LAN receive the frame. As we know Ethernet uses a CSMA/CD multiple access algorithm. Summarizing, recall that CSMA/CD employs the following mechanisms:

1. An adapter may begin to transmit at any time; that is, no slots are used.
2. An adapter never transmits a frame when it senses that some other adapter is transmitting; that is, it uses carrier sensing.
3. A transmitting adapter aborts its transmission as soon as it detects that another adapter is also transmitting; that is, it uses collision detection.
4. Before attempting a retransmission, an adapter waits a random time that is typically small compared with the time to transmit a frame.

These mechanisms give CSMA/CD much better performance than slotted ALOHA in a LAN environment. In fact, if the maximum propagation delay between stations is very small, the efficiency of CSMA/CD can approach 100 percent. But note that the second and third mechanisms listed above require each Ethernet adapter to be able to (1) sense when some other adapter is transmitting, and (2) detect a collision while it is transmitting. Ethernet adapters perform these two tasks by measuring voltage levels before and during transmission.

Each adapter runs the CSMA/CD protocol without explicit coordination with

the other adapters on the Ethernet. Within a specific adapter, the CSMA/CD protocol works as follows:

1. The adapter obtains a network-layer PDU from its parent node, prepares an Ethernet frame, and puts the frame in an adapter buffer.
2. If instead the adapter senses that the channel is idle (that is, there is no signal energy from the channel entering the adapter), it starts to transmit the frame. If the adapter senses that the channel is busy, it waits until it senses no signal energy (plus 96 bit times) and then starts to transmit the frame.

3. While transmitting, the adapter monitors for the presence of signal energy coming from other adapters. If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame.
4: If the adapter detects signal energy from other adapters while transmitting, it stops transmitting its frame and instead transmits a 48-bit jam signal.
5. After aborting (that is, transmitting the jam signal), the adapter enters an **exponential backoff** phase. Specifically, when transmitting a given frame, after experiencing the *n*th collision in a row for this frame, the adapter chooses a value for K at random from {0,1,2, . . .,2*m* 2 1} where *m*: 5 min(*n*,10). The adapter then waits K ? 512 bit times and then returns to Step 2. A few comments about the CSMA/CD protocol are certainly in order.

The purpose of the jam signal is to make sure that all other transmitting adapters become aware of the collision. Let's look at an example. Suppose adapter A begins to transmit a frame, and just before A's signal reaches adapter B, adapter B begins to transmit. So B will have transmitted only a few bits when it aborts its transmission. These few bits will indeed propagate to A, but they may not constitute enough energy for A to detect the collision. To make sure that A detects the collision (so that it too can also abort), B transmits the 48-bit jam signal. Next consider the exponential backoff algorithm. The first thing to notice here is that a bit time (that is, the time to transmit a single bit) is very short; for a 10 Mbps Ethernet, a bit time is 0.1 microsecond. Now let's look at an example. Suppose that an adapter attempts for the first time to transmit a frame, and while transmitting it detects a collision. The adapter then chooses K 5 0 with probability 0.5 and chooses K 5 1 with probability 0.5. If the adapter chooses K 5 0, then it immediately jumps to Step 2 after transmitting the jam signal. If the adapter

chooses K 5 1, it waits 51.2 microseconds before returning to Step 2. After a second collision, K is chosen with equal probability from {0,1,2,3}. After three collisions, K is chosen with equal probability from {0,1,2,3,4,5,6,7}. After ten or more collisions, K is chosen with equal probability from {0,1,2, . . .,1023}. Thus the size of the sets from which K is chosen grows exponentially with the number of collisions (until *n* 5 10); it is for this reason that Ethernet's backoff algorithm is referred to as "exponential backoff." The Ethernet standard imposes limits on the distance between any two nodes. These limits ensure that if adapter A chooses a lower value of K than all the other adapters involved in a collision, then adapter A will be able to transmit its frame without experiencing a new collision. We will explore this property in more detail in the homework problems.

We also note here that each time an adapter prepares a new frame for transmission, it runs the CSMA/CD algorithm presented above. In particular, the adapter does not take into account any collisions that may have occurred in the recent past. So it is possible that an adapter with a new frame will immediately be able to sneak in a successful transmission while several other adapters are in the exponential backoff state.

Ethernet Efficiency

When only one node has a frame to send, the node can transmit at the full rate of the Ethernet technology (either 10 Mbps, 100 Mbps, or 1 Gbps). However, if many nodes have frames to transmit, the effective transmission rate of the channel can be much less. We define the **efficiency of Ethernet** to be the long-run fraction of time during which frames are being transmitted on the channel without collisions when there is a large number of active nodes, with each node having a large number of frames to send. In order to present a closed-form approximation of the efficiency of Ethernet, let *tprop* denote the maximum time it takes signal energy to propagate between any two adapters. Let *ttrans* be the time to transmit a maximum-size Ethernet frame (approximately 1.2 msecs for a 10 Mbps Ethernet). A derivation of the efficiency of Ethernet is beyond the scope of this book (see [Lam 1980] and [Bertsekas 1991]). Here we simply state the following approximation:

$$\text{Efficiency} = \frac{1}{1 + 5\,tprop/ttrans}$$

We see from this formula that as *tprop* approaches 0, the efficiency approaches 1. This matches our intuition that if the propagation delay is zero, colliding nodes will abort immediately without wasting the channel. Also, as *ttrans* becomes very large, efficiency approaches 1. This is also intuitive because when a frame grabs the channel, it will hold on to the channel for a very long time; thus the channel will be doing productive work most of the time.

7.6 SUMMARY

Error detection and correction methods are necessary to assure the integrity of the data sent from one location to another. The types of methods used support both asynchronous and synchronous-type data streams. Asynchronous error detection is facilitated by the use of a parity bit with each character of data sent. Error correction for asynchronous data utilizes the LRC/VRC method, which duplicates the parity process (VRC) and examines each character by bit position (LRC). Synchronous data streams apply CRC or checksum for error detection and the Hamming code for error correction.

7.7 GLOSSARY

- HDLC: High-Level Data Link Control
- ADCCP: Advanced Data Communications Control Protocol used by ANSI
- SDLC: Synchronous Data Link Control developed by IBM in 1970 as a replacement for its binary synchronous (BSC) protocol.
- LAP-B: Link Access Protocol – Balanced
- LAP-D: Link Access Procedure D channel

7.8 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. CCNA (Cisco Certified Network Associate) First year Companion Guide - Cisco Press
3. Computer Networks – Andrew Tanenbaum; Prentice Hall India(PHI)

7.9 UNIT END QUESTIONS

1. What are error-detection & correction methods?
2. Give advantages of sliding-window over stop and wait protocol.
3. What is Piggybacking? Give its importance.
4. What is Hamming Code and Hamming distance?
5. What are the major services of Data Link Layer?
6. Give specifications for HDLC.
7. Give advantages and disadvantages for Parity bit.
8. What is the significance of multiple access protocols?
9. What is the difference between CSMA and CSMA/CD?

UNIT - 8
LOCAL AREA NETWORK

Structure of the Unit

8.0 OBJECTIVE

After complete this unit student should be able to understand the following tasks:

- Understand LAN specifications & application areas
- Understand IEEE conventions
- Examine the wireline & wireless networks
- Understand principles of ARP & RARP

8.1 INTRODUCTION

A LAN is a high-speed data network that is usually confined to a limited geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but can often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations. It typically connects workstations, personal computers, printers, servers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

8.2 LAN

LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network

Types of LAN Technology

Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and Local Talk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Applications Areas of LAN :

Asynchronous Transfer Mode (ATM)

ATM is a cell-based fast-packet communication technique that can support data-transfer rates from sub-T1 speeds to 10 Gbps. ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. It relies on the inherent integrity of digital lines to ensure data integrity.

ATM can be integrated into an existing network as needed without having to update the entire network. Its fixed-length cell-relay operation is the signaling technology of the future and offers more predictable performance than variable length frames. Networks are extremely versatile and an ATM network can connect points in a building, or across the country, and still be treated as a single network.

Power over Ethernet (PoE)

PoE is a solution in which an electrical current is run to networking hardware over the Ethernet Category 5 cable or higher. This solution does not require an extra AC power cord at the product location. This minimizes the amount of cable needed as well as eliminates the difficulties and cost of installing extra outlets.

8.3 WIRED AND WIRELESS

The main difference between a wired and wireless data communication infrastructure is the existence of physical cabling. The same, or similar techniques are employed for both types of data communication infrastructure in terms of the core elements of essential network services.The basic difference between a wired and a wireless network is self-explanatory. A wired network uses wires to communicate whereas a wireless network uses radio waves. Let us look at what are the other differences and how one technology gets an edge over the other. Wired networks are easy to set up and troubleshoot where wireless networks are comparatively difficult to set up, maintain, and troubleshoot. Wired networks make you immobile while wireless ones provide you with convenience of movement. Wired networks prove expensive when covering a large area because of the wiring and cabling while wireless networks do not involve this cost. Wired networks have better transmission speeds than wireless ones.In a wired network, a user does not have to share space with other users and thus gets dedicated speeds while in wireless networks, the same connection may be shared by multiple users.One of the most common questions we as consultants have to answer on a daily basis is the difference between wired and wireless networks.

Wired: The communication between two devices via cables.

Wireless: the communication between two devices without cables.

Now, is it that simple Not exactly, each method of networking has its own pros and cons. Wireless networks do not use any form of cable. The transmission of data (your files, music, printing to the printer etc) occurs over radio waves just like cordless phones or the Bluetooth headset that came with that snazzy phone you purchased recently. The major advantage of having a wireless device is the mobility and freedom that comes with it. Moreover, there is less clutter and fewer wires to worry about. But, you sacrifice in most cases on speed and security. Wired networks on the other hand have been around for some time now. Officially known today as the Ethernet, the cables usually connect these devices using CAT5 cables. The speed and security in this scenario are greatly enhanced. The latest Ethernet routers can support up to 1000Mb/s or a gigabit/sec. that's 10 times faster than the widely used 100 Mb/s router. Moreover the over all cost of a wired network is lower, provides high performance and better security than wireless networks.The choice depends on your day to day activities. Wireless networks won't become mainstream anytime soon in office environments. But as home users, wireless networks have become the choice. A little sacrifice in speed or security as a residential user is minimal but for an enterprise environment - well, it becomes a whole new ball game and, pretty detailed too.If a user or a company wants to make a data portable then Wireless networking is the answer. A wireless networking system can avoid the downtime, which may be caused in the wired network. A wireless network is also save your time and efforts in installing the lot of cables.Also, if you need to relocate a client machine in your office, you only need to move the computer with wireless network card.sWireless networking is very useful in the public places, libraries, hotels, schools, airports, railway stations where one might find wireless access to the internet. A drawback in the wireless internet is that quality of service (QOS) is not guaranteed if there is any interference then the connection may be dropped.

WLANS allow users in local area, such as in a university or a library to form a network and gain wireless access to the internet. A temporary network can be formed by a small number of users without the need of access point; given that they do not need to access the resources. Wireline allow the connectivity of multiple networks such as building in a city. The network connectivity is the alternative of copper or fiber cabling. Wired Equivalent Privacy is intended to stop the interference of radio frequency that is signaled by unauthorized users and this security measure is most suitable for the small networks. There is not key management protocol and each key is entered manually into the clients that's why this is very time consuming administrative task. The WEP security method is based on the RC4 encryption algorithm. In the WEP all the client computers and Access points are configured with the same encryption and decryption keys.

Service Set Identifier (SSID) acts a simple password by allowing WLAN network to be split up into different networks and each having a unique identifier. These identifiers are configured in the multiple access points. To access of any networks, a computer is configured in such a way that each is having a corresponding SSID identifier for that network. If the SSID match between the two computers or networks then access is granted to each other.

A list of the MAC addresses of the client computers can be inputted into an Access point and only those computers are granted to give the access to the network. When a computer makes a request, its MAC address is compared to the list of the MAC addresses to the Access point and based on this access permission granted to deny. This is a good security method but it is mainly involved in the small wireless networks because there is more manual work is involved of entering the MAC address into the Access point.

WLANS wireless networking type is very popular in home networking and more than 20 percent homes with broadband internet are using WLANS and this number is increasing. In a general estimate worldwide hotspots have now reached more than 30,000 and will grow about 210,000 in the next few years. Most large hotels already offer Wi-Fi and the business travelers are willing to pay wireless access. 802.11 is the next Wi-Fi speed standard is set to offer bandwidth around 108Mbps and is still under development. With the speed of 70 Mbps and a range up to 30 miles, the 80216 standard, known as WiMAX is sure to get boost.

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

An ad-hoc, or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. Each computer with a wireless interface can communicate directly with all of the others. A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

Types of Wireless Networks

WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet. A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources.

WPANS: Wireless Personal Area Networks

The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling.

WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an ISP.

Understanding the 802.11 family

The 802.11 standard first appeared in the 1990's and was developed by the Institute of Electrical and Electronics Engineers. It has now emerged and expanded to be one of the leading technologies in the wireless world.

802.11 Using either FHSS (frequency hopping spread spectrum) or DSSS (direct sequence spread spectrum) this provides a 1 to 2 Mbps transmission rate on the 2.4GHz band.

- 802.11a Using the OFDM (orthogonal frequency division multiplexing) this provides up to 54Mbps and runs on the 5GHz band.

- 802.11b This is also known as Wi-Fi or High Rate 802.11 uses DSSS and applies to wireless LANs. It is most commonly used for private use, at home. It provides an 11 Mbps transmission rate and has a fallback rate of 5.5, 2 and 1 Mbps.
- 802.11g This provides a 20+ Mbps transmission rate applies to LANs and runs on the 2.4GHz band.

Bluetooth

Bluetooth is a simple type of wireless networking that allows the formation of a small network with up to eight devices being connected at once. Such devices would include PDAs, Laptops, Mobile Phones and Personal Computers. However, Bluetooth may also be found in keyboards, mice, headsets and mobile phone hands-free kits, amongst others. It was originally invented by Ericsson in 1994. In 1998 the Bluetooth SIG (Special Interest Group) was formed by a small number of major companies – Ericsson, Nokia, Intel and Toshiba – to help each other develop and promote the technology. Bluetooth falls under personal area networking since it is has a very short range – 30 to 300 feet. This sort of range adds to the security of such a technology in that if someone wanted to sniff your connection they would not only need special equipment but they would have to be fairly close to you. The main features of Bluetooth are that unlike Infra Red, the signal is not affected by walls it uses radio technology, it is not very expensive, and has little power consumption.

8.4 ARP & RARP

Ethernet Addresses & Resolution

- A data link such as Ethernet or a token ring has its own addressing scheme
- When an Ethernet frame is sent from one host to another, it is the 48-bit Ethernet address that determines the destination
- The first 28-bits are the organization that made the Ethernet card, the second 28-bits are randomly assigned by the manufacturer
- The device driver software never looks at the destination IP address in the IP datagram

Address Resolution Protocol (ARP)

ARP (address resolution protocol) is a protocol used to do address resolution in the TCP/IP protocol suite (RFC826). ARP provides a dynamic mapping from an IP address to the corresponding hardware address.

ARP is required on multi-access channels and relies on the ability to broadcast. Address resolution provides a mapping between two different forms of addresses 32-bit IP addresses and whatever the data link uses, generally MAC address. The protocol is simple – (1) broadcast a packet containing the IP address of the destination machine; (2) the machine with that address, or possibly a server, sends a reply containing the hardware address; (3) upon receipt the hardware address is used to send the original packet

IP is an upper layer protocol to the data link layer. The data link layer of underlying physical network segment over which two communicating computers are directly connected (typically through a hub or a switch) uses its own addressing scheme at

hardware level. In order to send a packet from computer A to B, A needs to know the hardware address of B. This discovery and mapping of IP addresses onto the hardware addresses is done using Address Resolution Protocol (ARP).

ARP Cache

- Essential to the efficient operation of ARP is the maintenance of a cache on each host
- The cache maintains the recent IP to physical address mappings
- Each entry is aged (usually the lifetime is 20 minutes) forcing periodic updates of the cache
- ARP replies are often broadcast so that all hosts can update their caches Proxy ARP
- Proxy ARP lets a router answer ARP requests on one of its networks for a host on another of its networks

- This fools the sender of the ARP request into thinking that the router is the destination
- The router is acting as a proxy agent for the destination, relaying packets to it from other hosts

Reverse Address Resolution Protocol/DHCP

When a system boots, it typically gets its IP address from a file

- How does a system, without a disk, get its IP address?
- Since each system has a unique hardware address, that hardware address can be used to lookup the corresponding IP address
- RARP (RFC903) does exactly that : the RARP request is broadcast and the reply is sent to the requester
- Unlike ARP, designated RARP server(s) that handles RARP requests

Unlike the situation outlined for ARP, the case arises when a computer knows its data link layer address but not its IP address. This is a common scenario in private networks and Digital Subscriber Line (DSL) connections when the IP address of the machines are irrelevant. This is usually the case for work stations but not servers. RARP is an obsoleted method for answering this question: This is my hardware address, what is my IP address? RARP was replaced by BOOTP which, in turn, was replaced by Dynamic Host Configuration Protocol (DHCP). In addition to sending the IP address, DHCP can also send the NTP server, DNS servers, and more.

8.5 ETHERNET TECHNOLOGIES

Background

The term *Ethernet* refers to the family of local area network (LAN) implementations that includes three principal categories.

- Ethernet and IEEE 802.3—LAN specifications that operate at 10 Mbps over coaxial cable.
- 100-Mbps Ethernet—A single LAN specification, also known as Fast Ethernet, that operates at 100 Mbps over twisted-pair cable.
- 1000-Mbps Ethernet—A single LAN specification, also known as Gigabit Ethernet, that operates at 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.

This chapter provides a high-level overview of each technology variant. Ethernet has survived as an essential media technology because of its tremendous flexibility and its relative simplicity to implement and understand. Although other technologies have been touted as likely replacements, network managers have turned to Ethernet and its derivatives as effective solutions for a range of campus implementation requirements. To resolve Ethernet's limitations, innovators (and standards bodies) have created progressively larger Ethernet pipes. Critics might

dismiss Ethernet as a technology that cannot scale, but its underlying transmission scheme continues to be one of the principal means of transporting data for contemporary campus applications. This chapter outlines the various Ethernet technologies that have evolved to date.

Ethernet and IEEE 802.3

Ethernet is a baseband LAN specification invented by Xerox Corporation that operates at 10 Mbps using carrier sense multiple access collision detect (CSMA/CD) to run over coaxial cable. Ethernet was created by Xerox in the 1970s, but the term is now often used to refer to all CSMA/CD LANs. Ethernet was designed to serve in networks with sporadic, occasionally heavy traffic requirements, and the IEEE 802.3 specification was developed in 1980 based on the original Ethernet technology. Ethernet Version 2.0 was jointly developed by Digital Equipment Corporation, Intel Corporation, and Xerox Corporation. It is compatible with IEEE 802.3. Ethernet protocol is implemented either on an interface card or in circuitry on a primary circuit board. Ethernet cabling conventions specify the use of a transceiver to attach a cable to the physical network medium. The transceiver performs many of the physical-layer functions, including collision detection. The transceiver cable connects end stations to a transceiver. IEEE 802.3 provides for a variety of cabling options, one of which is a specification referred to as 10Base5. This specification is the closest to Ethernet. The connecting cable is referred to as an attachment unit interface (AUI), and the network attachment device is called a media attachment unit (MAU), instead of a transceiver.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet : The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Gigabit Ethernet : Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as "gigabit-Ethernet-over-copper" or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

10 Gigabit Ethernet : 10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined. Details are given later in this chapter.

LAN Technology Specifications

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

8.5.1 10Base/100Base

IEEE Naming Convention

10BaseTX/10Broad5

LAN Speed, in Mbps Baseband/Broadband Physical Media Type/Maximum length (in mts.)

Ethernet and IEEE 802.3 Frame Formats

Various frame fields exist for both Ethernet and IEEE 802.3.

Field len in Bytes Ethernet

8	6	6	6	45-1500	4
Preamble	Destination Address	Source Address	Type	Data	FCS

IEEE 802.3.

7	1	6	6	2	46-1500	4
Preamble	SOF	Destination Address	Source Address	Length	802.2 header &Data	FCS

The Ethernet and IEEE 802.3 frame fields illustrated in Figure 8-4 are as follows.

- *Preamble*—The alternating pattern of ones and zeros tells receiving stations that a frame is coming (Ethernet or IEEE 802.3). The Ethernet frame includes an additional byte that is the equivalent of the Start-of-Frame field specified in the IEEE 802.3 frame.
- *Start-of-Frame (SOF)*—The IEEE 802.3 delimiter byte ends with two consecutive 1 bits, which serve to synchronize the frame-reception portions of all stations on the LAN. SOF is explicitly specified in Ethernet.
- *Destination and Source Addresses*—The first 3 bytes of the addresses are specified by the IEEE on a vendor-dependent basis. The last 3 bytes are specified by the Ethernet or IEEE 802.3 vendor. The source address is always a unicast (single-node) address. The destination address can be unicast, multicast (group), or broadcast (all nodes).
- *Type (Ethernet)*—The type specifies the upper-layer protocol to receive the data after Ethernet processing is completed.
- *Length (IEEE 802.3)*—The length indicates the number of bytes of data that follows this field.
- *Data (Ethernet)*—After physical-layer and link-layer processing is complete, the data contained in the frame is sent to an upper-layer protocol, which is identified in the Type field. Although Ethernet Version 2 does not specify any padding (in contrast to IEEE 802.3), Ethernet expects at least 46 bytes of data.
- *Data (IEEE 802.3)*—After physical-layer and link-layer processing is complete, the data is sent to an upper-layer protocol, which must be defined within the data portion of the frame, if at all. If data in the frame is insufficient to fill the frame to its minimum 64-byte size, padding bytes are inserted to ensure at least a 64-byte frame.
- *Frame Check Sequence (FCS)*—This sequence contains a 4-byte cyclic redundancy check (CRC) value, which is created by the sending device and is recalculated by the receiving device to check for damaged frames.

100-Mbps Ethernet

100-Mbps Ethernet is a high-speed LAN technology that offers increased bandwidth to desktop users in the wiring center, as well as to servers and server clusters (sometimes called server farms) in data centers.

The IEEE Higher Speed Ethernet Study Group was formed to assess the feasibility of running Ethernet at speeds of 100 Mbps. The Study Group established several objectives for this new

higher-speed Ethernet but disagreed on the access method. At issue was whether this new faster Ethernet would support CSMA/CD to access the network medium or some other access method. The study group divided into two camps over this access-method disagreement: the Fast Ethernet Alliance and the 100VG-AnyLAN Forum. Each group produced a specification for running Ethernet (and Token Ring for the latter specification) at higher speeds: 100BaseT and 100VG-AnyLAN,

respectively. 100BaseT is the IEEE specification for the 100-Mbps Ethernet implementation over unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cabling. The Media Access Control (MAC) layer is compatible with the IEEE 802.3 MAC layer. Grand Junction, now a part of Cisco Systems Workgroup Business Unit (WBU), developed Fast Ethernet, which was standardized by the IEEE in

the 802.3u specification. 100VG-AnyLAN is an IEEE specification for 100-Mbps Token Ring and Ethernet implementations over 4-pair UTP. The MAC layer is *not* compatible with the IEEE 802.3 MAC layer. 100VG-AnyLAN was developed by Hewlett-Packard (HP) to support newer time-sensitive applications, such as multimedia. A version of HP's implementation is standardized in the IEEE 802.12 specification.

100BaseT Overview

100BaseT uses the existing IEEE 802.3 CSMA/CD specification. As a result, 100BaseT retains the IEEE 802.3 frame format, size, and error-detection mechanism. In addition, it supports all applications and networking software currently running on 802.3 networks. 100BaseT supports dual speeds of 10 and 100 Mbps using 100BaseT fast link pulses (FLPs). 100BaseT hubs must detect dual

speeds much like Token Ring 4/16 hubs, but adapter cards can support 10 Mbps, 100 Mbps, or both. Figure 8-5 illustrates how the 802.3 MAC sublayer and higher layers run unchanged on 100BaseT.

802.3 MAC and higher-layer protocols operate over 100BaseT.

Application software & Upper-Layer Protocols
802.3 MAC Sublayer
100BaseT Physical Layer

100BaseT Signaling

100BaseT supports two signaling types:

- 100BaseX
- 4T

Both signaling types are interoperable at the station and hub levels. The media-independent interface (MII), an AUI-like interface, provides interoperability at the station level. The hub provides interoperability at the hub level. The 100BaseX signaling scheme has a convergence sublayer that adapts the full-duplex continuous

signaling mechanism of the FDDI physical medium dependent (PMD) layer to the half-duplex, start-stop signaling of the Ethernet MAC sublayer. 100BaseTX's use of the existing FDDI specification has allowed quick delivery of products to market. 100BaseX is the signaling scheme used in the 100BaseTX and the 100BaseFX media types.

Components used for a 100BaseT physical connection include the following:

- *Physical Medium*—This device carries signals between computers and can be one of three 100BaseT media types:

  — 100BaseTX

  — 100BaseFX

  — 100BaseT4

- *Medium-Dependent Interface (MDI)*—The MDI is a mechanical and electrical interface between the transmission medium and the physical-layer device.
- *Physical-Layer Device (PHY)*—The PHY provides either 10-or 100-Mbps operation and can be a set of integrated circuits (or a daughter board) on an Ethernet port, or an external device supplied with an MII cable that plugs into an MII port on a 100BaseT device (similar to a 10-Mbps Ethernet transceiver).
- *Media-Independent Interface (MII)*—The MII is used with a 100-Mbps external transceiver to connect a 100-Mbps Ethernet device to any of the three media types. The MII has a 40-pin plug and cable that stretches up to 0.5 meters.

100BaseT Operation 100BaseT and 10BaseT use the same IEEE 802.3 MAC access and collision detection methods, and they also have the same frame format and length requirements. The main difference between 100BaseT and 10BaseT (other than the obvious speed differential) is the network diameter. The 100BaseT maximum network diameter is 205 meters, which is approximately 10 times less than 10-Mbps Ethernet. Reducing the 100BaseT network diameter is necessary because 100BaseT uses the same collision-detection mechanism as 10BaseT.With 10BaseT, distance limitations are defined so that a station knows while transmitting the smallest legal frame size (64 bytes) that a collision has taken place with another sending station that is located at the farthest point of the domain. To achieve the increased throughput of 100BaseT, the size of the collision domain had to shrink. This is because the propagation speed of the medium has not changed, so a station transmitting 10 times faster must have a maximum distance that is 10 times less. As a result, any station knows within the first 64 bytes whether a collision has occurred with any other station.

100BaseT FLPs

100BaseT uses pulses, called FLPs, to check the link integrity between the hub and the 100BaseT device. FLPs are backward-compatible with 10BaseT normal-link pulses (NLPs). But FLPs contain more information than NLPs and are used in the autonegotiation process between a hub and a device on a 100BaseT network.

100BaseT Media Types 100BaseT supports three media types at the OSI physical layer (Layer 1): 100BaseTX, 100BaseFX, and 100BaseT4. The three media types, which all interface with the IEEE 802.3 MAC layer.

100BaseTX

100BaseTX is based on the American National Standards Institutes (ANSI) Twisted Pair-Physical Medium Dependent (TP-PMD) specification. The ANSI TP-PMD supports UTP and STP cabling. 100BaseTX uses the 100BaseX signaling scheme over 2-pair Category 5 UTP or STP.

Table : Characteristics of 100BaseT Media Types

Characteristics	**100BaseTX**	**100BaseFX**	**100BaseT4**
Cable	Category 5 UTP, or type 1& 2 STP	62.5/125 micron multimode fiber	Category 3, 4, or 5 UTP
Number of pairs or Strands	2 pairs	2 strands	4 pairs
Connector	ISO 8877 connector	Duplex Scmedia -interface connector (MIC) ST	ISO 8877 (RJ-45) connector
Maximum segment meters Length	100 meters	400 meters	100
Maximum network meters diameter	200 meters	400 meters	200

The IEEE 802.3u specification for 100BaseTX networks allows a maximum of two repeater (hub) networks and a total network diameter of approximately 200 meters. A link segment, which is defined as a point-to-point connection between two medium Independent Interface (MII) devices, can be up to 100 meters. 100BaseFX 100BaseFX is based on the ANSI TP-PMD X3T9.5 specification for FDDI LANs. 100BaseFX uses the 100BaseX signaling scheme over two-strand multimode fiber-optic (MMF) cable. The IEEE 802.3u specification for 100BaseFX networks allows data terminal equipment (DTE)-to-DTE links of approximately 400 meters, or one repeater network of approximately 300 meters in length.

100BaseT4

100BaseT4 allows 100BaseT to run over existing Category 3 wiring, provided that all four pairs of cabling are installed to the desktop. 100BaseT4 uses the half-duplex 4T+ signaling scheme. The IEEE 802.3u specification for 100BaseT4 networks allows a maximum of two repeater (hub) networks and a total network diameter of approximately 200 meters. A link segment, which is defined as a point-to-point connection between two MII devices, can be up to 100 meters.

