

University of Technology
Department of Computer Science
Date: 2018-2019

Lecturer: Dr. Raheem Abdul Sahib Oglia
Material: computer networks
Branches : Security, Programming ,.....

=====Course One=====

المحاضر
د. رحيم عبد الصاحب الربيعي
المادة : شبكات الحاسوب ومقدمة للاتصالات
الملزمة الأولى
2023-2024

1. Computer Networking

Part 1

Data Communications and Networking

NETWORKING FUNDAMENTALS

Unit Structure

- 1.0 Objectives
 - 1.1 Introduction
 - 1.2 Data & Information
 - 1.3 Data Communication
 - 1.3.1 Characteristics of Data Communication
 - 1.3.2 Components of Data Communication
 - 1.4 Data Representation
 - 1.5 Data Flow
 - 1.5.1. Simplex
 - 1.5.2. Half Duplex
 - 1.5.3. Full Duplex
 - 1.6 Computer Network
 - 1.6.1 Categories of a network
 - 1.7 Protocol
 - 1.7.1 Elements of a Protocol
 - 1.8 Standards in Networking
 - 1.8.1 Concept of Standard
 - 1.8.2 Standard Organizations in field of Networking
 - 1.9 Network topology
 - 1.10 Network Types
 - 1.11 Transmission Media
- 1.9 References

1.0 OBJECTIVES:

- Introduce the readers to data communication and its fundamentals
- Define networks.
- Define protocols .
- Network topology.
- Transmissions Media

1.1 INTRODUCTION

This Lecture provides an introduction to computer networks and covers fundamental topics like data, information to the definition of communication and computer networks.

The main objective of data communication and networking is to enable seamless exchange of data between any two points in the world. This exchange of data takes place over a computer network.

1.2 DATA & INFORMATION

Data refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.

Ex. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.

The word **data** refers to any information which is presented in a form that is agreed and accepted upon by its creators and users.

1.3 DATA COMMUNICATION

Data Communication is a process of exchanging data or information

In case of computer networks this exchange is done between two devices over a transmission medium.

This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a **Protocol**.

The following sections are describes the fundamental characteristics that are important for the effective working of data communication process and is followed by the components that make up a data communications system.

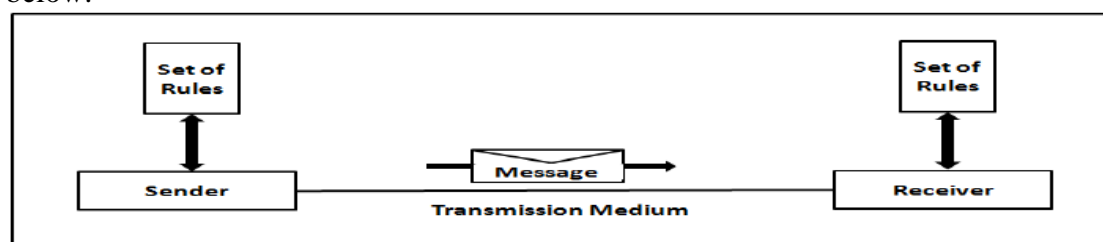
1.3.1 Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. **Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. **Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

1.3.2 Components of Data Communication

A Data Communication system has five components as shown in the diagram below:



Fig(1) Components of a Data Communication System

=====Course One=====

1. **Message:** Message is the information to be communicated by the sender to the receiver.
 2. **Sender:** The sender is any device that is capable of sending the data (message).
 3. **Receiver:** The receiver is a device that the sender wants to communicate the data (message).
 4. **Transmission Medium:** It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
 5. **Protocol:** It is an agreed upon set or rules used by the sender and receiver to communicate data.
- A **protocol** is a set of rules that governs data communication.
 - A **Protocol** is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

1.4 DATA REPRESENTATION

Data is collection of raw facts which is processed to deduce information. There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:

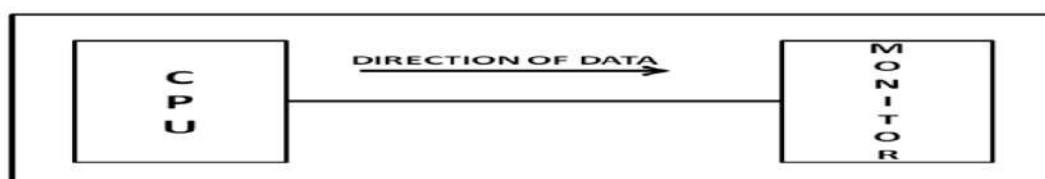
1. **Text:** **Text** includes combination of alphabets in small case as well as upper case. It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode
2. **Numbers:** Numbers include combination of digits from 0 to 9. It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode
3. **Images**
4. **Audio:** Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information.
Audio data is continuous, not discrete.
5. **Video:** **Video** refers to broadcasting of data in form of picture or movie

1.5 DATA FLOW

Two devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

1. Simplex
2. Half Duplex
3. Full Duplex

1.5.1 Simplex