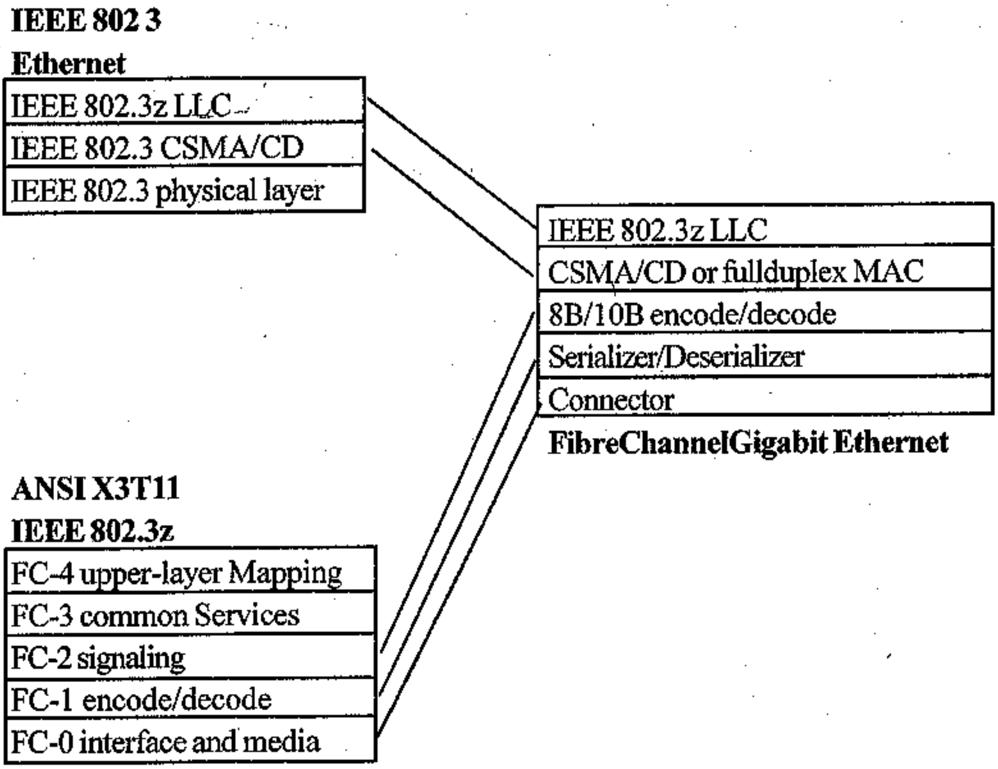
8.5.2 Gigabit Ethernet

Gigabit Ethernet is an extension of the IEEE 802.3 Ethernet standard. Gigabit Ethernet builds on the Ethernet protocol but increases speed tenfold over Fast Ethernet, to 1000 Mbps, or 1 Gbps. This MAC and PHY standard promises to be a dominant player in high-speed LAN backbones and server connectivity. Because Gigabit Ethernet significantly leverages on Ethernet, network managers will be able to leverage their existing knowledge base to manage and maintain Gigabit Ethernet networks.

Gigabit Ethernet Protocol Architecture

To accelerate speeds from 100-Mbps Fast Ethernet to 1 Gbps, several changes need to be made to the physical interface. It has been decided that Gigabit Ethernet will look identical to Ethernet from the data link layer upward. The challenges involved in accelerating to 1 Gbps have been resolved by merging two technologies: IEEE 802.3 Ethernet and ANSI X3T11 Fibre Channel. Figure below shows how key components from each technology have been leveraged to form Gigabit Ethernet.

The Gigabit Ethernet protocol stack was developed from a combination of the Fibre Channel and IEEE 802.3 protocol stacks.



Leveraging these two technologies means that the standard can take advantage of the existing high-speed physical interface technology of Fibre Channel while maintaining the IEEE 802.3 Ethernet frame format, backward compatibility for installed media, and use of full-or half-duplex (via CSMA/CD).

Gigabit Ethernet Campus Applications

The key application of Gigabit Ethernet is expected to be use in the building backbone for interconnection of wiring closets. A Gigabit multilayer switch in the building data center aggregates the building's traffic and provides connection to servers via Gigabit Ethernet or Fast Ethernet. WAN connectivity can be provided by traditional routers or via ATMswitching. Gigabit Ethernet can also be used for connecting buildings on the campus to a central multilayer Gigabit switch located at the campus data center. Servers located at the campus data center are also connected to the Gigabit multilayer switch that provides connectivity to the entire campus. Once again, Gigabit EtherChannel can be utilized to significantly increase the bandwidth available within the campus backbone, to high-end wiring closets, or to high-end routers.

8.6 NETWORKING ESSENTIALS

Hubs / Repeaters	-	Physical layer
Bridges/Switches	-	MAC layer
Routers	-	Network layer

8.6.1 Hubs

Physical Layer: Repeaters

- Distance limitation in local-area networks
  - – Electrical signal becomes weaker as it travels
  - – Imposes a limit on the length of a LAN
- Repeaters join LANs together
  - – Analog electronic device
  - – Continuously monitors electrical signals on each LAN
  - – Transmits an amplified copy

Physical Layer: Hubs

- Joins multiple input lines electrically
  - – Designed to hold multiple line cards
  - – Do not necessarily amplify the signal
- Very similar to repeaters
  - – Also operates at the physical layer

A special type of network device called the **hub** can be found in many home and small business networks. Though they've existed for many years, the hubs are being replaced by bridges/switches.

General Characteristics of Hubs

A hub is a small rectangular box, often made of plastic, that receives its power from an ordinary wall outlet. A hub joins multiple computers (or other network devices) together to form a single network segment.(A **segment** is a specially-configured subset of a larger network. The boundaries of a network segment are established by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters). On this network segment, all computers can communicate directly with each other.

Key Features of Hubs

Hubs classify as Layer 1 devices in the OSI model. At the physical layer, hubs can support little in the way of sophisticated networking. Hubs do not read any of the data passing through them and are not aware of their source or destination. Essentially, a hub simply receives incoming packets, possibly amplifies the electrical signal, and broadcasts these packets out to all devices on the network - including the one that originally sent the packet! Technically speaking, three different types of hubs exist: ?passive, ?active, ?intelligent.

Passive hubs do not amplify the electrical signal of incoming packets before broadcasting them out to the network. **Active hubs**, on the other hand, do perform this amplification, as does a different type of dedicated network device called a repeater. Some people use the terms **concentrator** when referring to a passive hub and **multiport repeater** when referring to an active hub. **Intelligent hubs** add extra features to an active hub that are of particular importance to businesses. An intelligent hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space). It also typically includes remote management capabilities via SNMP(Simple Network Management Protocol (SNMP) provides a standard mechanism to monitor and control network devices.) and virtual LAN (VLAN) support. (VLANs support logical grouping of network nodes to reduce broadcast traffic and allow more control in implementing security policies.)

Limitations of Repeaters and Hubs

- One large shared link
  - –Each bit is sent everywhere
  - –So, aggregate throughput is limited
  - –E.g., three departments each get 10 Mbps independently
  - –... and then connect via a hub and must share 10 Mbps
- Cannot support multiple LAN technologies
  - –Does not buffer or interpret frames
  - –So, can't interconnect between different rates or formats
  - –E.g., 10 Mbps Ethernet and 100 Mbps Ethernet
- Limitations on maximum nodes and distances
  - –Shared medium imposes length limits
  - –E.g., cannot go beyond 2500 meters on Ethernet

8.6.2 Bridges

Link Layer: Bridges

- Connects two or more LANs at the link layer
  - –Extracts destination address from the frame
  - –Looks up the destination in a table
  - –Forwards the frame to the appropriate LAN segment
- Each segment can carry its own traffic

What are Bridges and Switches?

Bridges and switches are data communications devices that operate principally at Layer 2 of the OSI reference model. As such, they are widely referred to as data link layer devices. Bridgesbecame commercially available in the early 1980s. At the time of their introduction, bridges connected and enabled packet forwarding between homogeneous networks. More recently, bridging between different networks has also been defined and standardized. Several kinds of bridging have proven important as internetworking devices. Transparent bridging is found primarily in Ethernet environments, while source-route bridging occurs primarily in Token Ring environments. Translational bridging provides translation between the formats and transit principles of different media types (usually Ethernet and Token Ring). Finally, source-route transparent bridging combines the algorithms of transparent bridging and sourceroute bridging to enable communication in mixed Ethernet/Token Ring environments. Today, switching technology has emerged as the evolutionary heir to bridging-based internetworking solutions. Switching implementations now dominate applications in which bridging technologies were implemented in prior network designs. Superior throughput performance, higher port density, lower per-port cost, and greater flexibility have contributed to the emergence of switches as replacement technology for bridges and as complements to routing technology.

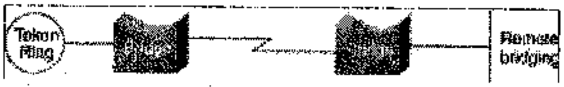
Link Layer Device Overview

Bridging and switching occur at the link layer, which controls data flow, handles transmission errors, provides physical (as opposed to logical) addressing, and manages access to the physical medium. Bridges provide these functions by using various link layer protocols that dictate specific flow control, error handling, addressing, and media-access algorithms. Examples of popular link layer protocols include Ethernet, Token Ring, and FDDI.Bridges and switches are not complicated devices. They analyze incoming frames, make forwarding decisions based on information contained in the frames, and forward the frames toward the destination. In some cases, such as source-route bridging, the entire path to the destination is contained in each frame. In other cases, such as transparent bridging, frames are forwarded one hop at a time toward the destination. Upper-layer protocol transparency is a primary advantage of both bridging and switching. Because both device types operate at the link layer, they are not required to examine upper-layer information. This means that they can rapidly forward traffic representing any network layer protocol. It is not uncommon for a bridge to move AppleTalk, DECnet, TCP/IP, XNS, and other traffic between two or more networks. Bridges are capable of filtering frames based on any Layer 2 fields. For example, a bridge can be programmed to reject (not forward) all frames sourced from a particular network. Because link layer information often includes a reference to an upperlayer protocol, bridges usually can filter on this parameter. Furthermore, filters can be helpful in dealing with unnecessary broadcast and multicast packets. By dividing large networks into self-contained units, bridges and switches provide several advantages. Because only a certain percentage of traffic is forwarded, a bridge or switch diminishes the traffic experienced by devices on all connected segments. The bridge or switch will act as a firewall for some potentially damaging network errors and will accommodate communication between a larger number of devices than would be supported on any single LAN connected to the bridge. Bridges and switches extend the effective length of a LAN, permitting the attachment of distant stations that was not previously permitted. Although bridges and switches share most relevant attributes, several distinctions differentiate these technologies. Bridges are generally used to segment a LAN into a couple of smaller segments. Switches are generally used to segment a large LAN into many smaller segments. Bridges generally have only a few ports for LAN connectivity, whereas switches generally have many. Small switches such as the Cisco Catalyst 2924XL have 24 ports capable of creating 24 different network segments for a LAN. Larger switches such as the Cisco Catalyst 6500 can have hundreds of ports. Switches can also be used to connect LANs with different media-for example, a 10-Mbps Ethernet LAN and a 100-Mbps Ethernet LAN can be connected using a switch. Some switches support cut-through switching, which reduces latency and delays in the network, while bridges support only store-and-forward traffic switching. Finally, switches reduce collisions on network segments because they provide dedicated bandwidth to each network segment.

Types of Bridges

Bridges can be grouped into categories based on various product characteristics. Using one popular classification scheme, bridges are either local or remote. **Local bridges** provide a direct connection between multiple LAN segments in the same area. **Remote bridges** connect multiple LAN segments in different areas, usually over telecommunications lines..

Ethernet
Local bridging

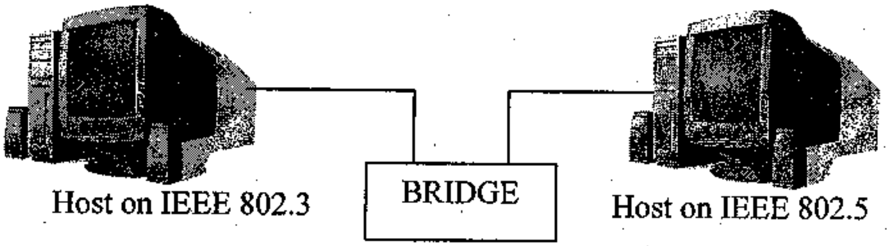


Local and Remote Bridges Connect LAN Segments in Specific Areas

Remote bridging presents several unique internetworking challenges, one of which is the difference between LAN and WAN speeds. Although several fast WAN technologies now are establishing a presence in geographically dispersed internetworks, LAN speeds are often much faster than WAN speeds. Vast differences in LAN and WAN speeds can prevent users from running delay-sensitive LAN applications over the WAN.

Remote bridges cannot improve WAN speeds, but they can compensate for speed discrepancies through a sufficient buffering capability. If a LAN device capable of a 3-Mbpstransmission rate wants to communicate with a device on a remote LAN, the local bridge must regulate the 3-Mbps data stream so that it does not overwhelm the 64-kbps serial link. This is done by storing the incoming data in onboard buffers and sending it over the serial link at a rate that the serial link can accommodate. This buffering can be achieved only for short

bursts of data that do not overwhelm the bridge's buffering capability.The Institute of Electrical and Electronic Engineers (IEEE) differentiates the OSI link layer into two separate sublayers: the Media Access Control (MAC) sublayer and the Logical Link Control (LLC) sublayer. The MAC sublayer permits and orchestrates media access, such as contention and token passing, while the LLC sublayer deals with framing, flow control, error control, and MAC sublayer addressing. Some bridges are MAC-layer bridges, which bridge between homogeneous networks (for example, IEEE 802.3 and IEEE 802.3), while other bridges can translate between different link layer protocols (for example, IEEE 802.3 and IEEE 802.5).



A MAC-Layer Bridge Connects the IEEE 802.3 and IEEE 802.5 Networks

An IEEE 802.3 host (Host A) formulating a packet that contains application information and encapsulating the packet in an IEEE 802.3-compatible frame for transit over the IEEE 802.3 medium to the bridge. At the bridge, the frame is stripped of its IEEE 802.3 header at the MAC sublayer of the link layer and is subsequently passed up to the LLC sublayer for further processing. After this processing, the packet is passed back down to an IEEE 802.5 implementation, which encapsulates the packet in an IEEE 802.5 header for transmission on

the IEEE 802.5 network to the IEEE 802.5 host (Host B). A bridge's translation between networks of different types is never perfect because one network likely will support certain frame fields and protocol functions not supported by the other network.

8.6.3 Switches

- Typically connects individual computers

  – A switch is essentially the same as a bridge

  – … though typically used to connect hosts, not LANs

- Like bridges, support concurrent communication

  – Host A can talk to C, while B talks to D

Types of Switches

Switches are data link layer devices that, like bridges, enable multiple physical LAN segments to be interconnected into a single larger network. Similar to bridges, switches forward and flood traffic based on MAC addresses. Any network device will create some latency. Switches can use different forwarding techniques-two of these are store-and-forward switching and cut-through switching.

In store-and-forward switching, an entire frame must be received before it is forwarded. This means that the latency through the switch is relative to the frame size—the larger the frame size, the longer the delay through the switch. Cutthrough switching allows the switch to begin forwarding the frame when enough of the frame is received to make a forwarding decision. This reduces the latency through the switch. Store-and-forward switching gives the switch the opportunity to evaluate the frame for errors before forwarding it. This capability to not forward frames containing errors is one of the advantages of switches over hubs. Cut-through switching does not offer this advantage, so the switch might forward frames containing errors. Many types of switches exist, including ATM switches, LAN switches, and various types of WAN switches.

APPLICATIONS

ATM Switch

Asynchronous Transfer Mode (ATM) switches provide highspeed switching and scalable bandwidths in the workgroup, the enterprise network backbone, and the wide area. ATM switches support voice, video, and data applications, and are designed to switch fixed-size information units called cells, which are used in ATM communications.

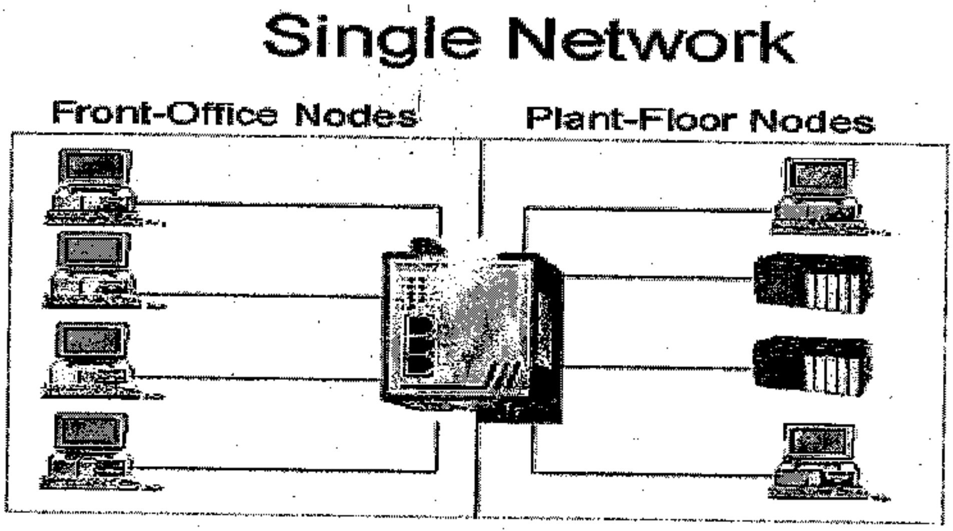
Ethernet, with its easy accessibility in the commercial market and its open, multi-protocol ability, is showing promise as the communication network of choice. As people began to implement Ethernet, however, they realized that network topology and component selection play a major role in the performance and availability of the network. Although Ethernet is an extremely fast and inexpensive communication platform, it is not designed with packet traffic control systems that are inherent in proprietary control networks. Industrial Ethernet users often are concerned that if they connect plant-floor Ethernet nodes on the same shared Ethernet system with their office LAN, they run the chance of having an office event, such as a network back-up, create havoc and reduce the speed of their plant-floor control system. Understanding more about how Ethernet works can help industrial network planners make a more informed decision about the network devices and topologies to implement in their industrial Ethernet networks.

When an Ethernet network node wants to communicate, it first listens to its network connection to determine if there is any traffic currently on the network. If there is no traffic at the instant that the node checks the network, then the Ethernet node will transmit its Ethernet packet. Just like someone picking up a telephone and realizing that the line is in use by someone else in the house, the Ethernet node will delay communication until the network is free of traffic. The Ethernet node that is interested in communicating will check the Ethernet link until the line is free and then transmit when an open line is sensed. In many proprietary networks, traffic is controlled by the passing of a signal between the nodes on the computer that allows each node to transmit only during a controlled window of time. Ethernet has a "wild-west" multiple access architecture, justified in large part by the terrific speed and bandwidth available to the Ethernet network. However, in the multiple access model, two nodes which check the line and see no traffic can simultaneously transmit a packet, creating a collision of the two packets and a failed transmission. The collision of the two packets generates a signal that is recognized by all of the Ethernet devices on the shared network. The collision of the two packets causes all the nodes on the shared network to halt communication and wait a brief period of time before beginning to transmit again. Obviously, as the total amount of network traffic and/or nodes increases, so does the opportunity for collision. An important term to remember is the term "collision domain." A collision domain is simply a collection of devices on a shared Ethernet network, all of which are connected to the same shared, unregulated Ethernet network.

Let's consider a real-world example, illustrating in more common terms the multiple-access principle of Ethernet. Imagine a small business made up of five workers in an office. When the business opens, the owner decides to install a phone on each worker's desk, but only one shared phone line (Multiple Access Collision Domain.) The owner is pleased that he only has to pay for one line, and in the beginning all goes well. In the event that one of the workers in the office wants to dial out, he would pick the phone up to see if any of his coworkers were talking. If they were, the worker would put the receiver down, and try again until the line was free (Carrier Detect.) Occasionally, though, two workers would simultaneously pick up the phone, hear the dial tone, and begin to dial. The simultaneous dialing would cause neither person's phone number to be dialed, and both would put the phone down, wait a while, and try again (Collision Detect.) This is analogous to the Ethernet multiple-access principle. Any node in a collision domain has the ability to check the party line at any time and is not limited as to number of phone calls it can make or when to make a phone call. As additional nodes are placed on the network or the amount of data generated by nodes increases, the network can become

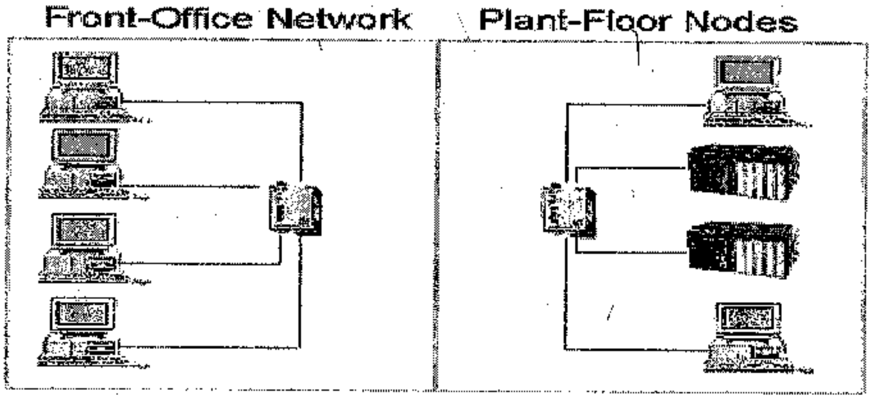
increasingly burdened and slow overall communication rates. Early plant-floor Ethernet networks often attempted to tie plant-floor equipment into the same Ethernet hubs that were handling front-office workstations. A hub is simply a multi-port broadcast device. It takes whatever comes in any port and broadcasts it out all the other ports. Even if two hubs are interconnected, you basically end up with one big collision domain, with all traffic shared. As network nodes are added or traffic increases, every node in the collision domain has a greater chance of slowing communication or having a collision.

Additionally, since Ethernet nodes currently do not differentiate between the relative importance of Ethernet packets, it is possible for non-essential traffic on the network (perhaps people backing-up their computers to the network server or printing a large document across the network) to slow or collide with essential traffic (such as inter-PLC communication, or HMI polling.)



The first solution to this problem was simply to create a separate control network from the office LAN network. By having a separately-wired system, the plant floor could be assured of being immune from office LAN shutdowns or slowdowns. This philosophy becomes a problem when people want to share easily the information that is created in the plant network with office network nodes. If two networks are completely physically isolated, the only way to share information is by making disks and copying files between the two networks—decidedly low tech!

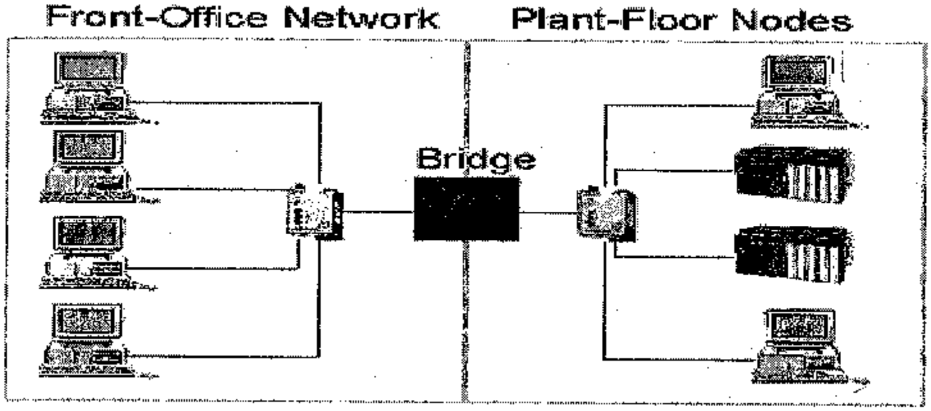
Separate Networks



The next advancement in Industrial network design was the bridge. Bridges act as a "gatekeeper" between two collision domains. By being physically wired into both LANs, this device is able to discern the source and destination address of an Ethernet packet. The bridge is also capable of "mapping" the locations of Ethernet nodes on either side of itself. By linking a control network and an office network with a bridge, you can stop

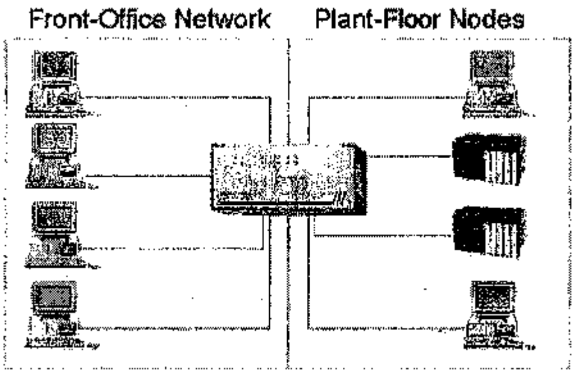
traffic that is meant to travel between two computers in the office LAN from burdening devices on the other side of the bridge. When traffic occurs that is addressed for a device on the other side of the bridge from the originating address, the bridge will allow this traffic to pass. Compared to the completely shared network, the bridged network can reduce, but not eliminate, the opportunity for collisions and network slowdowns.

Bridged Networks



The newest generation of networking equipment, however, combines the multi-connectivity of the hub with the selective routing of Ethernet packets of bridges. A switch is generally a multiport device which has the ability to "read" the address portion of an Ethernet packet and then send the packet out the port on which the destination node resides. Think of a switch as a multiport bridge. Most modern switches have buffers that allow them to store and forward the Ethernet packets that are sent to it. Each port of the switch can connect either directly to a node or to a hub(s) which can also have multiple nodes connected to it. Modern switches also have plug-and-play capability. This means that they are capable of learning the unique addresses of devices attached to them (even if those devices are plugged into a hub which in turn is then attached to the switch) without any programming. If a PC or PLC is plugged directly into a switch, the switch would only allow traffic addressed to that device to be sent down the connection cable to the device. By controlling the flow of information between ports, switches achieve major advantages over current shared environments: When all devices are directly connected into a switch port, the opportunity for collision between ports is eliminated. This assures that packets will arrive with much greater certainty than in a shared environment. Each port has more bandwidth available to it at any time. In a shared environment, any port in the system could consume the entire bandwidth in the network at any point in time. This means that during a peak in traffic, the network availability of any other node is greatly reduced. In a completely port-switched environment, however, the only traffic flowing down the wire between any node and the switch is either traffic destined for, or created by, that particular node.

Port Switched Network



Switches provide Industrial users with many of the safeguards that could only be provided by wiring distinct, proprietary-control networks in the past. The elimination of collisions by connecting every node to a switched port, coupled with the ability to keep control and office traffic from interacting unwontedly, while still using one physical network, allows industrial users to enjoy the open architecture and massive bandwidth and speed of Ethernet without compromising the integrity of their control traffic.

8.7 SUMMARY

Computer networks developed in response to business and government computing needs. Applying standards to network functions provided a set of guidelines for creating network hardware and software and provided compatibility among equipment from different companies. Information could move within a company and from one business to another.

Network devices, such as repeaters, hubs, bridges, switches and routers connect host devices together to allow them to communicate. Protocols provide a set of rules for communication.

The amount of information that can flow through a network connection in a given period of time is referred to as bandwidth. Network bandwidth is typically measured in thousands of bits per second (kbps), millions of bits per second (Mbps), billions of bits per second (Gbps) and trillions of bits per second (Tbps). The theoretical bandwidth of a network is an important consideration in network design. If the theoretical bandwidth of a network connection is known, the formula T=S/BW (transfer time = size of file / bandwidth) can be used to calculate potential data transfer time. However the actual bandwidth, referred to as throughput, is affected by multiple factors such as network devices and topology being used, type of data, number of users, hardware and power conditions.

8.8 GLOSSARY

- ATM – Asynchronous Transfer Mode
- Ethernet – A popular LAN technology
- **Bridge** - Read the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets but only sends packets intended for that segment they are attached to.

Broadband - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction.

- Broadcast - A transmission to all interface cards on the network.
- Brouter - Will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols.
- EMI (electromagnetic interference)- Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
- HMI – Human Machine Interface
- IEEE- Institute of Electrical & Electronics Engineers, a standard body
- Media - The hardware method used to connect computers over a network. The three main types are copper cable, fiber optic cable, and wireless.
- PLC : *power line communications*, plugging a computer device into an existing power outlet would connect the user to the Internet by tapping into already established national and global power grid networks.
- Protocol - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.
- Repeater - Used on a network to regenerate signals to be sent over long distances or tie computers together on a network.
- Router - Routes data packets between two networks. It reads the information in each packet to tell where it is going.
- Thicknet - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8).
- Thinnet - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps.
- Token Ring - A network architecture developed by IBM which sends tokens around a ring of computers to allow media access. Standardized to IEEE 802.5
- Topology - The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
- VPN - Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.

8.9 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. CCNA (Cisco Certified Network Associate)
   First year Companion Guide - Cisco Press
3. Computer Networks – Andrew Tanenbaum; Prentice Hall India(PHI)

8.10 UNIT END QUESTIONS

1. How do a Bridge differ from Switch?.
2. Differentiate between Ethernet and IEEE 802.3.
3. Give significance of ARP and RARP.
4. Differentiate between wireline & wireless networks.
5. What is major advantage of a Switch over a Hub ?
6. What is the IEEE naming convention that is common to different versions of Ethernet.
7. What is the function of Repeater? What is a Hub?
8. Differentiate between Switch and Bridge ?
9. Give details of various IEEE 802.11 versions.
10. List out various Ethernet applications.

UNIT - 9

NETWORK LAYER AND ROUTING

Structure of the Unit

9.0 OBJECTIVE

After complete this unit student should be able to understand the following tasks:

- Identify the role of the Network layer as it describes routing from source to destination
- Examine the most common types of Routing protocols
- Understand principles behind IPv4 and IPv6 addressing mechanism
- Difference between Routed and routing protocol
- Understand Routing protocols metrics

9.1 INTRODUCTION

Routing is the act of moving information across an inter-network from a source to a destination. Along the way, at least one intermediate node typically is encountered. It's also referred to as the process of choosing a path over which to send the packets. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the data link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways. The routing algorithm is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on, i.e. what should be the next intermediate node for the packet.

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A *metric* is a standard of measurement; such as path bandwidth, reliability, delay, current load on that path etc; that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Mainly Destination/Next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular node representing the "next hop" on the way to the final destination. A router has two basic functions: (1) Path determination occurs at the network layer, enables a router to evaluate the paths to a destination (2) Switching function is the internal process used by a router to accept a packet on one interface and forward it to a second interface on the same router.

When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop. Some of the routing algorithm allows a router to have multiple "next hop" for a single destination depending upon best with regard to different metrics.

Desirable properties of a router are as follows:

Correctness and simplicity: The packets are to be correctly delivered. Simpler the routing algorithm, it is better.

Robustness: Ability of the network to deliver packets via some route even in the face of failures.

Stability: The algorithm should converge to equilibrium fast in the face of changing conditions in the network.

Fairness and optimality: obvious requirements, but conflicting.

Efficiency: Minimum overhead While designing a routing protocol it is necessary to take into account the following design parameters:

Performance Criteria: Number of hops, Cost, Delay, Throughput, etc

Decision Time: Per packet basis (Datagram) or per session (Virtual-circuit) basis

Decision Place: Each node (distributed), Central node (centralized), Originated node (source)

Network Information Source: None, Local, Adjacent node, Nodes along route, All nodes

Network Information Update Timing: Continuous, Periodic, Major load change, Topology change

Routing tables contain information used by switching software to select the best route. In this section we will discuss the different nature of information they contain, and the way they determine that one route is preferable to others? Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

Path length

Delay

Bandwidth

Load

Communication cost

Reliability

Path length is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary costs to each network link. In this case, path length is the sum of the costs associated with each link traversed. Other routing protocols define **hop count**, a metric that specifies the number of passes through internetworking products, such as routers, that a packet must pass through in a route from a source to a destination.

Routing delay refers to the length of time required to move a packet from source to destination through the internet. Delay depends on many factors, including the bandwidth of intermediate network links, the port queues (receive and transmit queues that are there in the routers) at each router along the way, network congestion on all intermediate network links, and the physical distance to be traveled. Because delay is a conglomeration of several important variables, it is a common and useful metric.

Bandwidth refers to the available traffic capacity of a link. All other things being equal, a 10-Mbps Ethernet link would be preferable to a 64-kbps leased line. Although bandwidth is a rating of the maximum attainable throughput on a link, routes through links with greater bandwidth do not necessarily provide better routes than routes through slower links. For example, if a faster link is busier, the actual time required to send a packet to the destination could be greater.

Load refers to the degree to which a network resource, such as a router, is busy. Load can be calculated in a variety of ways, including CPU utilization and packets processed per second. Monitoring these parameters on a continual basis can be resource-intensive itself.

Communication cost is another important metric, especially because some companies may not care about performance as much as they care about operating expenditures. Although line delay may be longer, they will send packets over their own lines rather than through the public lines that cost money for usage time.

Reliability, in the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others. After a network fails, certain network links might be repaired more easily or more quickly than other links. Any reliability factor can be taken into account in the assignment of the reliability ratings, which are arbitrary numeric values, usually assigned to network links by network administrators.

9.2 NETWORK SERVICE MODEL

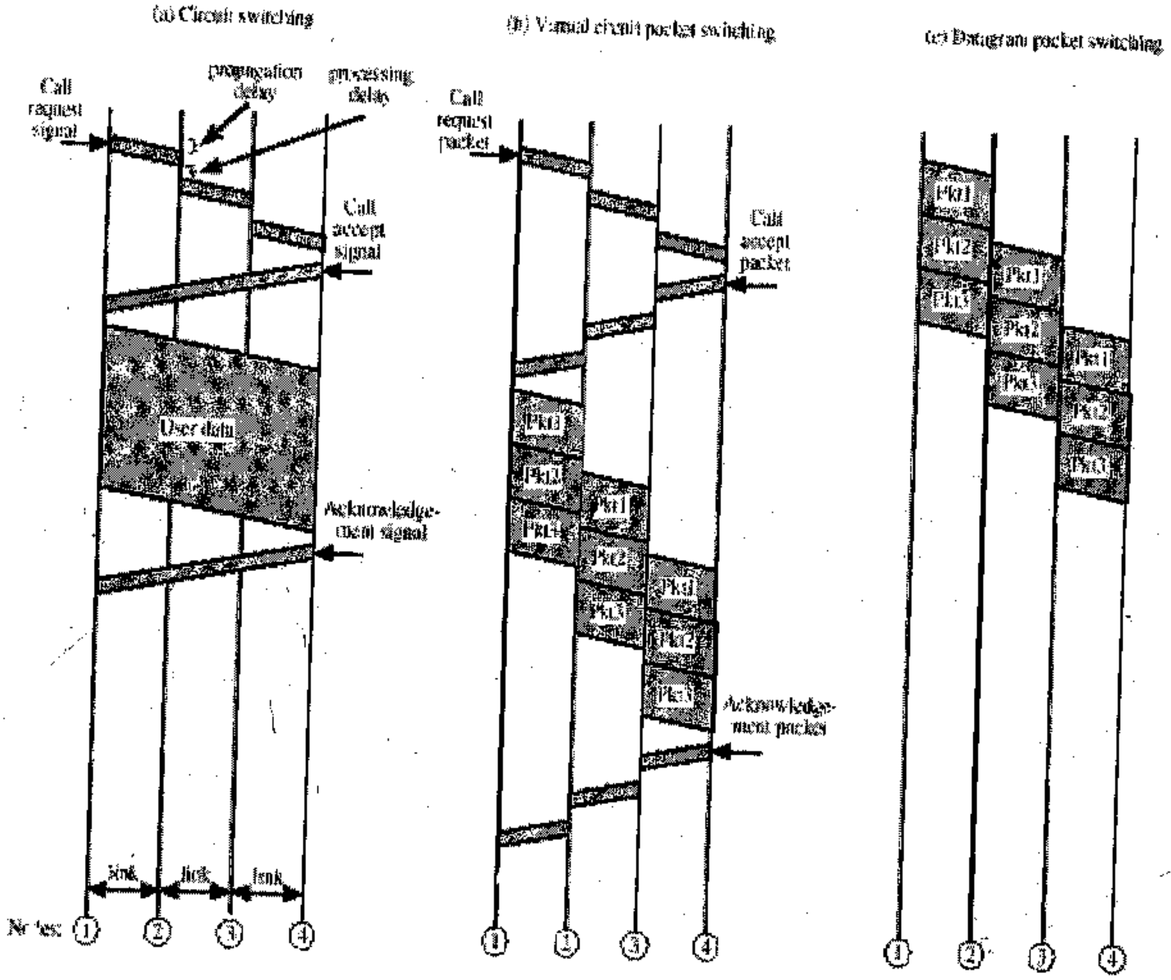
Two major types of service models exist. A **connection oriented service** includes the establishment of a logical connection between 2 processes: (1) establish logical connection (2)transfer data (3) terminate connection. **Connectionless services** involve sending of independent messages.

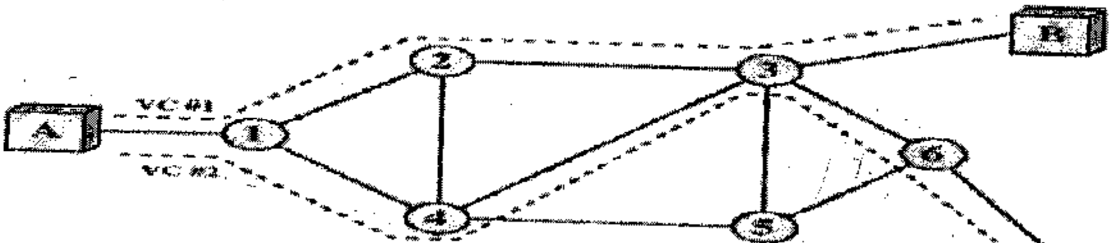
Datagram network is an example of connectionless network.Each datagram packet may be individually routed. Each packet treated independently

- Packets can take any practical route
- Packets may arrive out of order
- Packets may go missing
- Up to receiver to re-order packets and recover from missing packets

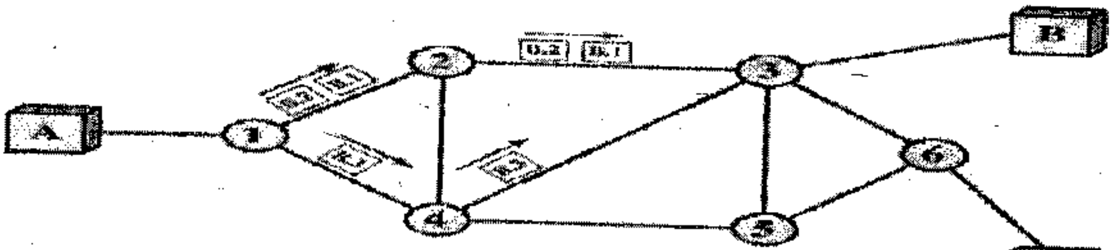
Virtual Circuit network is an example of connection-oriented service. Virtual circuit set up is required. All packets in a virtual circuit follow the same path. Operation is as follows : A preplanned route established before any packets sent by Call request and call accept packets establish connection (handshake); Each packet contains a virtual circuit identifier instead of destination address; No routing decisions required for each packet; clear request to drop circuit; Not a dedicated path.

The below two figures depict the differences.





(a) Internal virtual circuit. A route for packets between two stations is defined and labeled. All packets for that virtual circuit follow the same route and arrive in the same sequence.



(b) Internal datagram. Each packet is treated independently by the network. Packets are labeled with a destination address and may arrive at the destination node out of sequence.

9.3 ROUTING

- Routing algorithms can be classified based on the following criteria:
- Static versus Adaptive
- Single-path versus multi-path
- Intra-domain versus inter-domain
- Flat versus hierarchical
- Link-state versus distance vector
- Host-intelligent versus router-intelligent

Static versus Adaptive

This category is based on how and when the routing tables are set-up and how they can be modified, if at all. Adaptive routing is also referred as **dynamic routing** and Non-adaptive is also known as **static routing** algorithms. *Static routing algorithms* are hardly algorithms at all; the table mappings are established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple. Routing decisions in these algorithms are in no way based on current topology or traffic.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are *dynamic routing algorithms*, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly. Dynamic routing algorithms can be supplemented with static routes where appropriate.

Single-Path versus Multi-path

This division is based upon the number of paths a router stores for a single destination.

Single path algorithms are where only a single path (or rather single next hop) is stored in the routing table. Some sophisticated routing protocols support multiple paths to the same destination; these are known as multi-path algorithms. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability. This is generally called load sharing.

Intradomain versus Interdomain

Some routing algorithms work only within domains; others work within and between domains. The nature of these two algorithm types is different. It stands to reason, therefore, that an optimal intra-domain-routing algorithm would not necessarily be an optimal inter-domain-routing algorithm.

Flat Versus Hierarchical

Some routing algorithms operate in a flat space, while others use routing hierarchies. In a *flat routing system*, the routers are peers of all others. In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from non-backbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more non-backbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas. In *hierarchical systems*, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

Most routing algorithms can be classified into one of two categories: This category is based on the way the routing tables are updated. They are distance vector and link-state routing.

9.3.1 Distance Vector

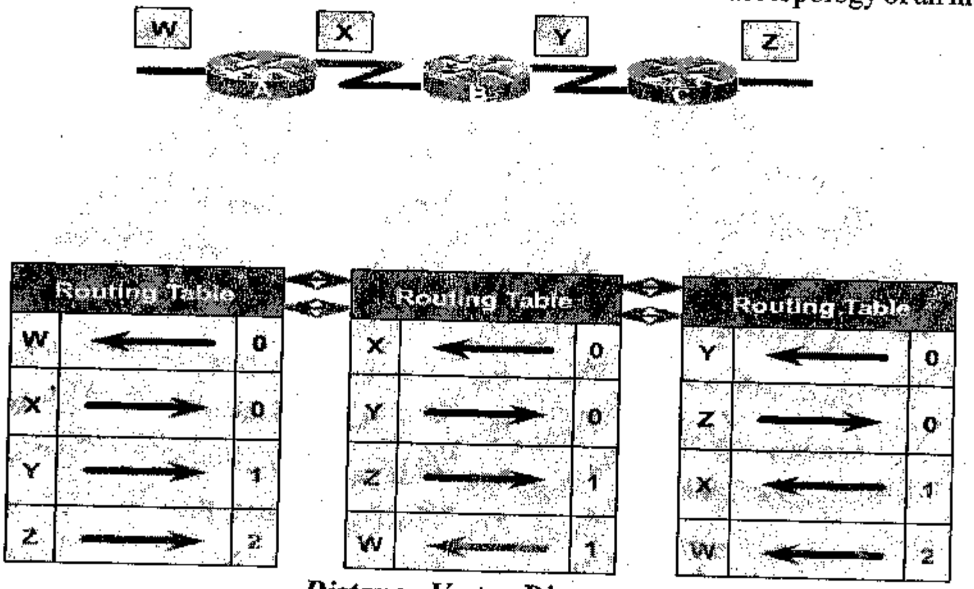
Distance vector algorithms (also known as Bellman-Ford algorithms): Key features of the distance vector routing are as follows:

–The Routers share the knowledge of the entire autonomous system

–Sharing of information takes place only with the neighbors

–Sharing of information takes place at fixed regular intervals, say every 30 seconds”

- Pass periodic routing update (copies of a routing table) from router to router.
- These regular updates between routers communicate topology changes.
- Each router receives a routing table from its directly connected neighbors.
- Distance-vector algorithms do not allow a router to know the exact topology of an internetwork.



Routing Table		
W	←	0
X	→	0
Y	→	1
Z	→	2

Routing Table		
X	←	0
Y	→	0
Z	→	1
W	←	1

Routing Table		
Y	←	0
Z	→	0
X	←	1
W	←	2

Distance Vector Discovery

9.3.2 Link-State Routing

Link-state algorithms (also known as shortest path first algorithms) have the following key feature

The routers share the knowledge only about their neighbors compared to all the routers in the autonomous system

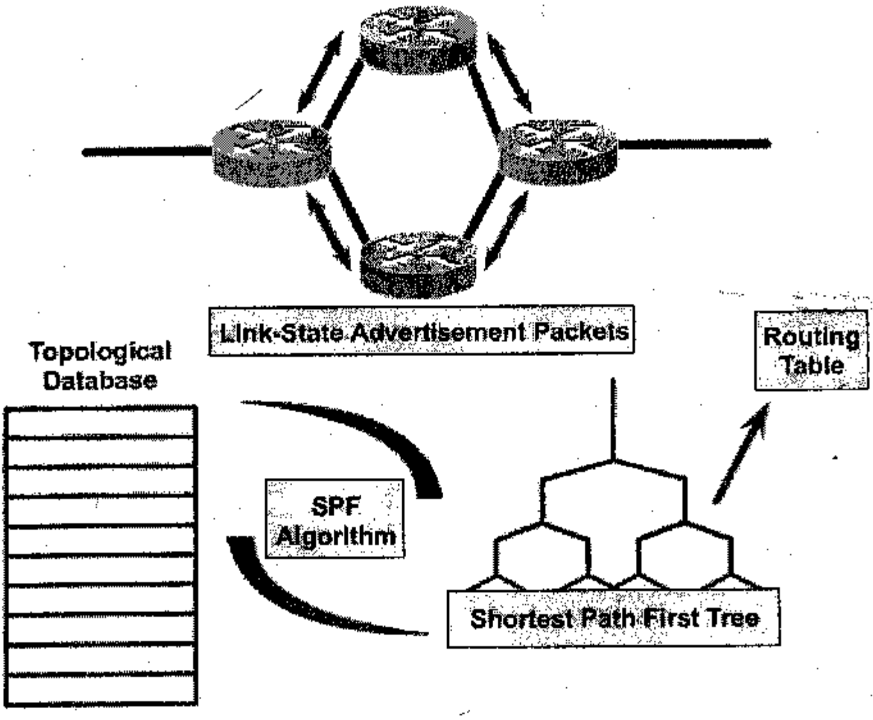
Sharing of information takes place only with all the routers in the internet, by sending small updates using flooding compared to sending larger updates to their neighbors

Sharing of information takes place only when there is a change, which leads to lesser internet traffic compared to distance vector routing

When all routers in an internetwork are operating with the same routing knowledge, the internetwork is said to have converged. During convergence, problems may occur like: routing loops, inconsistent traffic forwarding, inconsistent routing table entries. Fast convergence is desirable because it reduces the period of time in which routers would continue to make incorrect routing decisions

Because convergence takes place more quickly in link-state algorithms, these are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link-state algorithms require more processing power and memory than distance vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Link-state protocols are generally more scalable than distance vector protocols.

- Also known as Dijkstras algorithm or as SPF (shortest path first) algorithms.
- Link-state routing algorithms maintain acomplex database of topology information
- A link-state routing algorithm maintains full knowledge of distant routers and how they interconnect.



9.3.3 Hierarchical

Classless Inter-Domain Routing (CIDR) (RFC1518, RFC1519) that is used today for scalable Internet-wide routing is based on the technique of hierarchical routing. Essential to this technique is the assumption that Network layer addresses assigned to individual entities (e.g., hosts, routers) reflect the position of these entities within the network topology — addresses are said to be "topologically significant". With CIDR addresses assigned to most of the individual sites are expected to reflect providers the sites are connected to. CIDR uses "provider-based" addresses. One of the fundamental consequences of using hierarchical routing is that in order to preserve topological significance of network addresses, changes in the network opology may need to be accompanied by the corresponding changes in the addresses. Presence of multiple RFC 1787 Routing in a multi-provider Internet April 1995 providers serving the same geographical area implies that a subscriber should be able to switch from one provider to another. Since such a switch implies changes in the Internet topology, it follows that to retain topological significance of the (providerbased) addresses within the subscriber, the subscriber has to change the addresses of all of its entities — the process known as "renumbering". There are already tools to facilitate this process — Dynamic Host Configuration Protocol (DHCP). However, DHCP is not yet widely deployed. Further work is needed to improve these tools, get them widely deployed, and to integrate them with Domain Name System (DNS).

Multi-level hierarchical routing allows for recapturing additional routing information (routing entropy) due to the mismatch between addresses and topology at a particular level in the routing hierarchy at some higher level in the hierarchy (e.g., at an exchange point among providers). This enables the routing system to contain the scope of entities impacted by the mismatch. Containing the scope of entities could be an important factor to facilitate graceful renumbering. Further work is needed to develop appropriate deployment strategies to put these capabilities in place. It is important to emphasize that the requirement to maintain topologically significant addresses doesn't need to be applied indiscriminately to all the organizations connected to the Internet — hierarchical routing requires that most, but not all addresses be topologically significant. For a large organization it could be sufficient if the set of destinations within the organization can be represented within the Internet routing system as a small number of address prefixes, even if these address prefixes are independent of the providers that the organization uses to connect to the Internet ("provider-independent" addresses). The volume of routing information that a large organization would inject into the Internet routing system would be comparable to the (aggregated) routing information associated with a large number of small organizations. Existence of multiple providers allows a subscriber to be simultaneously connected to more than one provider (multi-homed subscribers). CIDR offers several alternatives for handling such cases. We need to gain more operational experience as well as better understand tradeoffs associated with the proposed alternatives.

An alternative to CIDR address assignment is to assign addresses based purely on the geographical location. However, address assignment that reflects geographical location of an entity implies that either (a) the Internet topology needs to be made sufficiently congruent to the geography, or (b) addresses aren't going to be topologically significant. In the former case we need to understand RFC 1787 Routing in a multi-provider Internet April 1995 the driving forces that would make the topology congruent to the geography. In the latter case techniques other than hierarchical routing need to be developed.

9.4 IGMP

Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is

an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses. IGMP does allow some attacks, and firewalls commonly allow the user to disable it if it will not be needed.

9.5 IP ADDRESSING

9.5.1 IPv4

Internet Protocol version 4 is the fourth iteration of the InternetProtocol (IP) and it is the first version of the protocol to be widely deployed. IPv4 is the dominant network layer protocol on the Internet and apart from IPv6 it is the only protocol used on the Internet.

It is described in IETF RFC 791 (September 1981) which made obsolete RFC 760 (January 1980). The United States Department of Defense also standardized it as MIL-STD-1777. IPv4 is a data-oriented protocol to be used on a packet switched internetwork (e.g., Ethernet). It is a best effort protocol in that it does not guarantee delivery. It does not make any guarantees on the correctness of the data; It may result in duplicated packets and/or packets out-of-order. These aspects are ddressed by an upper layer protocol (e.g., TCP, and partly by UDP). The entire purpose of IP is to provide unique global computer addressing to ensure that two computers communicating over the Internet can uniquely identify one another.

Addressing

IPv4 uses 32-bit (4-byte) addresses, which limits the address space to 4,294,967,296 possible unique addresses. However, some are reserved for special purposes such as private networks (~18 million addresses) or multicast addresses (~1 million addresses). This reduces the number of addresses that can be allocated as public Internet addresses. As the number of addresses available are consumed, an IPv4 address shortage appears to be inevitable, however Network Address Translation (NAT) has significantly delayed this inevitability. This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment and is currently the only contender to replace IPv4.

Address representations

Allocation

Originally, the IP address was divided into two parts: Network id, Host id. This created an upper limit of 256 networks. As the networks began to be allocated, this was soon seen to be inadequate. To overcome this limit, different classes of network were defined, in a system which later became known as classful networking. Five classes were created (A, B, C, D, & E), three of which (A, B, & C) had different lengths for the network field. The rest of the address field in these three classes was used to identify a host on that network, which meant that each network class had a different maximum number of hosts. Thus there were a few networks with lots of host addresses and numerous networks with only a few addresses. Class D was for multicastaddresses and class E was reserved. Around 1993, these classes were replaced with a Classless Inter-Domain Routing (CIDR) scheme, and the previous scheme was dubbed "classful", by contrast. CIDR's primary advantage is to allow re-division of Class A, B & C networks so that smaller (or larger) blocks of addresses may be allocated to entities (such as Internet service providers, or their customers) or Local Area Networks.

The actual assignment of an address is not arbitrary. The fundamental principle of routing is that address encodes information about a device's location within a network. This implies that an address assigned to one part of a network will not function in another part of the network. A hierarchical structure, created by CIDR and overseen by the Internet Assigned Numbers Authority (IANA) and its Regional Internet Registries (RIRs), manages the assignment of Internet address worldwide. Each RIR maintains a publicly searchable WHOIS database that provides information about IP address assignments; information from these databases plays a central role in numerous tools that attempt to locate IP addresses geographically.

Reserved address blocks	**CIDR address block Description**	**Reference**
0.0.0.0/8	Current network (only valid as source address)	RFC 1700
10.0.0.0/8	Private network	RFC 1918
14.0.0.0/8	Public data networks	RFC 1700
127.0.0.0/8	Loopback	RFC 3330
128.0.0.0/16	Reserved (IANA)	RFC 3330
169.254.0.0/16	Link-Local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
199.255.0.0/16	Reserved (IANA)	RFC 3330
192.0.0.0/24	Reserved (IANA)	RFC 3330
192.0.2.0/24	Documentation and example code	RFC 3330
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
223.255.255.0/24	Reserved (IANA)	RFC 3330
224.0.0.0/4	Multicasts (former Class D network)	RFC 3171
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	

Private networks

Of the 4 billion addresses allowed in IPv4, four ranges of address are reserved for private networking use only. These ranges are not routable outside of private networks, and private machines cannot directly communicate with public networks. They can, however, do so through network address translation.

The following are the four ranges reserved for private networks:

Name	IP address range	number of IPs	*Classful description*	largest CIDR block
24-bit Block	10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.39.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16
16-bit block	169.254.0.0 – 169.254.255.255	65,536	256contiguous class Cs	169.254.0.0/16

Localhost

In addition to private networking, the IP range 127.0.0.0 – 127.255.255.255 (or 127.0.0.0/8 in CIDR notation) is reserved for localhost communication. Any address within this range should never appear on an actual network and any packet sent to this address does not leave the source computer, and will appear as an incoming packet on that computer (known as Loopback).

Exhaustion

A concern that has spanned decades to the 1980s is the exhaustion of available IP addresses. This was the driving factor in classful networks and then later in the creation of CIDR addressing. Today, there are several driving forces to the next address allocation solution:

- Mobile devices — laptop computers, PDAs, mobile phones
- Always-on devices — ADSL modems, cable modems
- Rapidly growing number of internet users

The most visible solution is to migrate to IPv6 since the address size jumps dramatically from 32-bit to 128-bit which would allow about 18 quintillion people their own set of 18 quintillion addresses (3.4e38 total addresses). However, migration has proved to be a challenge in itself, and total Internet adoption of IPv6 is unlikely to occur for many years. Some things that can be done to mitigate the IPv4 address exhaustion are (not mutually exclusive):

- Network address translation (NAT)
- Use of private networks
- Dynamic Host Configuration Protocol (DHCP)
- Named based virtual hosting
- Tighter control by Regional Internet Registries on the allocation of addresses to Local Internet Registries
- Network renumbering to reclaim large blocks of address space allocated in the early days of the Internet

9.5.2 IPv6

Addressing under IPv6 is outlined in the main IPv6 RFC, RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification." However, most of the details of IPv6 addressing are contained in two other standards: RFC 3513, "Internet Protocol Version 6 (IPv6) Addressing Architecture," and RFC 3587, "IPv6 Global Unicast Address Format." These replaced the 1998 standards RFC 2373, "IP Version 6 Addressing Architecture," and RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format."

For brevity, IPv6 addresses are represented using eight sets of four hexadecimal digits, a form called *colon hexadecimal notation*. Additonal technques, called *zero suppresson* and *zero compression*, are used to reduce the size of displayed addresses further by removing unnecessary zeros from the presentation of the address.

IPv6 Addressing Model Characteristics

Here are some of the general characteristics of the IPv6 addressing model that are basically the same as in IPv4:

Core Functions of Addressing The two main functions of addressing are still network interface identification and routing. Routing is facilitated through the structure of addresses on the internetwork.

Network Layer Addressing IPv6 addresses are still the ones associated with the network layer in TCP/IP networks and are distinct from data link layer (also sometimes called physical) addresses.

Number of IP Addresses per Device Addresses are still assigned to network interfaces, so a regular host like a PC will usually have one (unicast) address, and routers will have more than one for each of the physical networks to which it connects.

Address Interpretation and Prefix Representation IPv6 addresses are like classless IPv4 addresses in that they are interpreted as having a network identifier part and a host identifier part (a network ID and a host ID), but that the delineation is not encoded into the address itself. A prefix-length number, using CIDR-like notation, is used to indicate the length of the network ID (prefix length)..

Private and Public Addresses Both types of addresses exist in IPv6, though they are defined and used somewhat differently.

IPv6 Supported Address Types

One important change in the addressing model of IPv6 is the address types supported. IPv4 supported three address types: unicast, multicast, and broadcast. Of these, the vast majority of actual traffic was unicast. IP multicast support was not widely deployed until many years after the Internet was established and it continues to be hampered by various issues. Use of broadcast in IP had to be severely restricted for performance reasons (we don't want any device to be able to broadcast across the entire Internet!).

IPv6 also supports three address types, but with the following changes:

Unicast Addresses These are standard unicast addresses as in IPv4, one per host interface.

Multicast Addresses These are addresses that represent various groups of IP devices. A message sent to a multicast address goes to all devices in the group. IPv6 includes much better multicast features and many more multicast addresses than IPv4. Since multicast under IPv4 was hampered in large part due to lack of support of the feature by many hardware devices, support for multicasting is a required, not optional, part of IPv6.

Anycast Addresses Anycast addressing is used when a message must be sent to any member of a group, but does not need to be sent to all of them. Usually the member of the group that is easiest to reach will be sent the message. One common example of how anycast addressing could be used is in load sharing among a group of routers in an organization.

Broadcast addressing as a distinct addressing method is gone in IPv6. Broadcast functionality is implemented using multicast addressing to groups of devices. A multicast group to which all nodes belong can be used for broadcasting in a network, for example.

An important implication of the creation of anycast addressing is removal of the strict uniqueness requirement for IP addresses. Anycast is accomplished by assigning the same IP address to more than one device. The devices must also be specifically told that they are sharing an anycast address, but the addresses themselves are structurally the same as unicast addresses.

The bulk of the remainder of this chapter focuses on unicast addressing, since it is by far the most important type. Multicast and anycast addressing are given special attention in a separate section later in this chapter.

IPv6 Address Size and Address Space

Of all the changes introduced in IPv6, easily the most celebrated is the increase in the size of IP addresses, which resulted in a corresponding massive increase in the size of the address space as well. It's not surprising that these sizes were increased compared to IPv4—everyone has known for years that the IPv4 address space was too small to support the future of the Internet. What's remarkable is the level of increase and the implications for how Internet addresses are used.

In IPv4, IP addresses are 32 bits long; these are usually grouped into 4 octets of 8 bits each. The theoretical IPv4 address space is 2^{32}, or 4,294,967,296 addresses. To increase this address space, we simply increase the size of addresses; each extra bit we give to the address size doubles the address space. Based on this, some folks expected the IPv6 address size to increase from 32 to 48 bits, or perhaps 64 bits. Either of these numbers would have given a rather large number of addresses.

However, IPv6 addressing doesn't use either of these figures. Instead, the IP address size jumps all the way to 128 bits, or 16 8-bit octets/bytes. The size of the IPv6 address space is, quite literally, astronomical. Like the numbers that describe the number of stars in a galaxy or the distance to the furthest pulsars, the number of addresses that can be supported in IPv6 is mind-boggling.

Since IPv6 addresses are 128 bits long, the theoretical address space, if all addresses were used, is 2^{128} addresses. This number, when expanded out, is 340,282,366,920,938, 463,463,374,607,431,768,211,456, which is normally expressed in scientific notation as about $3.4*10^{38}$ addresses. Whoa! That's about 340 trillion, *trillion, trillion* addresses. As I said, it's pretty hard to grasp just how large this number is. Consider these comparisons:

NOTE:

- It's enough addresses for many trillions of addresses to be assigned to every human being on the planet.
- The Earth is about 4.5 billion years old. If you had been assigning IPv6 addresses at a rate of 1 billion per second since the Earth was formed, you would have by now used up less than one trillionth of the address space.
- The Earth's surface area is about 510 trillion square meters. If a typical computer has a footprint of about one-tenth of a square meter, you would have to stack computers 10 billion high—blanketing the entire surface of the Earth—to use up that same trillionth of the address space.

OK, I think you get the idea. It's clear that one goal of the decision to go to 128-bit addresses is to make sure that we will never run out of address space again, and it seems quite likely that this will be the case.

There are drawbacks to having such a huge address space, too. Consider that even with a 64-bit address, we would have a very large address space; 264 equals 18,446,744,073,709,551,616, or about 18 million trillion. These are still probably more addresses than the Internet will ever need. However, by going to 128 bits instead, this has made dealing with IP addresses unruly (as you'll see in the next section). This has also increased overhead, since every datagram header or other place where IP addresses are referenced must use 16 bytes for each address instead of the 4 bytes that were needed in IPv4, or the 8 bytes that might have been required with a 64-bit address.

So why the overkill of going to 128 bits? The main reason is *flexibility*. Even though you can have a couple zillion addresses if we allocate them one at a time, this makes assignment difficult. The developers got rid of class-oriented addressing in IPv4 because it wasted address space. The reality, though, is that being able to waste address space is a useful luxury.

Having 128 bits allows us to divide the address space and assign various purposes to different bit ranges, while still not having to worry about running out of space. Later in this chapter, in the section describing the IPv6 global unicast address format, you'll see one way that those 128 bits are put to good use: They allow you to create a hierarchy of networks while still saving 64 bits for host IDs. This hierarchy has its own advantages.

IPv6 ADDRESS AND ADDRESS NOTATION AND PREFIX REPRESENTATION

Increasing the size of IP addresses from 32 bits to 128 bits expands the address space to a gargantuan size, thereby ensuring that we will never again run out of IP addresses, and thereby allowing flexibility in how they are assigned and used. Unfortunately, there are some drawbacks to this method, and one of them is that 128-bit numbers are very large. The size makes them awkward and difficult to use.

Computers work in binary, and they have no problem dealing with long strings of ones and zeros, but humans find them confusing. Even the 32-bit addresses of IPv4 are cumbersome for us to deal with, which is why we use dotted decimal notation for them unless we need to work in binary (as with subnetting). However, IPv6 addresses are so much larger than IPv4 addresses that it becomes problematic to use dotted decimal notation. To use this notation, we would split the 128 bits into 16 octets and represent each with a decimal number from 0 to 255. However, we would end up not with 4 of these numbers, but 16. A typical IPv6 address in this notation would appear as follows: 128.99.45.157.220.40.0.0.0.0.252.87.212.200.39.255

IPv6 Address Hexadecimal Notation

To make addresses shorter, the decision was made in IPv6 to change the primary method of expressing addresses to use hexadecimal instead of decimal. The advantage of this is that it requires fewer characters to represent an address, and converting from hexadecimal to binary and back again is much easier than converting from binary to decimal or vice versa. The disadvantage is that many people find hexadecimal difficult to comprehend and work with, especially because the notion of 16 values in each digit is a bit strange.

The hexadecimal notation used for IPv6 addresses is similar to the same method used for IEEE 802 MAC addresses, and for technologies like Ethernet. With these MAC addresses, 48 bits are represented by 6 octets, each octet being a hexadecimal number from 0 to FF, separated by a dash or colon, like this: 0A-A7-94-07-CB-D0

Since IPv6 addresses are larger, they are instead grouped into eight 16-bit words, separated by colons, to create what is sometimes called colon hexadecimal notation. So, the IPv6 address given in the previous example would be expressed as follows:

805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF

To keep the address size down, leading zeros can be suppressed in the notation so you can immediately reduce this to the following:

805B:2D9D:DC28:0:0:FC57:D4C8:1FFF

Well, it's definitely shorter than dotted decimal, but still pretty long. When you are dealing with numbers this big, there's only so much you can do. This is part of why the use of Domain Name System (DNS) names for hosts becomes much more important under IPv6 than it is in IPv4: Who could remember a hex address that long?

Zero Compression in IPv6 Addresses

Fortunately, there is a shortcut that can be applied to shorten some addresses even further. This technique is sometimes called zero compression. The method allows a single string of contiguous zeros in an IPv6 address to be replaced by double colons. So, for example, the previous address could be expressed as follows:

805B:2D9D:DC28::FC57:D4C8:1FFF

You know how many zeros are replaced by the two colons (::) because you can see how many fully expressed (uncompressed) hexadecimal words are in the address. In this case, there are six, so the :: represents two zero words. To prevent ambiguity, the double colons can appear only once in any IP address, because if it appeared more than once, you could not tell how many zeros were replaced in each instance. So, if the example address were 805B:2D9D:DC28:0:0:FC57:0:0, you could replace either the first pair of zeros or the second, but not both.

Zero compression doesn't make the example much shorter, but due to how IPv6 addresses are structured, long strings of zeros are common. For example, consider this address:

FF00:4501:0:0:0:0:0:32

With compression, this could be shortened as follows: FF00:4501::32

The technique works even better on special addresses. The full IPv6 loopback address is written as follows: 0:0:0:0:0:0:0:1

With compression, the loopback address looks like this: ::1

For even more fun, consider the especially odd IPv6 unspecified address, as shown here:

0:0:0:0:0:0:0:0

Apply zero compression to an address that is all zeros, and what do you get? Ans ::

No numbers at all! Of course, thinking of :: as an address does take some getting used to.

IPv6 Mixed Notation

There is also an alternative notation used in some cases, especially for expressing IPv6 addresses that embed IPv4 addresses (discussed later in this chapter). For these, it is useful to show the IPv4 portion of the address in the older dotted decimal notation, since that's what you use for IPv4. Since embedding uses the last 32 bits for the IPv4 address, the notation has the first 96 bits in colon hexadecimal notation and the last 32 bits in dotted decimal. So, to take the earlier example again, in mixed notation it would be shown as follows:

805B:2D9D:DC28::FC57:212.200.39.255

This isn't really a great example of mixed notation, because embedding usually involves long strings of zeros followed by the IPv4 address. Thus, zero compression comes in very handy here. Instead of seeing something like this:

0:0:0:0:0:0:212.200.39.255

You will typically see this:

::212.200.39.255

At first glance, this appears to be an IPv4 address. You must keep a close eye on those colons in IPv6!

IPv6 Address Prefix Length Representation

Like IPv4 classless addresses, IPv6 addresses are fundamentally divided into a number of network ID bits followed by a number of host ID bits. The network identifier is called the prefix, and the number of bits used is the *prefix length*. This prefix is represented by adding a slash after the address and then putting the prefix length after the slash. This is the same method used for classless IPv4 addressing with CIDR. For example, if the first 48 bits of the sample address were the network ID (prefix), then we would express this as 805B:2D9D:DC28::FC57:D4C8:1FFF/48.

Note: IPv6, the size of an address's prefix is indcated by the prefix length that follows the address, separated wth a slash, just as it is done in IPv4 classless addressing.

As in IPv4, specifiers for whole networks will typically end in long strings of zeros. These can be replaced by double colons (::) using zero compression. For example, the 48-bit network ID for the previous example is 805B:2D9D:DC28:0:0:0:0:0/48, or 805B:2D9D:DC28::/48. You must include the "::" if replacing the trailing zeros.

IPv6 ADDRESS SPACE ALLOCATION

After dealing for so many years with the very small IPv4 address space, the enormous number of addresses in IPv6 must have made the Internet Engineering Task Force (IETF) engineers feel like kids in a candy shop. They were good kids, however, and didn't run wild, grabbing all the candy they could find and gobbling it up. They very carefully considered how to divide the address space for various uses. Of course, when you have this much candy, sharing becomes pretty easy.

As was the case with IPv4, the two primary concerns in deciding how to divide the IPv6 address space were address assignment and routing. The designers of IPv6 wanted to structure the address space to make allocation of addresses to Internet service providers (ISPs), organizations, and individuals as easy as possible.

At first, perhaps ironically, this led the creators of IPv6 back full circle to the use of specific bit sequences to identify different types of addresses, just like the old classful addressing scheme. The address type was indicated by a set of bits at the start of the address, called the format prefix (FP). The format prefix was conceptually identical to the one to four bits used in IPv4 classful addressing to denote address classes, but was variable in length, ranging from three to ten bits. Format prefixes were described in RFC 2373.

In the years following the publication of RFC 2373, the gurus who run the Internet had a change of heart regarding how address blocks should be considered. They still wanted to divide the IPv6 address space into variably sized blocks for different purposes. However, they realized that many people were starting to consider the use of format prefixes to be equivalent to the old class-oriented IPv4 system. Their main concern was that implementers might program into IPv6 hardware logic to make routing decisions based only on the first few bits of the address. This was specifically not how IPv6 is supposed to work; for one thing, the allocations are subject to change.

Thus, one of the modifications maae in RFC 3513 was to change the language regarding IPv6 address allocations, and specifically, to remove the term format prefix from the standard. The allocation of different parts of the address space is still done based on particular patterns of the first three to ten bits of the address to allow certain categories to have more addresses than others. The elimination of the specific term denoting this is intended to convey that these bits should not be given special attention.

This is more complicated than the IPv4 classful scheme because there are so many more categories and they range greatly in size, even if most of them are currently unassigned.

An easier way to make sense of this table is to consider the division of the IPv6 address space into *eighths*. Of these eight groups, one (001) has been reserved for unicast addresses; a second (000) has been used to carve out smaller reserved blocks, and a third (111) has been used for sub-blocks for local and multicast addresses. Five are completely unassigned.

You can see that the IPv6 designers have taken great care to allocate only the portion of these "eighths" of the address space that they felt was needed for each type of address. For example, only a small portion of the part of the address space beginning 111 was used, with most of it left aside. In total, only 71/512ths of the address space is assigned right now, or about 14 percent. The other 86 percent is unassigned and kep aside for future use. (Bear in mind that even 1/1024th of the IPv6 address space is gargantuan—it represent trillions of trillions of addresses.)

Later sections in this chapter provide more information on several of these address blocks. Note that the 0000 0000 reserved block is used for several special address types, including the loopback address, the unspecified address, and IPv4 address embedding. The 1111 1111 format prefix identifies multicast addresses; this string is FF in hexadecimal, so any address beginning with FF is a multicast address in IPv6.

IPv6 SPECIAL ADDRESSES: RESERVED, PRIVATE UNSPECIFIED, AND LOOPBACK

Just as certain IPv4 address ranges are designated for reserved, private, and other unusual addresses, a small part of the monstrous IPv6 address space has been set aside for special addresses. The purpose of these addresses and address blocks is to provide addresses for special requirements and private use in IPv6 networks. Since even relatively small pieces of IPv6 are still enormous, setting aside 0.1 percent of the address space for a particular use still generally yields more addresses than anyone will ever need.

Special Address Types

There are four basic types of special IPv6 addresses:

Reserved Addresses A portion of the address space is set aside as reserved for various uses by the IETF, both present and future. Unlike IPv4, which has many small reserved blocks in various locations in the address space, the reserved block in IPv6 is at the "top" of the address space, beginning with 0000 0000 (or 00 for the first hexadecimal octet). This represents 1/256th of the total address space. Some of the special addresses you'll see shortly come from this block. IPv4 address embedding is also done within this reserved address area.

Private/Unregistered/Nonroutable Addresses A block of addresses is set aside for private addresses, just as in IPv4, except that like everything in IPv6 the private address block in IPv6 is much larger. These private addresses are local only to a particular link or site and, therefore, are never routed outside a particular company's network. Private addresses are indicated by the address having "1111 1110 1" for the first nine bits. Thus, private addresses have a first octet value of FE in hexadecimal, with the next hexadecimal digit being from 8 to F. These addresses are further divided into two types based on their scope: site-local and link-local, as discussed shortly.

Loopback Address Like IPv4, a provision has been made for a special loopback address for testing; datagrams sent to this address "loop back" to the sending device. However, in IPv6, there is just one address for this function, not a whole block (which was never needed in the first place). The loopback address is 0:0:0:0:0:0:0:1, which is normally expressed using zero compression as ::9.

Unspecified Address In IPv4, an IP address of all zeros has a special meaning: It refers to the host itself and is used when a device doesn't know its own address. In IPv6, this concept has been formalized, and the all-zeros address (0:0:0:0:0:0:0:0) is named the *unspecified address*. It is typically used in the source field of a datagram sent by a device seeking to have its IP address configured. Zero compression can be applied to this address; since it is all zeros, the address becomes just ::.

9.5.3 Transmission from IPv4 to IPv6

The migration mechanisms described in this report are based on the transition mechanisms defined in RFC 2893 through the IETF NGtrans workgroup. These are:

- Dual IP layer operation;
- Configured tunnelling of IPv6 over IPv4;
- Automatic tunnelling of IPv6 over IPv4;
- IPv4-compatible IPv6 addresses.
- 6to4

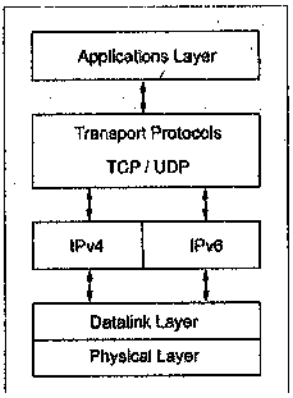
Furthermore, there exists other transition mechanisms. Network manufacturers have deployed various proprietary mechanisms, like the Intra Site Automatic Tunnel Addressing Protocol (ISATAP).

Dual IP Layer operation

The most used migration approach nowadays is the dual IP layer operation, also called the dual stack method. A host with a dual stack can interoperate with both IPv4 and IPv6 nodes using IPv4 or IPv6 packets. Dual stack has the possibility to disable one of the IP stacks for operational reasons.

A node configured with a dual stack can make decisions on TCP connections based on the IP header of the TCP packet:

- the IPv4 protocol stack will be used if the destination address used by the application is an IPv4 address;
- the IPv6 protocol stack will be used if the destination address used by the application is an IPv6 address;
- encapsulation of an IPv6 packet inside an IPv4 packet will occur if the destination address used by the application is an IPv6 address with embedded IPv4 address.

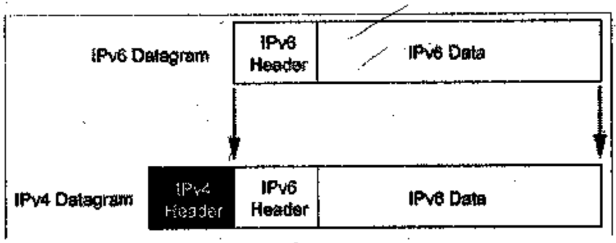


The dual stack approach

Dual stack makes it possible to continue provide access to IPv4 resources, while adding IPv6 functionality. The IP address acquisition in the dual stack nodes occurs by using IPv4 mechanisms like DHCP or IPv6 mechanisms, as for instance the stateless address auto-configuration. The ability to operate with different modes makes the dual stack approach a flexible and simple to deploy solution to work in networks that are connected with both IPv4 and IPv6 nodes. A disadvantage of this implementation is that two routing tables and two routing processes may be required. Hosts and routers that support dual stack may use tunnelling mechanisms to route IPv6 traffic over IPv4 networks.

Tunnelling

Because IPv6 will be developed over the IPv4 infrastructure, tunnelling provides a way to use the existing routing infrastructure to carry IPv6 traffic. Tunnelling IPv6 packets over IPv4 infrastructure is done by encapsulating IPv6 packets inside IPv4 packets as shown in figure below. The IPv6 header contains the address of the final destination and the IPv4 header contains the address of the tunnel endpoint.



Configured tunnelling of IPv6 over IPv4

As you can see on figures with Router-to-Router and Host-to-Router, the IPv6 traffic is tunneled to an endpoint, which is an IPv4/IPv6 router that is responsible for decoding and delivering the IPv6 packets to their final destination. Because the IP address of the router is not the same as the IP address of the final destination, a manual configuration of the tunnel endpoint is mandatory. This is called configured tunnelling. The decision of which packets to tunnel is done by the encapsulating node based on its routing table. The decapsulating node must ensure the validity of the tunnel source address before sending the decapsulated packets to their final destination. For this purpose, the other end of the tunnel has to check the IPv4 source address. For unidirectional configured tunnels, it is necessary to configure the decapsulating node with a list of valid source IPv4 addresses.

IPv4-compatible IPv6 addresses

IPv4-compatible IPv6 addresses are also known as 6over4. In this mechanism, existing IPv4 addresses are used to create IPv4-compatible IPv6 addresses. These addresses are identified by a 96bit zeros prefix followed by the 32bits IPv4 address. In this approach, IPv4 addresses become a virtual link-layer address by using IPv4 multicast group. Neighbour Discovery takes place by mapping IPv6 multicast addresses to IPv4 multicast addresses. The router must be configured as 6over4 in order to make IPv4 Multicast routing possible. The hard requirements and poor scalability characterize this implementation.

6to4

This mechanism consists of creating a unique /48 IPv6 prefix based on a globally unique IPv4 address. This provides many internal IPv6 networks in which nodes are either native IPv6 or dual stack. The 6to4 mechanism can be used at the edge of a network with no need to implement the mechanism internally. Addresses can be assigned from the /48 6to4 prefix by using the stateless or statefull configuration methods. Routing decisions are based on the embedded IPv4 addresses. Packets designated to a native IPv6 node will be forwarded by the 6to4 router to a special 6to4 relay where they will be treated. 6to4 is easy to deploy and does not require any application for an IPv6 address space from the registries. However, its impact on the global Internet is unknown.

9.6 ROUTING (CONTD.)

A routing protocol is the communication used between routers. A routing protocol allows one router to share information with other routers regarding the networks it knows about.

Examples of routing protocols are:

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)

An autonomous system (AS) is a collection of networks under a common administration sharing a common routing strategy. The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns an identifying number to each AS. This autonomous system number is a 16 bit number.

9.6.1 Autonomous system routing

Routing Information Protocol (RIP)

- ~~It is a~~ distance vector routing protocol.
- Hop count is used as the metric for path selection.
- If the hop count is greater than 15, the packet is discarded.
- Routing updates are broadcast every 30 seconds, by default.

Interior Gateway Routing Protocol (IGRP)

- Cisco proprietary protocol
- It is a distance vector routing protocol.
- Bandwidth, load, delay and reliability are used to create a composite metric.
- Routing updates are broadcast every 90 seconds, by default.

Open Shortest Path First (OSPF)

- It is a link-state routing protocol.
- Open standard routing protocol described in RFC 2328.

- Uses the SPF algorithm to calculate the lowest cost to destination.
- Routing updates are flooded as topology changes occur.

Enhanced-IGRP (EIGRP)

- Cisco proprietary protocol
- It is an enhanced distance vector routing protocol.
- Uses load balancing.
- Uses a combination of distance vector and link-state features.
- Uses Diffused Update Algorithm (DUAL) to calculate the shortest path.
- Routing updates are broadcast every 90 seconds or as triggered by topology changes.

9.6.2 Inter-Autonomous system routing

Border Gateway Protocol (BGP)

- Exterior routing protocol.
- It is a distance vector exterior routing protocol.
- Used between ISPs or ISPs and clients.
- Used to route Internet traffic between autonomous systems.

9.7 SUMMARY

The goal of a routing protocol is to build and maintain the routing table.

The Routing table contains the learned networks and associated ports for those networks. The routing protocol learns all available routes, places the best routes into the routing table, and removes routes when they are no longer valid. The network knowledgebase needs to reflect an accurate consistent view of the current topology.

9.8 GLOSSARY

1. Datagram – PDU for IP Layer in TCP/IP
2. DHCP - Dynamic Host Configuration Protocol is used to assign IP addresses dynamically to network cards works at the application layer. RFC 1541.
3. DNS - Domain Name System is used on the internet to correlate between IP address and readable names. RFC 1034, 1035, 1535-1537, 1591.

9.9 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. Computer Networks : A.Tanenbaum
3. Data & Computer Networks : William Stallings
4. CCNA - Second year Companion Guide - Cisco Press

9.10 UNIT END QUESTIONS

1. Differentiate between Routed & Routing protocols.
2. What are the major features of Datagram networks?
3. What are the major features of Virtual Circuit networks?
4. Differentiate between connection-oriented & connection-less protocols.
5. Describe major characteristics of IPv4 addressing technique.
6. Differentiate between IPv4 & IPv6 techniques.
7. Explain migration techniques from IPv4 to IPv6.
8. List out key features of RIP and OSPF.
9. Give significance of IGMP.
10. Define Autonomous System.

UNIT - 10

TRANSPORT SERVICES AND MECHANISM

Structure of the Unit

10.0 OBJECTIVE

After studying this unit, you will learn

- Functions of Transport layer

- Transmission Control Protocol(TCP)
- User Datagram Protocol(UDP)
- Congestion Control
- Quality of Service(Qos)
- Stream Control Transmission Protocol(SCTP)

10.1 INTRODUCTION

A transport layer is responsible for process to process delivery of the entire message. A process is an application program running on a host. A transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. The Internet model has three protocols at the transport layer: Transmission Control Protocol(TCP) ,User Datagram Protocol(UDP) and Stream Control Transmission Protocol(SCTP).

10.1.1 What is Transport Layer

The transport layer provides a mechanism for the exchange of data between end systems. This layer is also responsible for quality of service. In the TCP/IP protocol suite, there are two common transport layer protocols : the connection –oriented TCP(transmission control protocol) and the connectionless UDP(user datagram protocol). The connection-oriented transport service ensures that data are delivered error-free, in sequence, with no losses or duplication. Unlike the Connection-oriented services, Connectionless adds no reliability, flow control or error-recovery functions to IP.

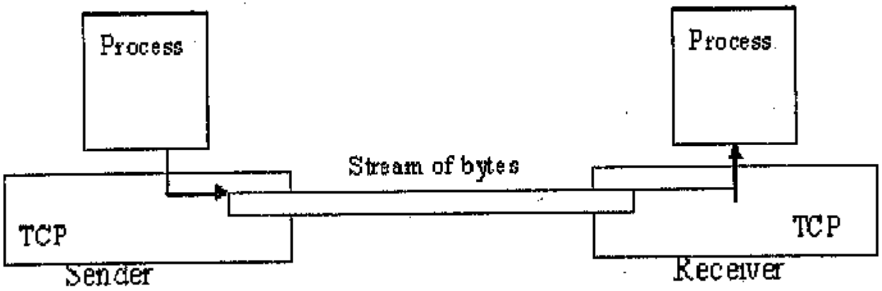
A new transport layer protocol, SCTP(Stream control transmission protocol), has been devised to answer the needs of some new applications(IP telephony). It is a transport layer protocol that combines the good features of UDP and TCP.

10.1.2 Type of Services

Transport layer protocol provides number of services like reliable, transparent transfer of data between end points. It also provides end-to-end error recovery and flow control.

There are number of services offered by the Transport layer , which are as follows:

1. **Process-to-process communication** : the transport protocol provides an end-to-end data transfer service that shields upper layer protocols from the details of the intervening network or networks. Similar to UDP , TCP provides process –to-process communication using port numbers. Well defined port numbers are dedicated to specific applications. For example system A communicate with system B by using TELNET, and at the same time system B communicate with system C by using HTTP. For theses processes to occur simultaneously , they need addresses . In TCP/IP architecture, the address assigned to a process is called a port address. It is 16-bit long.
2. **Stream delivery service :** TCP unlike UDP is a stream control protocol. we know that TCP transfers a contiguous stream of bytes through the internet . TCP is used to send messages by grouping the bytes , which are passed to IP for transmission to the destination. TCP creates an environment in which the two processes seem to be connected by an imaginary tube that carries data across the Internet.



3. **Reliability :** Transport layer service can be reliable or unreliable. TCP and SCTP is connection-oriented and reliable transport layer. Reliability means message or data must be received by the receiver without any error. So TCP uses an acknowledgement mechanism to check the safe arrival of data. To maintain the reliability system uses different error control techniques . we know that error control in the Data link layer is based on automatic repeat request, which is a retransmission of data . UDP is called a connectionless and unreliable transport protocol. It performs very limited error checking.

4. **Flow control:** We know that flow control coordinates the amount of data that can be sent to the receiver before receiving acknowledgement. Basically it is a procedure that tells the sender how much data it can transmit before it must wait for an acknowledgement(response) from the receiver. UDP is connection-less transport protocol, so there is no flow-control. The receiver may overflow with incoming messages. TCP unlike UDP provides flow control. The receiver of the data controls the amount of data that are to be sent by the sender. Flow control is used to prevent the receiver from being overwhelmed with data.

5. **Error control :** This function is basically maintained by the Data link layer. Error control is a technique which is used to maintain sending message reliable. There are number of error control techniques distinguished by their functions. TCP implements an error control. We know that TCP is a connection-oriented transmission protocol , so it sends message from one process to another process with reliable transmission. Error control considers a segment as a unit of data for error detection. Error control is byte-oriented.

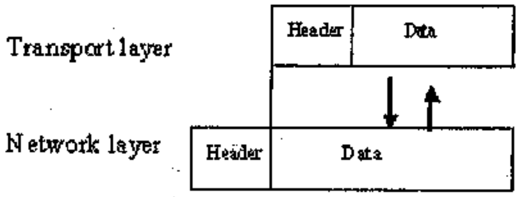
6. **Congestion control:** we know that congestion in a network may occur if the load on the network is greater than the capacity of the network. So congestion control refers to the methods and techniques to keep the load below the capacity. Transport layer is responsible for congestion control. Transport layer defines two categories such as prevention and removal methods.

10.1.3 Relationship between Transport layer and Network layer

We know that TCP/IP protocol suite was developed prior to the OSI model. So when TCP/IP is compared to OSI model , we know that the internet layer is equivalent to the network layer . Transport layer is same in both protocol suits . every layer can be defined by their protocols . So different protocols are distinguished by their different functions . So when we compare two layers such as Network layer and Transport layer, we must know about protocols which are used in these two layers.

Transport layer defines three protocols : Transmission control protocol(TCP), User datagram protocol(UDP) , and Stream control Transmission protocol(SCTP).

Network layer supports the Internetworking Protocol, which uses four supporting protocols : Address Resolution Protocol(ARP) , Reverse Address Resolution Protocol(RARP) , Internet Control Message Protocol(ICMP) and Internet Group Message Protocol(IGMP).



We know that Transport layer is responsible for process to process delivery of the entire message. When application layer generates message with the help of different protocols as FTP, HTTP, TELNET etc. Application layer is also responsible to send messages to the next layer. Next layer is Transport layer so transport layer receives message from the application layer and include header part. Header part includes control information such as source address , destination address etc. if transport layer is ready to send messages to the next layer (network layer), it includes port address in the header part to choose among multiple processes running on the destination host . The destination port number is needed for delivery, the source port number is needed for the reply. When network layer receives message from the transport layer, it includes IP address(logical address) in the header part.

We know that logical addresses are necessary for universal communication. It is required because network layer is responsible for source to destination delivery of a packet across multiple links. But if we send data from source to destination in the same network, there is no requirement for network layer. Network layer or logical address is required to send messages from one network to another network. The network layer oversees source to

destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message. the transport layer on the other hand ensures that the whole message arrives intact and in-order.

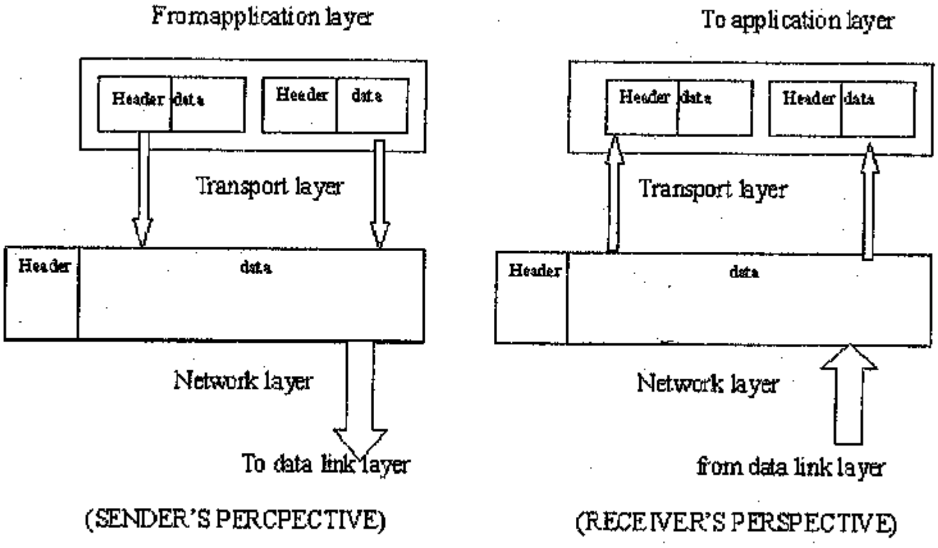


Figure : 10.3 Relationship between Transport layer and Network layer

10.1.4 Transport Layer In Internet

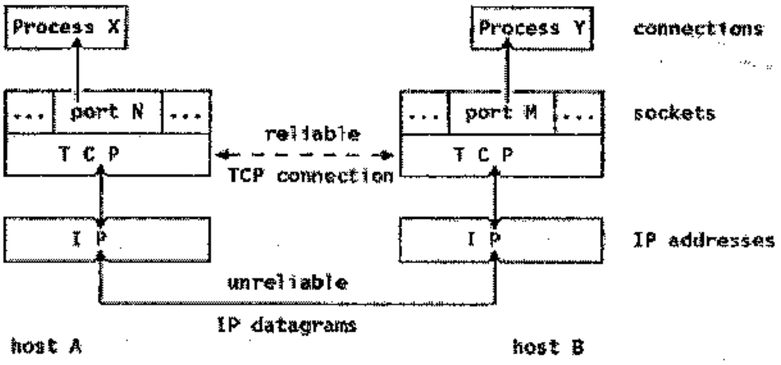
We know that an Internet is a collection of individual networks, connected by intermediate networking devices, that function as a single large networks. Internet is a global network of computer networks utilizing a suite of protocols called TCP/IP that supports interconnection of a number of different networks. Internet refers to the Industry, products, and procedures that meet the challenge of creating and administering Inter-networks. Internet can be defined as:

INTERNET := INTER(interconnected)+ NET(different networks).

Internet is network of computers that offer access to people and information. Over 60 million people use internet, and the number is expected to increase over 120 million within a few years. The kind of information freely available from internet includes Government documents, Scientific data, hobbyist lists, business and personal information, advertising databases and much more.

Transport layer plays an important role in Internet. Because the primary requirement of the Internet is reliable transmission, that can only be provided by the Transport layer. In Transport layer, reliable transmission or error free transmission can be achieved by Transmission control protocol(TCP). TCP accepts message information from the applications and divides it into multiple segments, and encapsulates each segment into a datagram. each datagram is passed over to the network layer protocol (IP) for further transmission and routing. At the receiver's end, TCP reassembles the data and distributes it to the concerned application program (SENDER'S PERSPECTIVE)

Transport layer provi :ion between source and destination. This logical connection can be established with port address, which is defined by the Transport layer.



here Internet protocol or IP can be defined as a postal department. Because it routes data packets or message to the address mentioned in the header field and fragments them.

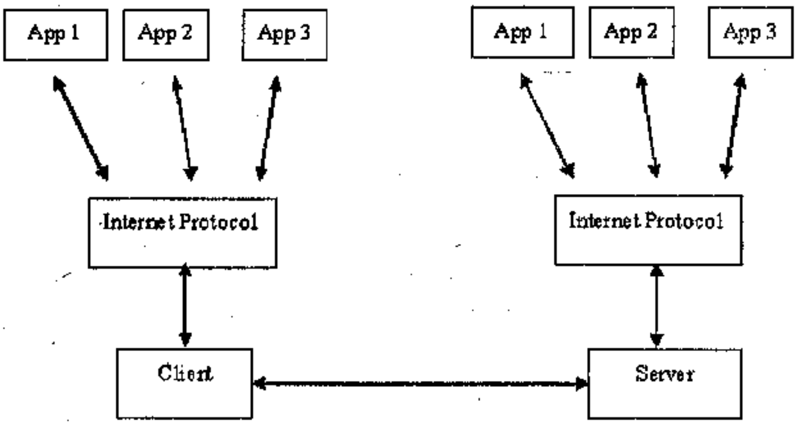
Message at the receiver site must be arranged in the same sequence as were in the sender site. The header also has a field called 'Time to live' or TTL is used to define the number of routers a data packet can encounter a route to its destination .

10.1.5 Multiplexing and De multiplexing

Most communication in TCP/IP takes the form of exchanges of information between a program running on one device, and a matching program on another device. Each instance of an application represents a copy of that application software that needs to send and receive information. These application instances are commonly called *processes*.

So, a typical TCP/IP host has multiple processes, each needing to send and receive data grams. All of them, however, must be sent using the same interface to the inter-network, using the IP layer. In the Transport layer the need for multiplexing arise in a number of ways. This means that the data from all applications (with some possible exceptions) is "funneled down", initially to the transport layer, where it is handled by either TCP or UDP. From there, messages pass to the device's IP layer, where they are packaged in IP datagrams and sent out over the inter-network to different destinations. Or we can say that at the sender site, there may be several processes that need to send packets. There is only one transport protocol at any time. This is a many to one relationship. The technical term for this is *multiplexing*. This term simply means combining, and its use here is a software analog to the way it is done with signals.

A complementary mechanism is responsible for receipt of datagrams. At the same time that the IP layer multiplexes datagrams from many application processes to be sent out, it receives many datagrams that are intended for different processes. The IP layer must take this stream of unrelated datagrams, and eventually pass them to the correct process (through the transport layer protocol above it). This is the reverse of multiplexing: *demultiplexing*. So we can say that at the receiver site, the relationship is one-to-many relationship and requires de multiplexing You can see an illustration of the basic concept behind TCP/IP process multiplexing and de multiplexing in the following figure:



Process Multiplexing and Demultiplexing In TCP/IP

TCP/IP is designed to allow many different applications to send and receive data simultaneously using the same Internet Protocol software on a given device. To accomplish this it is necessary to *multiplex* transmitted data from many sources as it is passed down to the IP layer. As a stream of IP datagrams is received, it is *demultiplexed* and the appropriate data passed to each application software instance on the receiving host.

10.2 CONNECTIONLESS TRANSPORT: UDP

The Internet makes two Transport protocols available to its applications: UDP and TCP.UDP is a connectionless Transport layer (layer 4) protocol in OSI model, which provides a simple and unreliable message-service-for-transaction-oriented-services. UDP is basically an interface between IP and upper-layer processes. The User datagram protocol(UDP) is called a connectionless, unreliable Transport protocol. UDP protocol ports distinguish multiple applications running on a single device from one another.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine, and some way to make sure replies get routedto the correct application on the source computer. This is accomplished through the use of the UDP "port numbers". For example, if a station wished to use a Domain Name System (DNS) on the station 128.1.123.1, it would address the packet to station 128.1.123.1 and insert destination port number 53 in the UDP header. The source port number identifies the application on the local station that requested domain name server, and all response packets generated by the destination station should be addressed to that port number on the source station.

UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control . it is not used for a process such as FTP that needs to send bulk data. Note that with UDP there is no handshaking between sending and receiving Transport-layer entities before sending a segment. For this reason, UDP is said to be *connectionless*. UDP is suitable for a process with internal flow and error control. It is suitable Transport protocol for *multicasting*. Multicasting capability is embedded in the UDP software but not in the TCP software. It is also used for management processes such as Simple Network Management Protocol(SNMP) and some routing updating protocols such as Routing Information Protocol(RIP).

DNS is an example of an application-layer protocol that uses UDP. When the DNS application in a host wants to make a query, it constructs a DNS query message and passes the message to a UDP socket, Without performing any handshaking, UDP adds a header fields to the message and passes the resulting segment to the network layer. The network layer encapsulates the UDP segment into a datagram and sends the datagram to a name server. The DNS application at the querying host then waits for a reply to its query. If it doesn't receive a reply (possibly because UDP lost the query or the reply), it either tries sending the query to another Name server, or it informs the invoking application that it can't get a reply.

Now you might be wondering why an application developer would ever choose to build an application over UDP rather than over TCP. Isn't TCP always preferable to UDP since TCP provides a reliable data transfer service and UDP does not? The answer is no, as many applications are better suited for UDP for the following reasons:

- **No connection establishment.** We know that TCP uses a three-way handshake before it starts to transfer data. UDP just blasts away without any formal preliminaries. Thus UDP does not introduce any delay to establish a connection. This is probably the principle reason why DNS runs over UDP rather than TCP . DNS would be much slower if it ran over TCP. HTTP uses TCP rather than UDP, since reliability is critical for Web pages with text..
- **No connection state.** TCP maintains connection state in the end systems. This connection state includes receive and send buffers, congestion control parameters, and sequence and acknowledgment number parameters. This state information is needed to implement TCP's reliable data transfer service and to provide congestion control. UDP, on the other hand, does not maintain connection

state and does not track any of these parameters. For this reason, a server devoted to a particular application can typically support many more active clients when the application runs over UDP rather than TCP.

- **Small segment header overhead.** The TCP segment has 20 bytes of header overhead in every segment, whereas UDP only has 8 bytes of overhead.
- **Unregulated send rate.** TCP has a congestion control mechanism that throttles the sender when one or more links between sender and receiver becomes excessively congested. This throttling can have a severe impact on real-time applications. On the other hand, the speed at which UDP sends data is only constrained by the rate at which the application generates data, the capabilities of the source (CPU, clock rate, etc.) and the access bandwidth to the Internet. We should keep in mind, however, that the receiving host does not necessarily receive all the data - when the network is congested, a significant fraction of the UDP-transmitted data could be lost due to router buffer overflow. Thus, the receive rate is limited by network congestion even if the sending rate is not constrained.

Nevertheless, many important applications run over UDP rather TCP. UDP is used for RIP routing table updates, because the updates are sent periodically, so that lost updates are replaced by more up-to-date updates. UDP is used to carry network management data. UDP is preferred to TCP in this case, since network management must often run when the network is in a stressed state - precisely when reliable, congestion-controlled data transfer is difficult to achieve. Also, as we mentioned earlier, DNS runs over UDP, thereby avoiding TCP's connection establishment delays.

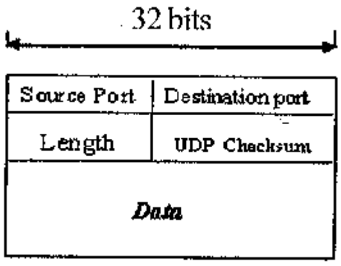
Application	**Application-layer protocol**	**Underlying Transport Protocol**
electronic mail	SMTP	TCP
remote terminal access	Telnet	TCP
Web	HTTP	TCP
file transfer	FTP	TCP
remote file server	NFS	typically UDP
streaming multimedia	proprietary	typically UDP
Internet telephony	proprietary	typically UDP
Network Management	SNMP	typically UDP
Routing Protocol	RIP	typically UDP
Name Translation	DNS	typically UDP

Popular Internet applications and their underlying transport protocols.

As shown in the above table, UDP is also commonly used today with multimedia applications, such as Internet phone, real-time video conferencing, and streaming of stored audio and video. TCP cannot be employed with multicast, multicast applications run over UDP.

10.2.1 UDP Segment Structure

UDP packets, called user datagrams, have a fixed-size header of 8 bytes. The UDP segment structure is defined as :



UDP segment structure

A UDP segment consists of 8 byte header followed by the data. The two ports serve the same function as they do in TCP : to identify the end points within the source and destination machines. The UDP length field includes the 8-byte header and the data. The UDP checksum includes the format as : the UDP header , UDP data , padded out to an even number of bytes. It is optional and stored as 0 if not computed. The application data occupies the data field of the UDP datagram. For example, for DNS, the data field contains either a query message or a response message. For a streaming audio application, audio samples fill the data field. The checksum is used by the receiving host to check if errors have been introduced into the segment during the course of its transmission from source to destination. UDP segment structure can be briefly defined as :

- **Source port** - Source port is an optional field. This is the port number used by the process running on the source host. It is 16 bits long. When used, it indicates the port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.
- **Destination port** - Destination port has a meaning within the context of a particular Internet destination address. It is 16 bits long. This is the port number used by the process running on the destination host .
- **Length** - It is the length in octets of this user datagram, including this header and the data. The minimum value of the length is eight. The length field in a UDP user datagram is actually not necessary . A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length.
- **Checksum** – This field is used to detect errors over the entire user datagram(header plus data). The sum of a pseudo header of information from the IP header, the UDP header and the data, padded with zero octets at the end, if necessary, to make a multiple of two octets.
- **Data** - Contains upper-level data information.

10.2.2 UDP Checksum

The UDP checksum calculation is different from the one for IP and ICMP. It includes three sections: a pseudo header, the UDP header and the data coming from the application layer. The pseudo header is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0's, and the protocol field is added to ensure that the packet belongs to UDP , not to other transport layer protocol. The UDP checksum provides for error detection. UDP at the sender side performs the one's complement of the sum of all the 16-bit words in the segment. This result is put in the checksum field of the UDP segment (In truth, the checksum is also calculated over a few of the fields in the IP header in addition to the UDP segment). When the segment arrives (if it arrives!) at the receiving host, all 16-bit words are added together, including the checksum. If this sum equals 1111111111111111, then the segment has no detected errors. If one of the bits is a zero, then we know that errors have been introduced into the segment.

Here we give a simple example of the checksum calculation. You can find details about efficient implementation of the calculation . As an example, suppose that we have the following three 16-bit words:

```
0110011001100110
0101010101010101
0000111100001111
```

The sum of first of these 16-bit words is:

```
0110011001100110
0101010101010101
----------------
1011101110111011
```

Adding the third word to the above sum gives

1011101110111011
0000111100001111
1100101011001010

The 1's complement is obtained by converting all the 0s to 1s and converting all the 1s to 0s. Thus the 1's complement of the sum 1100101011001010 is 0011010100110101, which becomes the checksum. At the receiver, all four 16-bit words are added, including the checksum. If no errors are introduced into the segment, then clearly the sum at the receiver will be 1111111111111111. If one of the bits is a zero, then we know that errors have been introduced into the segment. We know that the Internet checksum is not foolproof, even if the sum equals 111111111111111, it is still possible that there are undetected errors in the segment. For this reason, a number of protocols use more sophisticated error detection techniques than simple check summing.

10.3 CONNECTION ORIENTED TRANSPORT : TCP

TCP provides a different service than UDP. The **Transmission Control Protocol (TCP)** is one of the core protocols of the Internet Protocol Suite. TCP was one of the two original components, with Internet Protocol (IP), of the suite, so that the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Besides the Web, other common applications of TCP include e-mail and file transfer. Among its other management tasks, TCP controls message size, the rate at which messages are exchanged, and network traffic congestion.

TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details.

IP works by exchanging pieces of information called packets. A packet is a sequence of bytes and consists of a *header* followed by a *body*. The header describes the packet's destination and, optionally, the routers to use for forwarding—generally in the right direction—until it arrives at its final destination. The body contains the data which IP is transmitting. When IP is transmitting data on behalf of TCP, the content of the IP packet body is TCP payload.

Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost or delivered out of order. TCP detects these problems, requests retransmission of lost packets, rearranges out-of-order packets, and even helps minimize network congestion to reduce the occurrence of the other problems.

10.3.1 TCP segment structure

A TCP segment consists of two sections:

- Header
- data

The TCP header consists of 11 fields, of which only 10 are required. The eleventh field is optional and is aptly named "options".

- **Source port** – This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.
- **Destination port**– This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.
- **Sequence number**– This 32-bit field defines the number assigned to the first byte of data contained in this segment.

- **Acknowledgement number**–This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other host. Acknowledgement and data can be piggybacked together.
- **Data offset** –This is a 4-bit field that specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.
- **Reserved** – This is a 6-bit field reserved for future use.
- **Flags** (Control bits) – This field contains 6 1-bit flags, which are as follows:
  - **URG (1 bit)** – indicates that the value of the urgent pointer field is valid.
  - **ACK (1 bit)** – indicates that the Acknowledgment field is significant.
  - **PSH (1 bit)** – Push function.
  - **RST (1 bit)** – Reset the connection.
  - **SYN (1 bit)** – Synchronize sequence numbers.
  - **FIN (1 bit)** – No more data from sender or terminate the connection.
- **Window size** –The length of this field is 16 bits. the size of the **receive window**, which specifies the number of bytes (beyond the sequence number in the acknowledgment field) that the receiver is currently willing to receive .
- **Checksum**– The 16-bit checksum field is used for error-checking of the header and data
- **Urgent pointer**– if the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.
- **Options**– There can be up to 40 bytes of optional information in the TCP header.
- **Data** —As you might expect, this is the payload, or data portion of a TCP packet. The payload may be any number of application layer protocols. The most common are HTTP, Telnet, SSH, FTP, but other popular protocols also use TCP.

10.3.2 Round trip time estimation in reliable transport protocol

RTT is an acronym for Round Trip Time, it is a measure of the time it takes for a packet to travel from a computer, across a network to another computer, and back. Transport protocols like TCP which expect an acknowledgment to arrive after data has been successfully received, keep an estimate of the current RTT on each connection. They use the RTT estimate to determine how long to wait for an acknowledgment before retransmitting. The sending side records the clock when it transmits a packet, and then examines the clock again when an acknowledgment arrives. By subtracting the two values, it obtains a single estimate of the round trip time(RTT). It then combines that single estimate with previous estimates to get an average.

Dynamically estimating the round-trip time, the interval between the sending of a packet and the receipt of its acknowledgement, is a key function in many reliable Transport protocols . Such estimates are used to ensure that data is reliably delivered. If a packet remains unacknowledged for too long, it is assumed to have been lost and is retransmitted. Estimated round-trip times are used to determine when these retransmissions will occur. Two developments in IP networking have led to increased interest in the problems of estimating round-trip times. First, there has been an explosive growth in the size and complexity of IP *inter networks*, built by interconnecting existing sub networks. The best known example is the ARPA Internet. (The ARPANET is just one component sub network in the ARPA Internet.) The ARPA Internet has highly variable round-trip times. Because its paths are very complex, it also tends to lose more packets. Second, there has been a large increase in traffic on some of the major IP networks. Higher traffic loads have led to serious network congestion on some parts of the ARPA Internet . Like network size, congestion is known to cause highly variable round-trip times and higher packet loss rates.

Finally, recent research has shown that the standard approaches to estimating round-trip times for the Transmission Control Protocol (TCP) are inaccurate if packets are lost or round-trip times are highly variable . This discovery is distressing because it suggests that the mechanism reliable protocols depend upon to handle loss and variable round-trip times, namely the estimation of round-trip times, may not work well.

Concern about the accuracy of estimated round-trip times has led to some interesting research into reliability mechanisms which are less dependent on round-trip estimates . So it takes a different approach that tries to improve the data used to compute round-trip time estimates. Heterogeneous communication networks with their variety of application demands, uncertain time-varying traffic load, and mixture of wired and wireless links pose several challenging problem in modeling and control. our focus is on the Round-Trip Time (RTT), which is a particularly important variable for efficient end-to-end congestion control. Based on a simple aggregated model of the network, an algorithm combining a Kalman filter and a change detection algorithm is proposed for RTT estimation. It is illustrated on real data that this algorithm provides estimates of significantly better accuracy as compared to the RTT estimator currently used in TCP, especially in scenarios where new cross-traffic flows cause a bottle-neck link to rapidly build up a queue, which in turn induces rapid changes of the RTT.

10.3.3 Reliable Data Transfer

We know that Transport layer is responsible for process to process delivery of the entire message. A process can be defined as an application program on a host. .Transport layer header include a type of address called a service point address. Transport layer protocols can be either connectionless and connection-oriented . For reliable transmission, network use connection oriented transmission . So we can say that Transport layer service can be reliable or unreliable .If an application program or any process needs reliability , we use reliable Transport layer protocol. Any transmission can be reliable by implementing flow and error control at this layer. We know that data link layer is responsible for flow control and error control , the Transport layer may be responsible for flow and error control. Data link layer is responsible for reliability between two nodes , but if we need reliability between two ends , we need to implement reliability at the Transport layer. Flow and error control at the transport layer is performed end to end rather than across a single link. TCP protocol is based on connection oriented network between sender and receiver and also responsible for reliable data transfer.

A link level protocol that wants to deliver frames reliably must somehow recover from discarded (lost) frames.

This is usually accomplished using a combination of two fundamental mechanisms –

1. **Acknowledgements:-** An acknowledgement is a small control frame that a protocol sends back to its peer saying that it has received an earlier frame. By control frame we mean a header without any data . the receipt of an acknowledgement indicates to the sender of the original frame that its frame was successfully delivered.
2. **Timeouts :-** If the sender does not receive an acknowledgement after a reasonable amount of time , then it retransmits the original frame . This action of waiting a reasonable amount of time is called *timeouts.*

As a reliable, end-to-end Transport protocol, the Transmission Control Protocol(TCP) uses positive acknowledgements and retransmission to guarantee delivery. TCP implementations are expected to measure and adapt to changing network propagation delays so that its retransmission behavior balances user throughput and network efficiency. However, TCP suffers from a problem we call *retransmission ambiguity*: when an acknowledgment arrives for a segment that has been retransmitted, there is no indication which transmission is being acknowledged. Many existing TCP implementations do not handle this problem correctly.

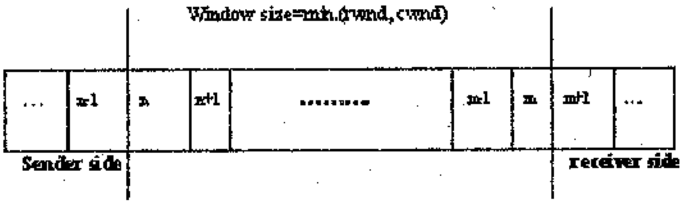
10.3.4 Flow control

The main task of the Transmission Control Protocol(TCP) is simple: packaging and sending data. Of course, almost every protocol packages and sends data. This system not only manages the basic data transfer process, it is also used to ensure that data is sent reliably, and also to manage the flow of data between devices to ensure that data is transferred efficiently without either device sending data faster than the other can receive it.

TCP uses an end-to-end flow control protocol to avoid having the sender send data too fast for the TCP receiver to reliably receive and process it. TCP uses a sliding window flow control protocol. The sliding window protocol in TCP looks like the Go-Back-N protocol because it does not use negative acknowledgement (NAKs) . it also looks like selective Repeat bacause the receiver holds the out of order segments until the missing ones arrive. There are two big differences between this sliding window and the one we used at the data link layer. First , the sliding window of TCP is byte oriented, but the one in the data link layer is frame oriented. Second, the TCP's sliding window is of variable size, but the one in the data link layer was of fixed size.

In each TCP segment, the receiver specifies in the **receive window** field the amount of additional received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that amount of data before it must wait for an acknowledgment and window update from the receiving host.

Having a mechanism for flow control is essential in an environment where machines of diverse network speeds communicate. For example, when a fast PC sends data to a slow hand-held PDA, the PDA needs to regulate the influx of data, or protocol software would be overrun quickly. Similarly, flow control is essential if the application that is receiving the data is reading it more slowly than the sending application is sending it.



The size of the window at one end is determined by the lesser of two values : receiver window (rwnd) or congestion window(cwnd). The receiver window (rwnd) shifts each time the receiver receives and acknowledges a new segment of data. Once it runs out of sequence numbers, the sequence number loops back to 0.

When a receiver advertises a window size of 0, the sender stops sending data and starts the **persist timer.** The persist timer is used to protect TCP from a deadlock situation that could arise if the window size update from the receiver is lost and the sender has no more data to send while the receiver is waiting for the new window size update. When the persist timer expires, the TCP sender sends a small packet so that the receiver sends an acknowledgement with the new window size.

If a receiver is processing incoming data in small increments, it may repeatedly advertise a small receiver window(rwnd). This is referred to as the silly window syndrome, since it is inefficient to send only a few bytes of data in a TCP segment, given the relatively large overhead of the TCP header. TCP senders and receivers typically employ flow control logic to specifically avoid repeatedly sending small segments.

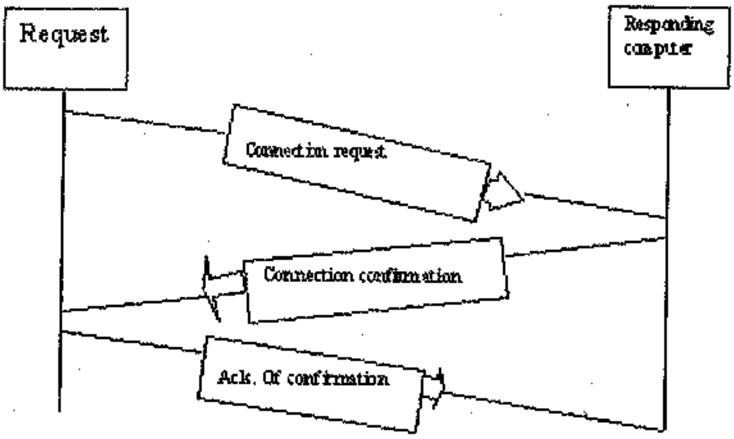
10.3.5 TCP Connection management

We know that TCP is connection oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgement process as well as retransmission of damaged or lost frames. We know that TCP uses the services of IP(connectionless) to deliver individual segments to the receiver, but it controls the connection itself.

In TCP, connection management requires three phases: connection establishment, data transfer and connection termination.

1. **Connection Establishment**

TCP transmits data in full duplex when two machines are connected, they are able to send packets to each other simultaneously. Before either communicating device can send data to the other, the initiating device first must determine the availability of the other to exchange data and a pathway must be found through the network by which the data can be sent. This step is called connection establishment. Connection establishment requires three actions in what is called a three-way handshake.



a. The computer requesting the connection sends a connection request packet to the intended receiver.

b. The responding computer returns a confirmation packet to the requesting computer.

c. The requesting computer returns a packet acknowledging the confirmation.

2. **Data Transfer :**

After connection is established, bi-directional data transfer can take place. The client and server can both send data and acknowledgements. The data segments sent by the client have the PSH(push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received. We know that the sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size.

The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP. The application program at the receiving site can request a push operation . This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

3. **Connection Termination**

Once all the data have been transferred, the connection must be terminated. Any of two parties involved in exchanging data(client or server) can close the connection, although it is usually initiated by the client. Connection termination also requires a three-way handshake:

a. The requesting computer sends a disconnection request packet.

b. The responding computer confirms the disconnection request.

c. The requesting computer acknowledges the confirmation.

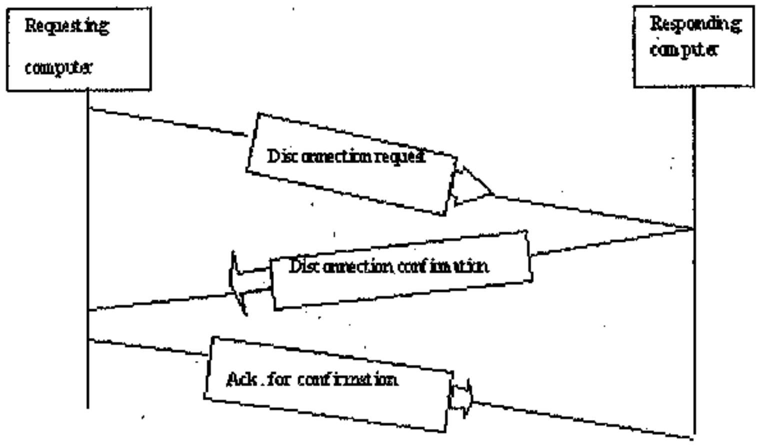


Figure :10.9

10.4 CONGESTION CONTROL

Congestion in a network may occur if users send data into the network at a rate greater than that allowed by network resources. For example, congestion may occur because the switches and routers have queues-have a limited buffer size to store arrived packets before processing and after processing . Congestion is an important issue in a packet-switched network. Congestion in a network may occur if the load on the network- the no. of packets sent to the network- is greater than the capacity of the network. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

10.4.1 Causes and Costs of Congestion

Congestion control involves two factors that measure the performance of a network delay and throughput. We identify that when the load is much less than the capacity of the network, the delay is at the minimum. We can define throughput in a network as the number of packets passing through the network in a unit of time . We notice that when the load is below the capacity of the network , the throughput increases proportionally with the load. Then the throughput in a network declines sharply. The reason is the discarding of packets by the routers.

10.4.2 Approaches to Congestion Control

It refers to techniques and mechanisms that can either prevent congestion before it happens, or remove congestion , after it has happened. Using congestion control techniques we try to alleviate congestion after it happens. We have number of techniques to control congestion are as follows:

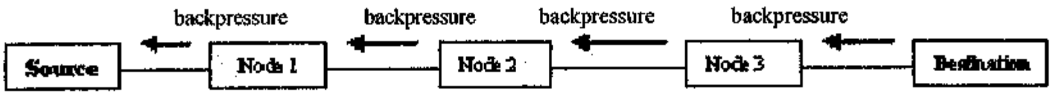
a. Backpressure

b. Choke Packet

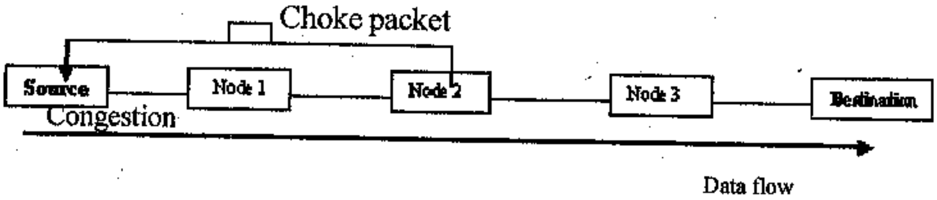
c. Implicit congestion signaling

d. Explicit congestion signaling

1. **Backpressure:** This technique produces an effect similar to backpressure in fluids flowing down a pipe. When the end of a pipe is closed , the fluid pressure backs up the pipe to the point of origin, where the flow is stopped.Backpressure is a node to node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. This technique can be applied only to virtual circuit networks



2. **Choke packet:-** A choke packet is a control packet generated at a congestion node and transmitted back to a source node to restrict traffic flow. Actually a chock packet is a packet sent by a node to the source to inform it of congestion. We know the difference between the backpressure and choke packet method , in backpressure the warning is from one node to its upstream node. But in the choke packet method, the warning if from router, which has encountered congestion, to the source station directly. We have used this type of control in ICMP, it informs the source host using a source quench ICMP message. The warning message goes directly to the source station. In addition a system may anticipate congestion and issue source quench messages when its buffers approach capacity.



3. **Implicit channel Signaling :-** we know that TCP maintains a new state variable for each connection , called congestion window(cwnd) which is used by the source to limit how much data it is allowed to have in transit at a given time. When network congestion occurs , two things may happen : 1) the transmission delay for an individual packet from source to destination increases and 2) packets are discarded. If a source is able to detect increased delays and packet discards, then it has implicit evidence of network congestion. In implicit signaling , there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network. For example , when a source sends several packets and there is no acknowledgement for a while , one assumption is that the network is congested. The delay in receiving an acknowledgement is interpreted as congestion in the network, the source should slow down. This type of signaling is used in TCP.

4. **Explicit channel signaling :-** It is desirable to use as much of the available capacity in the network as possible but still react to congestion in a controlled and fair manner. Explicit congestion control techniques operate over connection –oriented networks and control the flow of packets over individual connections . Explicit signaling can occur in either the forward and backward direction.

   a) **Backward :** A bit can be sent in a packet moving in the direction opposite to the congestion . This packet is used to warn the source that there is congestion and it needs to slow down to avoid the discarding of packets.

   b) **Forward:** A bit can be sent in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies , such as slowing down the acknowledgements to alleviate the congestion.

10.4.3 TCP Congestion Control

TCP uses congestion control to avoid congestion or alleviate congestion in the network. In TCP the **congestion window** determines the number of bytes that can be outstanding at any time. This is a means of stopping the link between two places from getting overloaded with too much traffic. The size of this window is calculated by estimating how much congestion there is between the two places. The sender maintains the congestion window. When a connection is set up, the congestion window is set to the Maximum segment size (MSS) allowed on that connection. Further variance in the collision window is dictated by an AIMD approach. This means that if all segments are received and the acknowledgments reach the sender on time, some constant is added to the window size. The window keeps growing linearly until a timeout occurs or the receiver reaches its limit. If a timeout occurs, the window size is halved.

TCP uses a congestion window in the sender side to do congestion avoidance. The sender window size is determined by the available buffer space in the receiver (rwnd). Today, the senders window size is determined not only by the receiver but also by the congestion in the network. So the actual size of the window is the minimum of these two.

Actual window size = minimum (receiver window size, congestion window size)

Where the congestion window size(cwnd) indicates the maximum amount of data that can be sent out on a connection without being acknowledged.

TCP's congestion policy is based on three phases: slow start, congestion avoidance and congestion detection .

1. **Slow start :-** One of the algorithims used in TCP congestion control is called slow start. Slow start algorithim is operates by that the rate at which new packets should be injected into the network is the rate at which the acknowledgments are returned by the other end. Slow start adds another window to the sender's TCP: the congestion window, called "cwnd". When a new connection is established with a host on another network, the congestion window is initialized to one segment.

2. **Congestion Avoidance :-** At some point the capacity of the internet can be reached, and an intermediate router will start discarding packets. This tells the sender that its congestion window has gotten too large. Congestion can also occur when multiple input streams arrive at a router whose output capacity is less than the sum of the inputs. Congestion avoidance is a way to deal with lost packets.

   The assumption of the algorithm is that packet loss caused by damage is very small (much less than 1%), therefore the loss of a packet signals congestion somewhere in the network between the source and destination. There are two indications of packet loss: a timeout occurring and the receipt of duplicate ACKs. Congestion avoidance and slow start are independent algorithms with different objectives. But in practice they are implemented together.

   Congestion avoidance and slow start require that two variables be maintained for each connection: a congestion window, cwnd, and a slow start threshold size, sthresh. When congestion occurs (indicated by a timeout or the reception of duplicate ACKs), one-half of the current window size (the minimum of cwnd and the receiver's advertised window, but at least two segments) is saved in sthresh. Additionally, if the congestion is indicated by a timeout, cwnd is set to one segment (i.e., slow start).

3. **Congestion Detection :-** TCP detects congestion when it fails to receive an acknowledgement for a packet within the estimated timeout. In such a situation, it decreases the congestion window to one maximum segment size (MSS), and under other cases it increases the congestion window by one MSS. There also exists a congestion window threshold, which is set to half the congestion window size at the time when a re-transmit was required.

   The inherent assumption in this mechanism is that lack of an acknowledgement is due to network congestion. If a packet, however, is lost by the network for reasons other than network congestion, then waiting for the timer to run out is wasteful. This is a situation that may happen quite frequently in wireless networks.

10.4.4 ATM ABR CONGESTION CONTROL

10.4.4.1 What is ATM ?

Asynchronous Transfer mode(ATM), sometimes referred to as cell relay. ATM can be viewed as an evolution from frame relay. The most obvious difference between frame relay and ATM is that frame relay uses variable-length packets, called frames, and ATM uses fixed-length packets called cells. ATM is a very complex technology, perhaps the most complex ever developed by the networking industry. While the structure of ATM cells and cell switching do facilitate the development of hardware intensive, high performance ATM switches, the deployment of ATM networks requires the overlay of a highly complex, software intensive, protocol infrastructure.

Such as its connection oriented nature, which contributes to the complexity of ATM protocols. The fact that ATM is connection-oriented implies the need for ATM specific signaling protocols and addressing structures, as well as protocols to route ATM connection requests across the ATM network. These ATM protocols, in turn, influence the manner in which existing higher layer protocols can operate over ATM networks.

10.4.4.2 Service categories

ATM was modified to explicitly list the service categories commonly used in order to allow equipment vendors to optimize their adaptors boards and switches for some or all of these categories. These service categories can be defines as follows:

1. **Continuous Bit Rate[CBR] :** End systems would use CBR connection types to carry constant bit rate traffic with a fixed timing relationship between data samples, for circuit emulation.
2. **Variable Bit Rate-Real Time[(VBR(RT)]:** The VBR(RT) service class is used for connections that carry variable bit rate traffic , in which there is a fixed timing relationship between samples. For such applications as variable bit rate video compression.
3. **Variable Bit Rate—Non-Real Time[(VBR(NRT)]:** The VBR(NRT) service class is used for connections that carry variable bit rate traffic in which there is no timing relationship between data samples, but a guarantee of QoS is still required.
4. **Available Bit Rate[ABR] :**The ATM forum is currently focusing its work on the ABR service. ABR supports variable rate data transmissions and does not preserve any timing relationships between source and destination. Available bit rate(ABR) service category is designed for bursty traffic whose bandwidth range is known roughly. The ABR service does not provide any guaranteed bandwidth to the user. Rather, the network provides a "best effort" service, in which feedback flow control mechanisms is used to increase the bandwidth available to the user. Through such flow control mechanisms, the network can control the amount of traffic that it allows into the network, and minimize cell loss within the network due to congestion.

10.4.4.3 Rate based congestion control

The ATM forum is currently working on a "rate based" mechanism for ABR congestion control, where Resource Management (RM) cells or the explicit forward congestion indication bit within ATM cells are used to indicate the presence of congestion within the network to the source system. A specified traffic algorithm is used at the source to control the traffic rate into the network, based either upon the number of RM cells received with a congestion indication or an explicit rate indication from the network. ABR is designed to map to existing LAN protocols that opportunistically use as much bandwidth as is available from the network, but can either back off, or be buffered in the presence of congestion . With ABR traffic , it is possible and reasonable for the network to signal one or more senders and ask them to slow down temporarily until the network can recover.

10.4 QUALITY OF SERVICE

QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. QoS is especially important for the new generation of Internet applications such as VoIP, video-on-demand and other consumer services. Some core networking technologies like Ethernet were not designed to support prioritized traffic or guaranteed performance levels, making it much more difficult to implement QoS solutions across the Internet.

Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN, and service provider networks. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

10.5.1 Approaches to QoS support

Fundamentally, QoS enables you to provide better service to certain flows. QoS involves prioritization of network traffic. This is done by either raising the priority of a flow or limiting the priority of another flow. When using congestion-management tools, you try to raise the priority of a flow by queuing and servicing queues in different ways. The queue management tool used for congestion avoidance raises priority by dropping lower-priority flows before higher-priority flows. There are number of techniques to improve the Quality of service, which are as follows:

1. **Scheduling:** A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling technique are designed to improve the quality of service . for example, in First-in First-out queuing packets wait in a buffer (queue) until the node is ready to process them. In Priority queuing , packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest queue are processed first.
2. **Traffic Shaping:** It is a mechanism to control the amount and the rate of the traffic sent to the network. For example, a leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full. And in the token bucket , it allows bursty traffic at a regulated maximum rate.
3. **Resource reservation:** A flow of data needs resources such as a buffer, bandwidth , CPU time and so on .The Quality of service is improved if these resources are reserved beforehand.
4. **Admission control:** It refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications.

10.6 ATM AAL LAYER PROTOCOLS

The use of Asynchronous Transfer Mode (ATM) technology and services creates the need for an adaptation layer in order to support information transfer protocols, which are not based on ATM. This adaptation layer defines how to segment and reassemble higher-layer packets into ATM cells, and how to handle various transmission aspects in the ATM layer. The AAL is also responsible for isolating higher-layer protocols from the details of the ATM processes.

Examples of services that need adaptations are Gigabit Ethernet, IP, Frame Relay, SONET/SDH, UMTS/ Wireless, etc.

The main services provided by AAL (ATM Adaptation Layer) are:

- Segmentation and reassembly
- Handling of transmission errors
- Handling of lost and misinserted cell conditions
- Timing and flow control

The following ATM Adaptation Layer protocols (AALs) have been defined by the ITU-T. It is meant that these AALs will meet a variety of needs. The AAL layer is orgainized in two logical sublayers : the convergence sublayer(CS) and segmentation and reassembly sublayer(SAR) . the convergence sublayer provides the functions needed to support specific applicatios using AAL. Each AAL user attaches to AAL at a service access point(SAP), which is simply the address of the application. The classification is based on whether a timing relationship must be maintained between source and destination, whether the application requires a constant bit rate, and whether the transfer is connection oriented or connectionless.

The following ATM Adaptation Layer protocols (AALs) have been defined for Asynchronous Transfer Mode(ATM). These protocols are loosely associated with the various classes of traffic expected to be carried:

- **AAL 1 :** Supports constant bit rate, connection-oriented, synchronous traffic (e.g., uncompressed voice).
- **AAL 2 :** Definition never completed, but was envisioned to be assigned for variable bit rate, connection-oriented, synchronous traffic.
- **AAL 3/4 :** Supports variable bit rate, connection- oriented, asynchronous traffic (e.g., X.25 data) or connectionless packet data (e.g., SMDS traffic) with an additional 4-byte header in the information payload of the cell.
- **AAL 5 :** Similar to AAL 3/4 with a simplified information header scheme; this AAL assumes that the data is sequential from the end user and uses the PTI bit to indicate the last cell in a transmission Examples of services that use AAL 5 are Classic IP over ATM, and LAN Emulation (LANE). AAL 5 is the most widely used ATM Adaptation Layer Protocol.

10.7 STREAM CONTROL TRANSMISSION PROTOCOL(SCTP)

In computer networking, the **Stream Control Transmission Protocol** (SCTP) is a Transport Layer protocol, serving in a similar role as the popular protocols Transmission Control Protocol(TCP) and User Datagram Protocol (UDP). Indeed, it provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with congestion control.

SCTP is new reliable, message oriented transport layer protocol. It is mostly designed for Internet applications that have recently been introduced. SCTP applications submit their data to be transmitted in messages (groups of bytes) to the SCTP transport layer. SCTP places messages and control information into separate *chunks* (data chunks and control chunks), each identified by a *chunk header*. A message can be fragmented over a number of data chunks, but each data chunk contains data from only one user message. SCTP chunks are bundled into SCTP packets. The SCTP packet, which is submitted to the Internet Protocol, consists of a packet header, SCTP control chunks when necessary, followed by SCTP data chunks when available.

TCP preserves byte order in the stream by assigning a sequence number to each packet. SCTP, on the other hand, assigns a sequence number to each *message* sent in a stream. This allows independent ordering of messages in different streams. However, message ordering is optional in SCTP; a receiving application may choose to process messages in the order they are received instead of the order they were sent.

The term *multi-streaming* refers to the capability of SCTP to transmit several independent streams of chunks in parallel, for example transmitting Web page images together with the Web page text. In essence, it is the bundling of several connections into a single SCTP association, operating on messages (or chunks) rather than bytes.

Features of SCTP :

- **Multihoming : -** An SCTP support in which one (or both) endpoints of a connection can consist of more than one IP address. The sending and receiving host can define multiple IP addresses in each end for an association. In this fault-tolerant approach , when one path fails, another interface can be used for data delivery without interruption.
- **Multiple Streams** — We know that TCP is a stream-oriented protocol. The problem with this approach is that a lost at any point in the stream blocks the delivery of the rest of the data. But SCTP allows multi-stream service in each connection, which is called association in SCTP terminology. If one of the streams is blocked , the other stream can still deliver their data.
- **Path Selection and Monitoring** — selects a "primary" data transmission path and tests the connectivity of the transmission path.
- **Validation and acknowledgment mechanisms** — Protect against flooding attacks and provides notification of duplicated or missing data chunks. In SCTP, acknowledgement numbers are used to acknowledge only data chunks. Control chunks are acknowledged by other control chunks if necessary.

- **Improved error detection suitable for jumbo Ethernet frames-** Like TCP, SCTP implements error control to provide reliability. TSN numbers and acknowledgement numbers are used for error control.

10.8 SUMMARY

In this module we have discussed the Transport service and mechanism .

- Transport layer provides reliable, transparent transfer of data between end points. It also provides end-to-end error recovery and flow control.
- Transmission control Protocol(TCP) is one of the transport layer protocols in the TCP/IP suite.
- A TCP connection normally consists of three phases: connection establishment, data transfer and connection termination.
- UDP is a connectionless, unreliable transport layer protocol.
- The UDP packet is called a user datagram.
- Congestion control refers to the mechanisms and techniques to control congestion and keep the load below capacity.
- A flow can be characterized by its reliability, delay, jitter and bandwidth.
- ATM can handle real-time transmission.
- SCTP is a message-oriented, reliable protocol that combines the good features of UDP and TCP.
- SCTP provides flow control, error control and congestion control.

10.9 GLOSSARY

Client : A running program on a local site that requests service from a running application program on a remote site.

Server: A program that can provide services to other programs called clients.

Reliability : A QoS flow characteristic, dependability of the transmission.

Multiplexing : The process of combining signals from multiple sources for transmission across a single data link.

Transmission Control Protocol: A transport protocol in the TCP/IP protocol suite.

User Datagram Protocol: A connectionless TCP/IP transport layer protocol.

Congestion: Excessive network or internetwork traffic causing a general degradation of service.

Quality of Service: A set of attributes related to the performance of the connection.

10.10 FURTHER READINGS

1. Andrew S. Tanenbaum, *Computer Networks*, 4/e, Pearson education, 2003.
2. Behrouz A. Fourouzan, *Data Communicatios and networking*, 2/e Tata McGrawhill, 2000.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson education, 2002 .
4. Larry L. Peterson and Bruce S. davie, Computer Networks, 4/e Morgan Kaufmann,2008.
5. Richard Stevens. W,TCP/IP Utilities-Vol. I, the protocols, Addison Wesley, 1994.
6. http://en.wikipedia.org/wiki/Transport_Layer
7. http ://www.linuxsecurity.com/docs/PDF/cisco-understanding-tcpip.pdf

10.11 ANSWER TO SELF LEARNING EXERCISES

1. The maximum size of a UDP datagram
2. Do port addresses need to be unique? Why or why not.
3. The maximum and minimum size of the TCP header.
4. Compare the TCP header and the UDP header.
5. Definition of burst data .

6. Traffic descriptor, Traffic shaping.
7. Mechanism to alleviate congestion.

10.12 UNIT END QUESTIONS

1. Explain how TCP provides reliable service when the underlying IP layer provides best effort service.
2. Why a three-way handshake is preferred to a two way handshake for connection establishment by a transport entity residing over an unreliable network entity?
3. What is slow start mechanism ? Explain how it plays a role in congestion control ?
4. What is the difference between open-loop congestion control and closed-loop congestion control ?
5. What are four general techniques to improve Quality of service?
6. Enumerate and explain the seven issues that TCP must address.
7. What is the total efficiency of ATM using AAL1?
8. In a connection, the value of cwnd is 2500 and the value of rwnd is 4500. the host has sent 2000 bytes which has not been acknowledged . How many more bytes can be sent?

UNIT 11

APPLICATION LAYER AND NETWORK SECURITY

Structure of the Unit

11.1 OBJECTIVE

After studying this unit , you will learn

- Application layer protocol
- World Wide Web(WWW)
- Hyper Text Transfer Protocol(HTTP)
- File Transfer Protocol(FTP)
- Domain Name System(DNS)
- Simple Mail Transfer Protocol(SNMP)

- Simple Network Management Protocol(SNMP)
- Network Security
- Security in different layers.

11.2 INTRODUCTION

We briefly discuss the application layer that enables the user , whether human or software , to access the network. It also provides user interfaces and support for services such as e-mail, file access and transfer , access to system resources , surfing the WWW , and network management . we begin this module by giving the description of application layer protocols: HTTP, FTP& SNMP .

11.2.1 What is Application layer?

Application layer provides access to the OSI environment for users and also provides distributed information services. There are applications consisting of application processes that perform information processing. An aspect of theses application processes and the protocols by which they communicate comprise the Application Layer as the highest layer of the architecture.

11.2.2 TYPES OF SERVICES

There are specific services provided by the application layer include the following :

- **Network virtual terminal :** A network virtual terminal is a software of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host.
- **File transfer, access and management:** this application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services :** the application provides the basis for email forwarding and storage.
- **Directory services :** the application layer provides distributed database sources and access for global information about various objects and services.

11.2.3 APPLICATION LAYER PROTOCOLS

Application Layer is a term used in categorizing protocols and methods in architectural models of computer networking. Both the OSI model and the Internet Protocol Suite (TCP/IP) contain an application layer.

In TCP/IP, the Application Layer contains all protocols and methods that fall into the realm of process-to-process communications via an Internet Protocol (IP) network using the Transport Layer protocols to establish underlying host-to-host connections.

The common application layer services provide semantic conversion between associated application processes. *Note:* Examples of common application services of general interest include the virtual file, virtual terminal, and job transfer and manipulation protocols. Application layer contains a variety of protocols that are commonly needed. It contains all the higher-level protocols . the early ones included virtual terminal(TELNET) , file transfer protocol(FTP) and electronic mail(SMTP). The virtual terminal protocol allows a user on one machine to log into a distant machine and work there. The file transfer provides a way to move data more efficiently from one machine to another machine. Electronic mail is used for this purpose. Many other protocols have been added to these over the years , such as the Domain Name service(DNS) for mapping host names onto their network addresses. And HTTP for fetching pages on the World wide web, and many others.

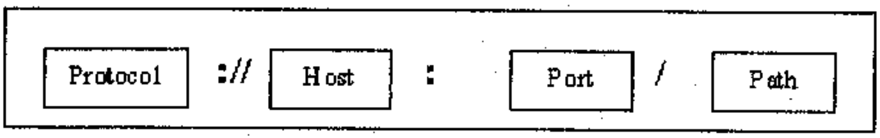
11.3 WORLD WIDE WEB(WWW)

Many people use the terms *Internet* and *World Wide Web* (or just the *Web*) interchangeably, but these terms are not synonymous. The Web(known as WWW) began in 1989 at CERN, the European center for nuclear research. The World Wide Web is a huge set of interlinked documents, computer graphics and other resources, linked by hyperlink and URLs. These hyperlinks and URLs allow the web servers and other machines that store originals, and cached copies of these resources to deliver them as required using HTTP (Hypertext Transfer Protocol). HTTP is only one of the communication protocols used on the Internet.the WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

Software products that can access the resources of the Web are correctly termed user agents . In normal use, web browsers, such as Internet Explorer, Firefox and Apple safari, access web pages and allow users to navigate from one to another via hyperlinks. Web documents may contain almost any combination of Computer data including graphics, sounds, plain text, web video, multimedia and interactive content including web game, office applications and scientific demonstrations.

The Web is basically a client-server system, in which a client using a browser can access a service using a server. And the services provided is distributed over many locations called sites. Where each site holds one or more documents, referred to as Web pages. The pages can be retrieved and viewed by using browser. Here client sends a request through its browser, a program that is designed to fetch Web documents . the server finds the document and sends it to the client.

1. **Client (Browser) :** Each client(browser) usually consists of three parts : a controller, a client protocol and interpreters. Where the controller receives input from the keyboard or the mouse . the client protocol can be one of the protocols such as FTP or HTTP . the interpreter can be HTML , Java, JavaScript, depending on the type of document.
2. **Server :** The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. A server can also become more efficient through multithreading or multiprocessing.
3. **Uniform Resource Locator(URL) :** a client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world , HTTP uses locators. The Uniform resource locator(URL) is a standard for specifying any kind of information on the internet. Every document on the internet has a unique uniform resource locator .URL is the way to represent site name on the world wide web . URL's are similar to postal addresses or telephone numbers which are used to represent the destination. all URL's consists of four parts:



1) Service type (Protocol) : the protocol is the client-server program used to retrieve
2) Host or domain name (Host)
3) Directory or subdirectory information (Port) and
4) Filename (Path)

For example : we have a URL "**http: // www.google.com/books/children.html**" . this URL can be described as:

http : it defines the address of Internet server that uses the Hypertext transfer protocol.

www : it signifies that the site is part of the World wide web.

google : the secondary domain name

Com : the top level domain signifying a commercial site.

Books : it signifies folder where webpage is located.

Children : it specifies actual page

Html: it defines the type of file

4. **Cookies :** A string of characters that hold some information about the client and must be returned to the server untouched.The creation and storage of cookies depend on the implementation. When

a server receives a request from a client, it stores information about the client in a file or a string, the this information may include the domain name of the client, the contents of the cookies(information the server has gathered about the client such as name, registration number and so on). The contents of the cookie are never read by the browser or disclosed to the user. It is a cookie made by the server and eaten by the server.

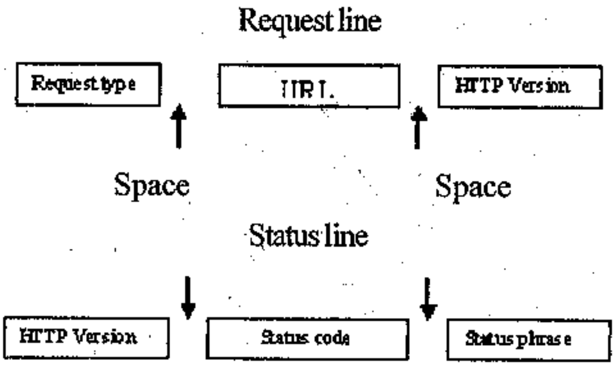
11.4 HYPERTEXT TRANSFER PROTOCOL (HTTP)

HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. Its use for retrieving inter-linked resources led to the establishment of the World Wide Web.

HTTP development was coordinated by the World Wide Web Consortium and the Internet Engineering Task Force (IETF), culminating in the publication of a series of Requests for Comments , most notably , which defines HTTP/1.1, the version of HTTP in common use.

HTTP is a request/response standard of a client and a server. A client is the end-user, the server is the web site. The client making a HTTP request—using a web browser, spider, or other end-user tool—is referred to as the *user agent*. The responding server—which stores or creates *resources* such as HTML files and images—is called the *origin server*. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels. HTTP is not constrained to using TCP/IP and its supporting layers, although this is its most popular application on the Internet. Indeed HTTP can be "implemented on top of any other protocol on the Internet, or on other networks". HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used.

Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connection to a particular port on a host (port 80 by default; see List of TCP and UDP port numbers). An HTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back a status line, such as "HTTP/1.1 200 OK", and a message of its own, the body of which is perhaps the requested resource, an error message, or some other information. All the new versions of HTTP support two kinds of requests: simple requests and full requests. A simple request is just a single GET line naming the page desired, without the protocol version. The response is just the raw page, with no headers, no MIME and no encoding. Full requests are indicated by the presence of the protocol version on the GET request line. Requests may consist of multiple lines, followed by a blank line to indicate the end of the request. The first line in a request message is called a request line, the first line in the response message is called the status line.



Resources to be accessed by HTTP are identified using Uniform Resource Identifiers (URIs)—or, more specifically, Uniform Resource Locators (URLs)—using the http: or https URI schemes.

11. 5 FILE TRANSFER PROTOCOL(FTP)

Copying files from one machine to another machine is one of the most frequently used operations. The data transfer between client and server can be in either direction . **File Transfer Protocol** (**FTP**) is a standard Network Protocol used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet. FTP is built on a Client-server architecture and utilizes separate control and data connections between the client and server applications. Client applications were originally interactive command-line tools with a standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. FTP is also often used as an application component to automatically transfer files for program internal functions. FTP can be used with user-based password authentication or with anonymous user access.

FTP uses TCP as a transport protocol to provide reliable end-to-end connections. Two connections are used : the first is for login and follows the TELNET protocol and the second is for managing the data transfer.

- To promote sharing of files (computer programs and/or data).
- To encourage indirect or implicit use of Remote computer.
- To shield a user from variations in file storage systems among different Server.
- To transfer data reliably, and efficiently.

FTP differs from other client-server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Sepration of commands and data trasfer makes FTP more efficient. FTP uses two well known TCP ports ; port 21 is used for the control connection, and port 20 is used for the data connection . The two FTP connections, control and data, use different strategies and different port numbers.

11.5.1 Command Processing

FTP uses the control connection to establish a communication between the server control process and the client control process. During this communication, the commands are sent from the client to the server and the responses are sent from the server to the client.

1) **Commands :** commands , which are sent from the FTP client control process, are in the form of ASCII uppercase, which may or may not be followed by an argument. We can roughly divide the commands into Six groups: access command, file management commands, data formatting commands, port defining commands, file transferring commands and miscellaneous commands.

   a) **Access command :** These commands let the user access the remote system. For example: USER(for User id) , PASS(for User password), ACCT(for account information),QUIT(for logout of the system) etc.

   b) **File management commands:** these commands let the user access the file system on the remote computer. They allow the user to navigate through the directory structure, create new directory, delete files and so on. For example: CWD(change to another directory), DELE(delete a file), RMD(delete a directory), RNTO(rename the file) etc.

   c) **Data formatting commands:** these comands let the user define the data structure, file type, and transmission mode. For example: TYPE(define the file type), MODE(define the transmission mode) etc.

   d) **Port defining commands:** theses commands define the port number for the data connection on the client. For example: PORT(client chooses a port) , PASV(server chooses a port).

   e) **File transfer commands:** these commsnds actually let the user transfer files. For example: RETR(retrieve files), STOR(store files) etc.

   f) **Miscellaneous commands:** theses commands deliver information to the FTP user at the client site. For example: HELP,NOOP(check if server is alive), SITE etc.

2) **Responses:** Every FTP command generates at least one response. A response has two parts; a three digit number followed by text. The numeric part defines the code and the text part defines needed parameters. The responses can be defined as:

   a) **Positive preliminary reply:** the action has started . the server will send another reply before accepting another command.

b) **Positive completion reply:** the action has been completed . the server will accept another command.

c) **Transient negative completion reply:** the action did not take place, but the error is temporary.

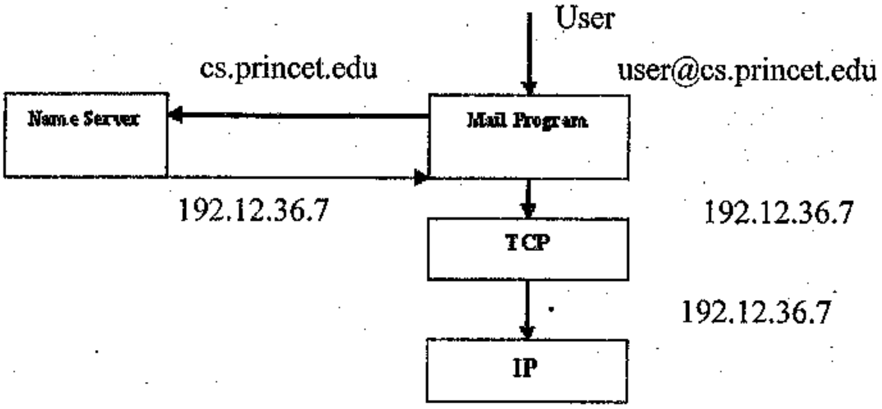
d) **Permanenet negative completion reply:** the command was not accepted and should not be retried again.

11.6 DOMAIN NAME SYSTEM

We know that the client/server programs can be divided into two categories : those that can be directly used by the user, such as an e-mail, and those that support other application programs. The **Domain Name System (DNS)** is a supporting program that is used by other programs such as an e-mail. The DNS protocol was developed and defined in the early 1980s and published by the Internet Engineering Task Force. A DNS program can support an e-mail program to find the IP address of an e-mail recipient. A user of an e-mail program may know the email address of the recipient , the IP protocol needs the IP address. The DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address. The **Domain Name System (DNS)** is a hierarchical naming system for computers, services, or any resource participating in the Internet. It associates various information with domain names assigned to such participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices world-wide. For example, *www.example.com* translates to *208.77.188.166.*

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed, fault tolerant, and helped avoid the need for a single central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a world-wide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet. The Internet is divided into several hundred top-level domains, where each domain covers many hosts. Each domain is partitioned into sub-domains, and these are further partitioned , and so on. All theses domains can be represented by a tree , where the leaves of the tree represent domains that have no sub-domains. A leaf domain may contain a single host, or it may represent a company and contains thousands of hosts.



Names translated into addresses

A name space that maps each address to a unique name can be organized in two ways:

Flat name space: In a flat name space , a name is assigned to an address. A name in this space is a sequence of characters without structure. The names may or may not have a common section; if they do, it has no meaning. The main disadvantage of a flat name space is that it can not be used in a large system such as the Internet.

Hierarchical name space: In a hierarchical name space, each name is made of several parts. The first part can define the nature of the organization, the second part can define the name of the organization , the third part can define departments in the organization, and so on. In this case the authority to assign and control the name spaces can be decentralized. The central authority can assign the part of the name that defines the nature of the organization and the name of the organization. The responsibility of the rest of the name can be given to the organization itself. In the mid- 1980s , the domain naming system was put into place. DNS employs a hierarchical namespace rather than a flat name space, and the "table" of bindings that implements this name space is partitioned into disjoint pieces and distributed throughout the Internet

11.7 SIMPLE MAIL TRANSFER PROTOCOL(SMTP)

We know that Electronic mail(E-mail) is probably the most widely used TCP/IP application. To send a mail, a system must have the client, and to receive mail, a system must have a server. The formal protocol that defines the client and server in the internet is called the Simple mail transfer protocol(SMTP). SMTP protocol is used to transfer messages from one host to another. Since the start the SMTP has traditionally been limited to the delivery of simple text messages. In recent years, there has been a demand for the capability of delivery mail containing various types of data, including voice, images and video clips. SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.

SMTP is based on end-to-end delivery, an SMTP client will contact the destination host's SMTP server directly to deliver the mail. It will keep the mail item being transmitted until it has been successfully copied to the recipients SMTP. In various implementations there is a possibility to exchange mail between the TCP/IP SMTP mailing system and the locally used mailing systems. These applications are known as mail gateways or mail bridges. Each SMTP message can be defined as :

1. A header, or envelope , the structure which is strictly defined by RFC 822. the mail header is terminated by a null line.
2. contents everything after the null line is the message body which is a sequence of lines containing ASCII characters .

The basic idea is that the multiple formats and styles preferred by humans in the user interface are replaced by a standardized list suitable for the SMTP send program. The ***SMTP sender*** takes messages from the outgoing mail queue and transmits them to the proper destination host via SMTP transactions over one or more TCP connection to port 25 on the target hosts. The SMTP sender must deal with a variety of errors. The ***SMTP protocol*** is used to transfer a message from the SMTP sender to the SMTP receiver over a TCP connection. SMTP attempts to provide reliable operation but does not guarantee to recover from lost messages. It is generally considered reliable. The SMTP receiver accepts each arriving message and either places it in the appropriate user mailbox or copies it to the local outgoing mail queue if forwarding is required. The SMTP receiver must be able to verify local mail destinations and deal with errors , including transmission errors and lack of disk file capacity.

The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and receiver. The initiative is with the SMTP sender, who establishes the TCP connection. Once the connection is established , the SMTP sender sends **commands** over the connection to the receiver. Each command generates exactly one reply from the SMTP receiver is called **response**.

Each command consists of a single line of text, beginning with a four-letter command code followed in some cases by an argument field. Most replies are a single line, although multiple-line replies are possible. Each reply begins with a three digit code and must be followed by additional information. The leading digit indicates the category of the reply which is as follows:

a) **Positive completion reply :** the requested action has been successfully completed. A new request may be initiated.

b) **Positive intermediate reply :** the command has been accepted, but the requested action is being held in abeyance, pending receipt of further information.

c) **Transient negative completion reply:** the command was not accepted and the requested action did not occur. However, the error condition is temporary and the action may be requested again.

d) **Permanent negative completion reply :** the command was not accepted and the requested action did not occur.

Basic SMTP operation occurs in three phases : connection setup, exchange of one or more command-response pairs, and connection termination.

Connection setup:- an SMTP sender will attempt to set up a connection with a target host when it has one or more mail messages to deliver to that host.

Mail transfer: once the connection has been established, the SMTP sender may send one or more messages to the SMTP receiver.

Connection closing: The SMTP sender closes the connection in two steps. First, the sender send a QUIT command and waits for reply, . the second step is to initiate a TCP close operation for the TCP connection. The receiver initiates its TCP close after sending its reply to the QUIT command.

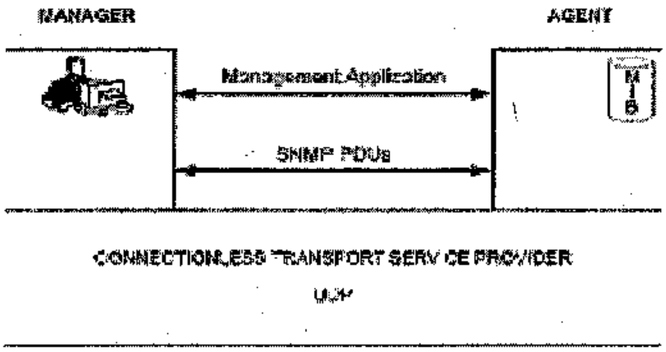
11.8 SIMPLE NETWORK MANAGEMENT PROTOCOL(SNMP)

We know that a Network is a complex system, both in terms of the number of nodes that are involved and in terms of the suite of protocols that can be running on any node. The nodes we want to keep track of are distributed, our only real option is to use the network to manage . this means we need a protocol that allows us to read, and possibly write, various pieces of state information on different network nodes . the most widely used protocol for this purpose is the Simple Network Management Protocol(SNMP).

SNMP is essentially a specialized request/reply protocol that supports two kinds of request messages : GET and SET. The former is used to retrieve a piece of state from same node, and the latter is used to store a new piece of state in same node. A system administrator interacts with a client program that displays information about the network. This client program usually has a graphical interface. Whenever the administrator selects a certain piece of information that user wants to see, the client program uses SNMP to request that information from the node in question. An SNMP server running on that node receives the request, locates the appropriate piece of information, and returns it to the client program, which then displays it to the user. An SNMP-managed network consists of three key components:

- Managed device
- Agent
- Network management system (NMS)

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be any type of device including, but not limited to routers, Network access server, Network switch, Network bridge, Network hub, IP phone, Host(network) and computer printer. An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.



A Network management system (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

SNMP is part of the Internet network management architecture. To do management tasks, SNMP uses two protocols : **Structre of management information (SMI)** and **Management Information Base (MIB)** . In other words management on the Internet is done through the coorporation of the three protocols SNMP, SMI and MIB. SNMP has very specific roles in network management. It defines the format of the packet to be sent from a manager to an agent and vice versa. The packets exchanged contain the object(variable) names and their status(values). SNMP is responsible for reading and changing these values. To use SNMP , we need rules for naming objects . The SMI defines the rules for describing management information. This is important because the objects in SNMP form a hierarchical structure (an object may have a parent object and some children objects). We must know that SMI only defines the rules, it does not define how many objects are managed in an entity or which object uses which type. So we can say that SMI is a collection of general rules to name objects and to list their types . for each entity to be managed , MIB protocol must define the number of objects, name them according to the rules defined by SMI , and associate a type to each named object. This protocol is MIB. MIB creates a set of objects defined for each entity similar to a database. It is also responsible for finding the object that holds the number of the UDP user datagrams received.

11.9 MULTIMEDIA

A multimedia system is the computer controlled, integrated production, manipulation, presentation, storage and communication of independent information that is encoded at least through continuous (time-dependent) and discrete(time-independent) systems. Actually "it is a combination of text, graphics, sound, animation and video elements along with the computer acting as a brain so that the user has total control over what is heard or seen"

Multimedia systems now have enormous capabilities in terms of the physical componenets that make up such a system. Both the hardware and the software contribute to the complexity of a multimedia system.

Multimedia is widely used in various applications, with growing competition and new and better products introduced in the market every day. Multimedia applications can be shown as:

1) Multimedia and communication technology
2) Entertainment
3) Edutainment
4) Business communication
5) Public access
6) Publishing industry

We know that people want to use the Internet not only for text and image communications, but also for audio and video services. We can divide audio and video services into three broad categories: **Streaming stored audio/video, Streaming live audio/video** and **Interactive audio/video.** Streaming means a user can listen the file after the downloading has started. Streaming stored audio/video refers to on-demand request for compressed audio/video files. Streaming live audio/video refers to the broadcasting of radio and TV programs through the Internet. Interactive audio/video refers to the use of the internet for Interactive audio/video applications.

Audio and video compression

To send audio and video over the Internet requires compression.

1) **Audio compression :** Audio compression can be used for speech or music. For speech, we need to compress a 64-kHz digitized signal. For music we need to compress a 1.411-MHz signal. two categories of techniques are used for audio compression: predictive encoding and perceptual encoding.

   a) Predictive Encoding: In predicive encoding, the difference between the samples are encoded instead of encoding all the sampled vales. This type of compressio is normally used for speech.

   b) Perceptual Encoding (MP3): the most common compression technique that is used to create CD-quality audio is based on the perceptual encoding techniques. MP3 and a part of the MPEG standard uses this technique.

2) **Video compression:** we know that video is composed of multiple frames. Each frame is one image. We can compress video by first compressing images. Two standards are prevalent in the market. Joint Photographic Experts Group(JPEG) is used to compress images. Moving Picture Experts Group(MPEG) is used to compress video.

   a) Image compression(JPEG) : If the picture is not in color(gray scale), each pixel can be represented by an 8-bit integer(256 levels). If the picture is in color, each pixel can be represented by 24 bits(3*8 bits), with each 8-bits representing red, blue or green(RGB). The whole idea of JPEG is to change the picture into a linear(vector) set of numbers that reveals the redundancies. The redundancies(lack of chane) can then be removed by using the text compression methods.

   b) Video compression(MPEG) : this method is used to compress video. In principle, a motion picture is a rapid flow of a set of frames, where each frame is an image. In other words, a frame is a spatial combination of pixels and a video is a temporal combination of frames that are sent one after another. Compressing video, that, means spatially compressing each frame and temporally compressing a set of frames.

11.10 REMOTE PROCEDURE CALL

RPC is actually more than just a protocol – it is a popular mechanism for structuring distributed system. RPC is popular because it is based on the sematics of a local procedure call, the application program makes a call into a procedure without regard for whether it is local or remote and blocks until the call returns. When the procedures being called are actually methods of remote objects in an object-oriented language, RPC is known as remote method invocation(RMI). While the RPC concept is simple, there are two main problems that make it more complicated than local procedure calls:

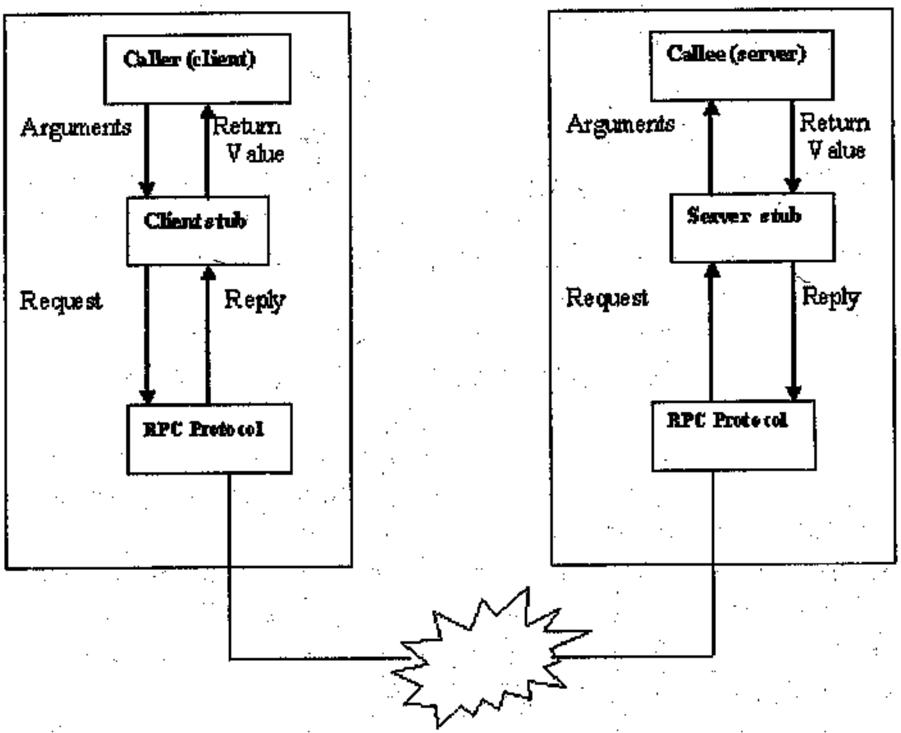
1) The network between the calling process and the called process has much more complex properties than the backplane of a computer

2) The computer on which the calling and called processes run may have significantly different architectures and data representation formats.

thus a complete RPC mechanism actually involves two major components:

1) A protocol that manages the messages sent between the client and the server processes and then deals with the potentially undesirable properties of the underlying network.

2) Programming language and compiler support to package the arguments into a request message on the client machine and then to translate this message back into the arguments on the server machine, with the return value.



In RPC, the client calls a local stub for the procedure, passing it the arguments required by the procedure. This stub hides the fact that the procedure is remote by translating the arguments into a request message and then invoking an RPC protocol to send the request message to the server machine. At the server, the RPC protocol delivers the request message to the server stub, which translates it into the arguments to the procedure and then calls the local procedure. After the server procedure completes, it returns the answer to the server stub.

Two functions that must be performed by any RPC protocol are:

a) Provide a name space for uniquly identifying the procedure to be called.

b) Match each reply message to the corresponding request message.

11.11 SECURITY IN COMPUTER NETWORKS

No one can deny the importance of security in data communications and networking. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message.
- Some secret information shared by the two principals and it is hoped, unknown to the opponent.

Security in networking is based on cryptography.

11.11.1 Principles of Cryptography

Suppose that someone wants to send a message to a receiver, and wants to be sure that no-one else can read the message. However, there is the possibility that someone else opens the letter or hears the electronic communication.

Cryptography can provide several aspects of security related to the interchange of messages through networks. Theses aspects are confidentiality , integrity, authentication and nonrepudiation. Cryptography can also be used to authenticate the sender and receiver of the message to each other. Cryptography, a word with Greek origins, means "secret writing". So we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

In Cryptographic terminology, the message is called **plaintext** or **cleartext**. Encoding the contents of the message in such a way that hides its contents from outsiders is called **encryption**. The encrypted message is called the **ciphertext**. The process of retrieving the plaintext from the ciphertext is called **decryption**. Encryption and decryption usually make use of a **key**, and the coding method is such that decryption can be performed only by knowing the proper key.

There are two classes of key-based encryption algorithms, **Symmetric** (or **secret-key**) and **Asymmetric** (or **public-key**) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

11.11.1.1 Symmetric Key

Symmetric key algorithms can be divided into **stream ciphers** and **block ciphers**. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

Modern cryptographic algorithms are no longer pencil-and-paper ciphers. Strong cryptographic algorithms are designed to be executed by computers or specialized hardware devices. In most applications, cryptography is done in computer software. Generally, symmetric algorithms are much faster to execute on a computer than asymmetric ones.

we normally use symmetric-key cryptography in our network security, which were character-oriented . but today's ciphers are much more complex, which are bit-oriented.

1) **Traditional Ciphers :** traditional ciphers are character-oriented. Although these are now obsolete. We can divide traditional ciphers into two broad categories: **substitution ciphers and transposition ciphers.**

   a) **Substitution Ciphers:** It substitutes one symbol with another. If the symbol in the plain text are alphabetic characters, we replace one character with another. For example we can replace character A with S and D with P and so on.

   b) **Transposition Ciphers:** In a transposition cipher, there is no substitution of characters, instead , their locations change. A character in the first position may appear in the eighth position. Or we can say that a transposition cipher reorders symbols in a block of symbols.

2) **Simple Modern Ciphers:** we know that traditional ciphers are character-oriented. With the advent of the computer, ciphers need to be bit-oriented.

   a) **Substitution cipher(S-box) :** an S-box(substitution box) parallels the traditional substitution cipher for characters. The input to an S-box is a stream of bits with length N, the result is another stream of bits with length M.

   b) **Transposition cipher(P-box):** a P-box(permutation box) for bits parallels the traditional transposition cipher for characters. It performs a transposition at the bit-level. It transposes bits

3) **Modern Round ciphers:** the ciphers of today are called round ciphers because they involve multiple rounds. The key used in each round is a subset of the general key called the round key. We introduce two modern symmetric-key ciphers: DES and AES. These ciphers are referred to as block ciphers.

a) **Data Encryption Standard(DES) :** it was designed by IBM. The algorithm encrypts a 64-bit plaintext block using a 64-bit key. DES has two transposition blocks(P-box) and 16 complex round ciphers. Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key. The initial and final permutations are keyless straight permutations that are the inverse of each other. The DES function applies a 48-bit key to the rightmost 32 bits Ri to produce a 32-bit output. This function is made up of four operations: an XOR, an expansion permutation, a group of S-boxes and a P-box.

b) **Advanced Encryption Standard(AES) :** the Advanced Encryption Standard (AES) was designed because DES's key was too small. AES is designed with three key sizes: 128, 192 or 256 bits. AES has 10 round, 128-bit key configuration. The structure and operation of the other configuration are similar. There is an initial XOR operation followed by 10 round ciphers. The last round is slightly different from the preceding rounds; it is missing one operation.

11.11.1.2 Asymmetric-key cryptography :

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys-one a public key and one a private key. It is also known as public-key encryption. Asymmetric encryption transforms plaintext into cipher text using a one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plain text is recovered from the cipher text.

Asymmetric encryption can be used for confidentiality , authentication, or both. The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite number.

a) **RSA :** the most common public key algorithm is RSA, named for its inventors **Rivest, Shamir, and Adleman(RSA).** It uses two numbers e, d as the public and private key.

The two keys, e, d have a special relationship to each other. This relationship can be defined as

Receiver use the following steps to select the private and public keys:

1. receiver chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.
2. receiver multiples the two primes to find n, the modulus for encryption and decryption , as **$n=p'q$.**
3. receiver calculates another number **$\phi=(p-1)\times(q-1)$.**
4. receiver chooses a random integer e. It then calculates d so that **$d\times e=1 \bmod \phi$**
5. receiver announces e and n to the public. It keeps ϕ and d secret.

Encryption: anyone who needs to send a message to receiver can use n and e. sender can calculate the cipher text using this formula: **$C=P^e(\text{mod } n)$**

Decryption: receiver keeps ϕ and d private. When receiver receives the cipher text , it uses its private key d to decrypt the message: **$P=C^d(\text{mod } n)$**.

11.11.2 Digital Signatures

A **digital signature** or **digital signature scheme** is a type of Asymmetric Key algorithm. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signature in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide Non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a Bitstring: examples include Electronic mail, contact, or a message sent via some other Cryptographic protocol .

Digital signatures are often used to implement Electronic signature, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures

In cryptosystem, we use the private and public keys of the receiver . but in digital signature , we use the private and public keys of the sender.

Comparison

Let us discuss the differences between two types of signatures: Conventional and digital

a) **Inclusion :** when we sign a document digitally, we send the siganture as a separate document. The sender sends two documents: the message and the signature. The receipient receives both documents and verifies. But in conventional signature, it is not a separate document.

b) **Verification:** In conventioal signature, the recipient needs to have a copy of this signature on file for comparison. But in digital , the recipient needs to apply a verification method to the combination of the message and the signature varify the authenticity.

c) **Duplicity:** In conventional signature, a copy of the signed document can be distinguished from the original one on file. In digital signature, there is no such distinction unless there is a factor of time(such as a timestamp) on the document.

11.11.3 Firewalls

A **firewall** is a dedicated appliance, or software running on computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication. It is a device or set of devices configured to permit, deny, Encrypt, Decrypt as proxy server for all computer traffic between different security domains based upon a set of rules and other criteria.

A firewall's basic task is to regulate some of the flow of traffic between computer network of different trust levels. Typical examples are the Internet , which is a zone with no trust and an Intranet , which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or demilitarized zone(computing) (DMZ).

Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

1. **Packet Filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
2. **Application gateway :** Applies security mechanisms to specific applications, such as FTP and TELNET servers. This is very effective, but can impose a performance degradation.
3. **Circuit-level gateway :** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
4. **Proxy server :** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

11.12 SECURITY IN DIFFERENT LAYER

Security can be applied to the network, transport and application layers of the Internet model. For security ,first we need to create MAC . then we need to encrypt the message and probably, the MAC.the header and trailer of the security protocolmay or may not be included in the encryption process. To send secure data, we need a set of security parameters. We can use public key cryptography if each person has a private and public key pair. There are number of protocols which are used for security in different layers. These protocols are: IPSec, SSL/TLS , PGP and so on.

11.12.1 Secure E-mail

In virtually all distributed environments, electronic mail is the most heavily used network-based application . it is also the only distributed application that is widely used across all architectures and vendor platforms. One of the protocols to provide security at the application layer is Pretty Good Privacy(PGP). PGP is an open-source freely available software package for e-mail security. It provides authentication through the use of digital sigature. PGP is designed to create authenticated and confidential e-mails. Sending an e-mail is a one-time activity. Here we assume that the two parties create a session between themselves and exchange data in both directions. In e-mail, there is no session.

Operational Description : the actual operation of PGP, as opposed to the management of keys, consists of five services: authentication, confidentiality,compression, e-mail compatibility and segmentation.

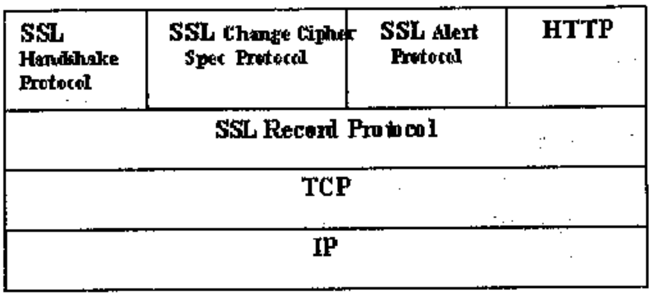
1) **Authentication :** the digital signature service provided by PGP. The recipient is assured that only the processor of the matching private key can generate the signature and no one else could generate a new message that matches the hash code and hence the signature of the original message.
2) **Confidentiality :** confidentiality is provided by encrypting messages to be stored locally as files. In both cases, the symmetric encryption algorithm CAST-128 may be used. The 64-bit cipher feedback(CFB) mode is used. In PGP, each symmetric key is used only once. That is , a new key is generated as a random 128-bit number for each message. Thus, although this is reffered to in the documentation as a session key, it is in reality a one time key.
3) **Compression:** as a fault, PGP comresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission and for file storage.
4) **E-mail compatibility:** when PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted(with the sender's private key). If the confidentiality service is used, the message plus signature are encrypted(with a one time symmetric key). PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.
5) **Segmentation:** e-mail facilities often are restricted to a maximum message length. Internet imposes a maximum length of 50,000 octets. Any message longer than that must be broken up into smaller segments, each of which is mailed seperately.

11.12.2 Secure Socket Layer(SSL)

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a sinle protocol but rather two layers of protocols. The SSL record protocol provides basic security services to various higher layer protocols. The HTTP provides the transfer service for web client/server interaction , can operate on top of SSL. Three higher layer protocols are defined as part of SSL: the Handshake protocol , the Change Cipher Spec Protocol and Alert Protocol.

Two important SSL concepts are the SSL session and the SSL connection, which are defined in the specification as follows:

- **Connection :** A connection is a transport that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
- **Session :** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Session defines a set of cryptographic security parameters, which can be shared among multiple connetions. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.



SSL Protocol Stack

SSL Record Protocol: The SSL Record Protocol provides two services for SSL connections:

- **Confidentiality :** the Handshack Protocol defines a shared sceret key that is used for conventional encryption of SSL payloads.
- **Message Integrity:** the Handshake Protocol also defines a shared secret key that is used to form a message authentication code(MAC).

11.12.3 IPSecurity(IPSec)

IPSecurity is collection of protocols designed by the Internet Engineering Task Force(IETF) to provide security for a packet at the network level. IPSec helps to create authentication and confidential for the IP layer. IPSec operates in one of two different modes: the transport mode or the tunnel mode.

a) **Transport mode:** In the Transport mode, IPSec protects what is delivered from the transport layer to the network layer. The transport layer protects the network layer payload. Transport layer does not protect the IP header. It protects only the packet from the transport layer. The transport mode is normally used when we need host-to-host protection of data. The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer. The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.

b) **Tunnel mode:** In the tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header , applies IPSec security methods to the entire packet, and then adds a new IP header. The new IP header, has different informaion than the original IP header. The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host . so the entire original packet is protected from intrusion between the sender and the receiver.

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s) , and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, authentication header (AH) and a combined encryption/ authentication protocol designed by the format of the packet for that protocol, Encapsulating security payload(ESP). The services are:

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replaced packets
- Confidentiality
- Limited traffic flow confidentiality.

11.13 SUMMARY

- The Domain name system (DNS) is a client/server application that identifies each host on the Internet.

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.
- FTP requires two connections for data transfer: a control connection and a data connection.
- SNMP uses the services of two other protocols: Structure of Management Information(SMI) and Management Information Base(MIB).
- Audio and video need to be digitized before being sent over the Internet.
- Cryptography is the science and art of transforming messages to make them secure and immune to attacks.
- IPSec operates in the transport mode or the tunnel mode.
- PGP uses the idea of certificate trust levels.
- SSL is designed to provide security and compression services to data generated from the application layer.

11.14 GLOSSARY

Cipher : An encryption/decryption algorithm.

DNS server : A computer that holds information about the name space.

HTML : The computer language for specifying the contents and format of a web document.

SNMP : The TCP/IP protocol that specifies the process of management in the Internet.

SMTP: The TCP/IP protocol defining electronic mail service on the Internet.

Secure Socket Layer(SSL) : A protocol designed to provide security and compression.

11.15 FURTHER READING

1. Andrew S. Tanenbaum, *Computer Networks*, 4/e, Pearson education, 2003.
2. Behrouz A. Fourouzan, *Data Communicatios and networking*, 2/e Tata McGrawhill, 2000.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson education, 2002.
4. Larry L. Peterson and Bruce S. davie, Computer Networks, 4/e Morgan Kaufmann,2008.
5. William Stallings , Cryptography and network security, fourth edition
6. http ://en.wikipedia.org/wiki/Application_Layer
7. http://pdf.codev2.cc/Lessig-Codev2.pdf

11.16. UNIT END QUESTIONS

1. Define Passive and Active security threats.
2. Define the role of compression in multimedia.
3. Role of Digital signature in network security
4. How to secure E-mail ?
5. Define RPC.
6. Explain SMTP, SNMP and FTP.
7. Design three design goals for a Firewall?
8. List For techniques used by Firewalls to control access and enforce a security policy.
9. What is the difference between an SSl connection and an SSL session?
10. What protocols comprise SSL?
11. What services are provided by IPSec ?
12. List and briefly define categories of security services.
13. Define security management and its purpose.
14. Define network management.
15. How is HTTP similar to SMTP?
16. What is URL and what are its components?

UNIT 12

THE INTERNET

12.1 OBJECTIVE

After studying this unit, you will learn

- Functions of Internet
- Internet Protocol(IP)
- IP packet format
- ICMP
- Ping command
- Round trip response time

12.2 INTRODUCTION

The **Internet** is a global system of interconnected computer network. A computer that connects to the Internet can access information from a vast number of server and other computers. An Internet connection also allows the computer to send information onto the network; that information may be saved and ultimately accessed by a variety of servers and other computers. Much of the widely accessible information on the Internet consists of the interlinked Hypertext documents and other resources of the WWW. Web users typically send and receive information using a Web browser; other software for interacting with computer networks includes specialized programs for E-mail, Online chat, File transfer and file sharing.

What is Internet ?

The **Internet** is a global network of interconnected computers, enabling users to share information along multiple channels. Typically, a computer that connects to the Internet can access information from a vast array of available and other computers by moving information from them to the computer's local memory. So a collection of interconnected networks is called an internetwork or just Internet.

Information is moved around the Internet by packet switching using the standardized Internet protocol suite (TCP/IP). It is a "network of networks" that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, optical fiber cables, Wireless connections, and other technologies.

Uses of Internet

- **E-mail**

The concept of sending electronic text messages between parties in a way analogous to mailing letters or memos predates the creation of the Internet. Even today it can be important to distinguish between Internet and internal e-mail systems. Internet e-mail may travel and be stored unencrypted on many other networks and machines out of both the sender's and the recipient's control. Today you can send pictures and attach files on e-mail. Most e-mail servers today also feature the ability to send e-mail to multiple E-mail addresses.

- **The World Wide Web(WWW)**

The World Wide Web is a huge set of interlinked documents , computer graphics and other resources , linked by hyperlink and URL's. These hyperlinks and URLs allow the web servers and other machines that store originals, and cached copies of, these resources to deliver them as required using HTTP (Hypertext Transfer Protocol). HTTP is only one of the communication protocols used on the Internet.

Web server also use HTTP to allow software systems to communicate in order to share and exchange business logic and data.In the early days, web pages were usually created as sets of complete and isolated HTML text files stored on a web server. More recently, websites are more often created using content management or software with, initially, very little content. Contributors to these systems, who may be paid staff, members of a club or other organisation or members of the public.

- **Remote access**

The Internet allows computer users to connect to other computers and information stores easily, wherever they may be across the world. They may do this with or without the use of computer security, authentication and encryption technologies, depending on the requirements.

This is encouraging new ways of working from home, collaboration and information sharing in many industries. An accountancy sitting at home can audit the books of a company based in another country, on a server(computing) situated in a third country that is remotely maintained by IT specialists in a fourth.

- **Collaboration**

The low cost and nearly instantaneous sharing of ideas, knowledge, and skills has made collaboration work dramatically easier. Not only can a group cheaply communicate and share ideas, but the wide reach of the Internet allows such groups to easily form in the first place. Business and project teams can share calendars as well as documents and other information. Such collaboration occurs in a wide variety of areas including scientific research, software development, conference planning, political activism and creative writing.

- **File Sharing**

This simple feature of the Internet, over a worldwide basis, are used to change the production, sale, and distribution of anything computer file at for transmission. This includes all manner of print publications, software products, news, music, film, video, photography, graphics and the other arts. This in turn has caused seismic shifts in each of the existing industries that previously controlled the production and distribution of these products.

- **Internet Telephony(VoIP)**

VoIP stands for Voice-over-Internet protocol, referring to the protocol that underlies all Internet communication. The idea began in the early 1990s with walkie-talkie-like voice applications for personal computers. In recent years many VoIP systems have become as easy to use and as convenient as a normal telephone. The benefit is that, as the Internet carries the voice traffic, VoIP can be free or cost much less than a traditional telephone call, especially over long distances and especially for those with always-on Internet connections such as cable modem or ADSL.

12.3 INTERNET PROTOCOL(IP)

The **Internet Protocol (IP)** is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet protocol version 6 "IPv6" is being deployed actively worldwide.

As a consequence of this design, the Internet Protocol only provides best effort delivery and its service can also be characterized as *unreliable*. In network architectural language it is a *connection-less* protocol, in contrast to so-called connection-oriented modes of transmission. The lack of reliability allows any of the following fault events to occur:

- data corruption
- lost data packets
- duplicate arrival
- out-of-order packet delivery; meaning, if packet 'A' is sent before packet 'B', packet 'B' may arrive before packet 'A'. Since routing is dynamic and there is no memory in the network about the path of prior packets, it is possible that the first packet sent takes a longer path to its destination.

IP address

IP address is a logical address which is defined by the Internet Protocol layer(IP layer). IP address is a unique address assigned to each computer connected to the internet . it is used by TCP/IP to route packets of information from a sender to a location on the Internet.

IP address consists of four sets of numbers ranging from 0 to 255, e.g. 250.7.13.53 .

We can explain this IP address as

a) the first two number sets designate the network.

b) the third number set identy of the local address and

c) the fourth number set identy of the particular machine.

There are basically four types of IP addresses: classes A,B, C and D. A particular class address has a unique network address size and a unique host address size. When we examine the first decimal value in the dotted decimal notation: all classes A addresses are in the range of 0-127, all classes B addresses are in the range of 128-191, and all classes C addresses are in the range of 192-223. remaining range of addresses belongs to class D.

The original designers of TCP/IP defined an IP address as a "32 bit" number and this system, now named (IPv4), is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of the address space, a new addressing system ("Ipv6"), using 128 bits for the address, was developed .

12.3.1 Names and Addresses

All entities in a data communications network must be uniquely identified to allow data to be directed to the intended recipient. This process is known as "***addressing***" and the identifier allocated to a node is known as its address. Each node is usually allocated at least one address. The addresses (which resemble telephone numbers) are normally quoted in a numeric format (e.g. hexadecimal, decimal, or dotted decimal), which is easily encoded into binary for transmission across the network.

Most users are able only to remember a few numbers but are able to memorize the entire lists of words. This could be one of the reasons people are normally identified by name rather than social security number! It is therefore easier to allocate a name (label) corresponding to the addresses used by the network. An email address is a name, as is a free-phone number. To use a name, it is first necessary to find the corresponding numeric address, this is usually performed by a name-server, which is a network resource which has a list of all names and the corresponding addresses.

More precisely, A ***name*** is a symbol, such as human-readable text string, which identifies a resource such as a process, device, or service. An address is a data structure, understood by the network, used to specify the destination of a connection/message/packet. A name server provides a service which resolves a name into an address.

A network provides the connections between two types of node. If a node allows users to login or run processes on it, the node is called an End System(ES) sometimes also known as a host. A node which does not have any users, but only routes packets from other nodes, is known as an Intermediate System(IS). Some nodes provide both functions and may be called by either name, depending upon which function they perform.

The neighboring nodes in a network are connected by links. A route is an address of a neighbor node, this is the link to be used to transmit a specific message towards its intended destination. Using a succession of routes between Intermediate systems the network finds a path from the source end system to the destination end system. The selection of an appropriate series of routes between intermediate systems is known as routing.

The major distinction between names and addresses is whether they are intended to be human-readable or machine-readable. Names range from simple names of only local applicability, such as mail used to access mail service after gaining access to a computer providing this facility, to universal names. An example of a truly universal name is

```
        <galaxy><star><planet><country><network><host><port>
```

The term port is an identifier number that specifies an individual process or user program running on the destination computer.

A typical address could be 8036565901, or a binary expansion of such a number, for example, 1000 0000 0011 0110 0101 0110 0101 1001 0000 0001.

12.3.2 Flat and Hierarchical Structures

There are also two types of addressing used, flat and hierarchical.

When the networks use a ***hierarchical address*** structure, the network may use this information to help perform the routing. A typical example of a hierarchical addressing system is the telephone numbering scheme.

Many networks use a ***flat addressing*** scheme (e.g. the MAC hardware address, the IP network address), where the actual address used does not have a relationship to the hierarchical name which it represents. This type of address is easily administered and assumes no specific network topology.

Although easy to administer, a flat address scheme provides no indication of the location of a computer in the network. It is therefore complex to arrange routing between end systems in a large flat network. The social security system is an example of a flat address space. Social security numbers are allocated to people in the order in which they are processed in a particular area. The number itself says nothing about the individual or where she/he may be found (the only information is the social security office where the person's records were processed!)

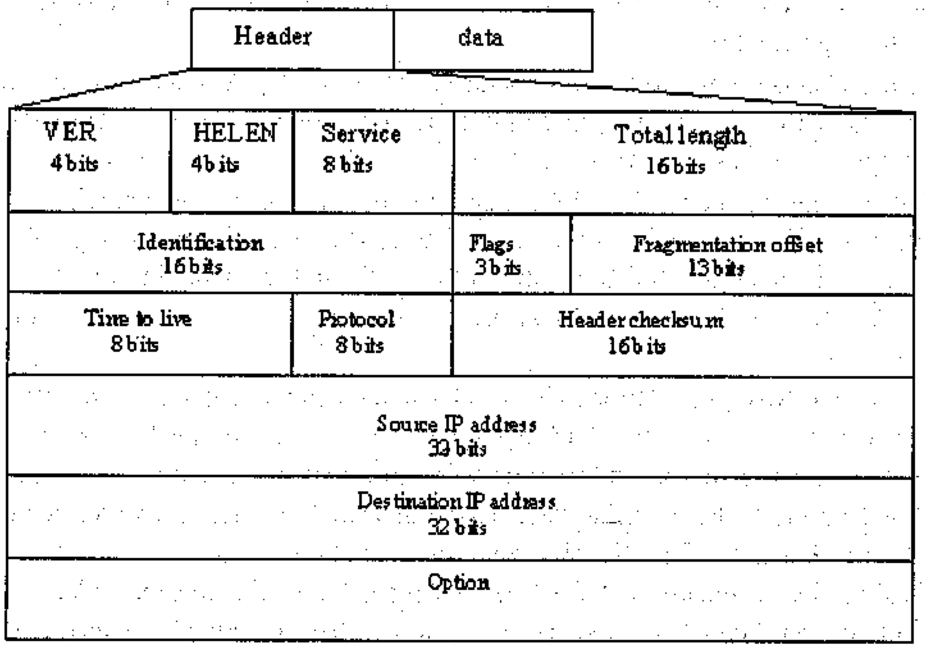
Both hierarchical and flat address spaces have advantages. Hierarchical addresses can simplify routing, since successive steps may depend on individual fields. For example, successively locating a country, an area, a central office, and a subscriber. It is also simple to assign hierarchical addresses without the need for a central authority. Abbreviation of addresses for local use is easy; for example, country and area codes do not need to be dialed for local phone calls. On the other hand, hierarchical address must be changed if subscribers move and the address space may be inefficiently used since the number of addresses available at a hierarchy level is largely independent of how many are needed. Both types of addressing are common

12.3.3 Packet format

An IP packet consists of a header section and a data section.

Header

The header consists of 13 fields, of which only 12 are required. The 13th field is optional (red background in table) and aptly named: options. The fields in the header are packed with the most significant byte first, and for the diagram and discussion, the most significant bits are considered to come first. The most significant bit is numbered 0, so the version field is actually found in the four most significant bits of the first byte, for example.



IP frame format

Version(VER) : The first header field in an IP packet is the four-bit version field. For IPv4, this has a value of 4 (hence the name IPv4).

Header length(HLEN): The second field (4 bits) is the Internet Header Length (IHL) telling the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum value for this field is 5 , which is a length of 5×32 = 160 bits. Being a 4-bit value, the maximum length is 15 words or 480 bits.

Differentiated Services (DS) : The original intention of the **Type of Services** (TOS) field was for a sending host to specify a preference for how the datagram would be handled as it made its way through an internet. For instance, one host could set its IPv4 datagrams' TOS field value to prefer low delay, while another might prefer high reliability. In practice, the TOS field was not widely implemented. However, a great deal of experimental, research and deployment work has focused on how to make use of these eight bits, resulting in the current DS field definition.

Total Length : This 16-bit field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 — the maximum value of a 16-bit word. The minimum size datagram that any host is **required** to be able to handle is 576 bytes, but most modern hosts handle much larger packets. Sometimes subnetworks impose further restrictions on the size, in which case datagrams must be fragmented. Fragmentation is handled in either the host or packet switch in

Identification : This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.

Flags : A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):

- Reserved; must be zero.
- Don't Fragment (DF)
- More Fragments (MF)

If the DF flag is set and fragmentation is required to route the packet then the packet will be dropped. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation.

When a packet is fragmented all fragments have the MF flag set except the last fragment, which does not have the MF flag set. The MF flag is also not set on packets that are not fragmented — an unfragmented packet is its own last fragment.

Fragment Offset : The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of $(2^{13} - 1) \times 8 =$ 65,528 which would exceed the maximum IP packet length of 65,535 with the header length included.

Time To Live (TTL) : An eight-bit time to live(TTL) field helps prevent datagrams from persisting (e.g. going in circles) on an internet. This field limits a datagram's lifetime. It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In latencies typical in practice, it has come to be a hop count field. Each packet switch (or router) that a datagram crosses decrements the TTL field by one. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded. Typically, an ICMP message (specifically the time exceeded) is sent back to the sender that it has been discarded. The reception of these ICMP messages is at the heart of how traceroute works.

Protocol : This field defines the protocol used in the data portion of the IP datagram. The Internet Assigned Numbers Authority maintains a list of Protocol numbers . Common protocols and their decimal values are shown below (*see Data*).

Header Checksum : The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded. Note that errors in the data field are up to the encapsulated protocol to handle — indeed, both UDP and TCP have checksum fields.

Since the TTL field is decremented on each hop and fragmentation is possible at each hop then at each hop the checksum will have to be recomputed.

The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

In other words, all 16-bit words are summed together using one's complement(with the checksum field set to zero). The sum is then one's complemented and this final value is inserted as the checksum field.

Source address : An IPv4 address is a group of four eight-bit octets for a total of 32 bits. The value for this field is determined by taking the binary value of each octet and concatenating them together to make a single 32-bit value. Thus, reply packets sent by the receiver are routed to the NATing machine, which translates the destination address to the original sender's address.

Destination address : Identical to the source address field but indicates the receiver of the packet.

Options : Additional header fields may follow the destination address field, but these are not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List, 0x00) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header.

Data :The last field is not a part of the header and, consequently, not included in the checksum field. The contents of the data field are specified in the protocol header field and can be any one of the transport layer protocols. Some of the most commonly used protocols are listed below including their value used in the protocol field:

- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Open Shortest Path First (OSPF)
- Stream Control Transmission Protocol (SCTP)

12.4 IP OVER ETHERNET

Ethernet was originally developed by Digital, Intel and Xerox (DIX) in the early 1970's and has been designed as a 'broadcast' system, i.e. stations on the network can send messages whenever and wherever it wants. All stations may receive the messages, however only the specific station to which the message is directed will respond.

Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD). When an Ethernet station is ready to transmit, it checks for the presence of a signal on the cable i.e. a voltage indicating that another station is transmitting. If no signal is present then the station begins transmission, however if a signal is already present then the station delays transmission until the cable is not in use. If two stations detect an idle cable and at the same time transmit data, then a collision occurs.

The most commonly used link layer protocol for Local area network (LAN) is Ethernet and this is frequently used to support a range of network layer protocols, including Internet protocol. The IP datagrams are transmitted by encapsulation in Media access control(MAC) frames (or LLC frames using MAC(encapsulation). For example IP datagram (with carrying ICMP message) for transmission over Ethernet can be define as:

Ethernet header	IP header	ICMP header	User data	Ethernet CRC

IP introduces an extra protocol, known as the ARP to map between the destination hardware address in a MAC frame and an IP network address. The protocol stack is shown in the figure below together with the position of each protocol within the OSI reference model.

12.5 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

We know that IP provides unreliable and connectionless datagram delivery. It was designed to make efficient use of network resources. The IP protocol is a best-effort delivery service that delivers a datagram from its original source to its final destination. But the IP protocol has no error-reporting or error correcting mechanism. And the IP protocol also lacks a mechanism for host and management queries. The **Internet**

Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. The **Internet Control Message Protocol (ICMP)** is one of the core protocols of the Internet Protocol Suite. It is mainly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached. ICMP is used for error and control messages within the IP world and is very much integrated with IP. IP is not designed to be totally reliable although many common network errors are dealt with. ICMP messages give information when things do not go according to plan, however even these can get lost so for this reason no ICMP messages are sent as a result of previous ICMP messages going missing. ICMP relies on IP to perform its tasks, and it is an integral part of IP. It differs in purpose from transport protocols such as TCP and UDP in that it is typically not used to send and receive data between end systems. It is usually not used directly by user network applications.

ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6. ICMP messages are constructed at the IP layer, usually from a normal IP datagram that has generated an ICMP response. IP encapsulates the appropriate ICMP message with a new IP header (to get the ICMP message back to the original sending host) and transmits the resulting datagram in the usual manner.

For example, every machine (such as an intermediate router) that forwards an IP datagram has to decrement the time to live (TTL) field of the IP header by one; if the TTL reaches 0, an ICMP Time to live exceeded in transit message is sent to the source of the datagram. Each ICMP message is encapsulated directly within a single IP datagram, and thus, like UDP, ICMP is unreliable.

ICMP messages are divided into two categories : **error reporting messages** and **query messages.** The error reporting messages report problems that a router or a host may encounter when it processes an IP packet.

12.5.1 Error reporting message

one of the main responsibility of ICMP is to report errors. So error checking and error control is not a concern of IP. ICMP does not correct errors-it simply reports. Error correction is left to the higher-level protocols. Error messages are sent to the original source because the only information available in the datagram about the route is the source and destination addresses. ICMP uses the source IP address to send error message to the source of the datagram.

Five types of errors are handled: destination unreachable, source quench, time exceeded, parameter problems and redirection.

- **Destination unreachable :** when a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that intimated the datagram.
- **Source quench :** we know that IP protocol is a connectionless protocol. The source quench message in ICMP was designed to add a kind of flow control to the IP. When a router or host discards a datagram due to congestion. It sends a source quench message to the sender of the datagram. It informs the source that the datagram has been discarded.
- **Time Exceeded :** if there is an error in one or more routing tables, a packet can travel in a loop going from one router to the next or visiting a series of routers endlessly. When the time-to-live value reaches 0, after decrementing the router discards the datagram.
- **Parameter problem:** if a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter problem message back to the source.
- **Redirection :** when a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router. The same is true if the sender is a host. Both routers and hosts, then must have a routing table to find the address of the router or the next router.

12.5.2 Echo request and reply

In addition to error reporting, ICMP can diagnose some network problem. This is accomplished through the query messages. Echo request and reply is one of the query messages in ICMP. In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet.

The Echo request and Echo reply messages are designed for diagnostic purposes. Network managers and users utilize this pair of messages to identify network problems. The combination of Echo request and Echo reply messages determines whether two systems can communicate with each other. The Echo request and Echo reply message can be used determine if there is communication at the IP level. Because ICMP messages are encapsulated in IP datagrams, the receipt of an Echo reply message by the machine that sent the Echo request is a proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram. To day most systems provide a version of the ping command that can create a series of Echo request and Echo reply messages, providing statistical information.

12.5.3 ICMP Message format

An ICMP message has an 8-byte header and a variable-size data section. Where the first field ICMP type, defines the type of the message. The code field specifies the reason for the particular message type. The last common field is the checksum field. The rest of the header is specific for each message type. The data section in error messages carries information for finding the original packet that had the error in query messages, the data section carries extra information based on the type of the query.

Header

The ICMP header starts after bit 160 of the IP header (unless IP options are used).

Bits	160-167	168-175	176-183	184-191
160	Type	code	Checksum	
192	ID		Sequence	

- **Type** - ICMP type as specified below.
- **Code** - further specification of the ICMP type; e.g. : an ICMP Destination Unreachable might have this field set to 1 through 15 each bearing different meaning.
- **Checksum** - This field contains error checking data calculated from the ICMP header+data, with value 0 for this field.
- **ID** - This field contains an ID value, should be returned in case of ECHO REPLY.
- **Sequence** - This field contains a sequence value, should be returned in case of ECHO REPLY.

It is the responsibility of the network layer (IP) protocol to ensure that the ICMP message is sent to the correct destination. This is achieved by setting the destination address of the IP packet carrying the ICMP message. The source address is set to the address of the computer that generated the IP packet (carried in the IP source address field) and the IP protocol type is set to "ICMP" to indicate that the packet is to be handled by the remote end system's ICMP client interface.

12.6 PING PROGRAM

The "ping" program contains a client interface to ICMP. It may be used by a user to verify an end-to-end Internet Path is operational. The ping program also collects performance statistics (i.e. the measured round trip time and the number of times the remote server fails to reply. Each time an ICMP echo reply message is received, the ping program displays a single line of text. The text printed by ping shows the received sequence number, and the measured round trip time (in milliseconds). Each ICMP Echo message contains a sequence number (starting at 0) that is incremented after each transmission, and a timestamp value indicating the transmission time.

'***Ping***' is a computer network tool used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a speed test. It works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. Ping measures the round-trip time and records any packet loss, and prints when finished a statistical summary of the echo response packets received, the minimum, mean, max and in some versions the standard deviation of the round trip time.

The word *ping* is also frequently used as a verb or noun, where it is usually incorrectly used to refer to the round-trip time, or measuring the round-trip time.

The term 'ping' is commonly used to indicate an effectively contentless message. For instance, a short or empty instant message, email, voice mail or "missed call" notification can be used to indicate availability, or anything else that can be conveyed with a single bit of information at a given time.

the *ping* command's output gives:

- The **IP address** which corresponds to the name of the remote machine;
- The ICMP **sequence number**;
- The packet's **time to live** (*TTL*). The time to live (TTL) field shows how many routers the packet went through as it travelled between the two machines. Each IP packet has a TTL field with a relatively high value. Each time it goes through a router, the value is reduced. If this number ever reaches zero, the router interprets this to mean that the packet is going around in circles, and terminates it;
- The **round-trip delay** field corresponds to the length of time in milliseconds of a round trip between the source and target machines. As a general rule, a packet must have a delay no longer than 200 ms;
- The **number of lost packets**.

fping is a *ping* like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up. fping is different from ping in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. Instead of trying one host until it timeouts or replies, fping will send out a ping packet and move on to the next host in a round-robin fashion. If a host replies, it is noted and removed from the list of hosts to check. If a host does not respond within a certain time limit and/or retry limit it will be considered unreachable.

In this case there is only one Intermediate System (IS) (i.e. IP router). In this case two types of message are involved the ECHO request (sent by the client) and the ECHO reply (the response by the server). Each message may contain some optional data. When data are sent by a server, the server returns the data in the reply which is generated. ICMP packets are encapsulated in IP for transmission across an internet.

12.7 ROUND TRIP TIME

Heterogeneous communication networks with their variety of application demands, uncertain time -varying traffic load, and mixture of wired and wireless links pose several challenging problem in modeling and control. here we focus on the Round-Trip Time(RTT), which is a particularly important variable for efficient end-to-end congestion control. Based on a simple aggregated model of the network, an algorithm combining a Kalman filter and a change detection algorithm is proposed for RTT estimation. It is illustrated on real data that this algorithm provides estimates of significantly better accuracy as compared to the RTT estimator currently used in TCP, especially in scenarios where new cross-traffic flows cause a bottle-neck link to rapidly build up a queue, which in turn induces rapid changes of the RTT.

Congestion control is one of the key components that has enabled the dramatic growth of the Internet. The original idea was to adjust the transmission rate based on the loss probability.. This algorithm (together with some of its siblings) is now the dominating transport protocol on the Internet. The throughput and delay experienced by individual users are depending on several factors, including the TCP protocol, link capacity and competition from other users. There are also lower layers that may affect the achieved delay and bandwidth, particularly if part of the end-to-end connection is a wireless link.

TCP is window-based which means that each sender has a window that determines how many packets in flight that are allowed at any given time. The transmission rate is regulated by adjusting this window. Motivated by the previous discussion on the importance of accurate RTT estimates, we now take a closer look at short-range RTT from a statistical perspective. The raw RTT measurements, obtained from packet acknowledgements (ACK's), include delays caused by transient effects in the network (attributed to short-lived cross-traffic).

The short-lived duration of these flows means that their contribution to the RTT can be considered as noise from the point of view of congestion control. It is thus reasonable to filter them out. In present versions of TCP this is done with a first-order low-pass filter. The average RTT (averaged over a few RTT) often makes sudden changes due to the appearance of a long-lived cross-flow somewhere along the path. It is then important for the filter to react quickly to this change, since otherwise buffers will start to build up with enlarged risk of packet loss and increased delay as consequences. It is impossible with a first-order filter to rapidly adjust to these changes.

12.8 SUMMARY

- The **Internet** is a global network of interconnected computers, enabling users to share information along multiple channels.
- TCP is window-based which means that each sender has a window that determines how many packets in flight that are allowed at any given time.
- The **Internet Control Message Protocol (ICMP)**is one of the core protocols of the Internet Protocol Suite
- The "ping" program contains a client interface to ICMP.
- Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- An eight-bit time to live(TTL) field helps prevent datagrams from persisting (e.g. going in circles) on an internet.
- Hierarchical addresses can simplify routing, since successive steps may depend on individual fields.

12.9 GLOSSARY

- Internet : A global internet that uses the TCP/IP protocol suite.
- Internet Assigned Number Authority(IANA): a group supported by the U.S. government that was responsible for the management of Inter domain names.
- Internet Control Message Protocol(ICMP) : A protocol in the TCP/IP suite that handles error and control message.
- Checksum : A value used for error detection.
- Datagram : In packet switching, an independent data unit.

12.10 FURTHER READINGS

1. Andrew S. Tanenbaum, *Computer Networks*, 4/e, Pearson education, 2003.
2. Behrouz A. Fourouzan, *Data Communicatios and networking*, 2/e Tata McGrawhill, 2000.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson education, 2002 .
4. Larry L. Peterson and Bruce S. davie, Computer Networks, 4/e Morgan Kaufmann,2008.

12.12 UNIT END QUESTIONS

1. Differentiate between Flat and hierarchical name space.
2. Define echo request and echo reply.
3. What is the Use of Ping command in ICMP
4. Differentiate between IPv4 and IPv6 frame format.

5. Define Time-to live(TTL).
6. How to measure round trip response time
7. Explain error reporting in ICMP.
8. What is the role of IP in Ethernet ?
9. Define any four error reporting messages of ICMP.
10. Explain the procedure for checksum calculation and verification in the IPv4 protocol.
11. What is a mask in IPv4 addressing? What is a default mask in IPv4 addressing.
12. Define IPv4 frame format in detail.
13. What is the use of Round trip time in networking ?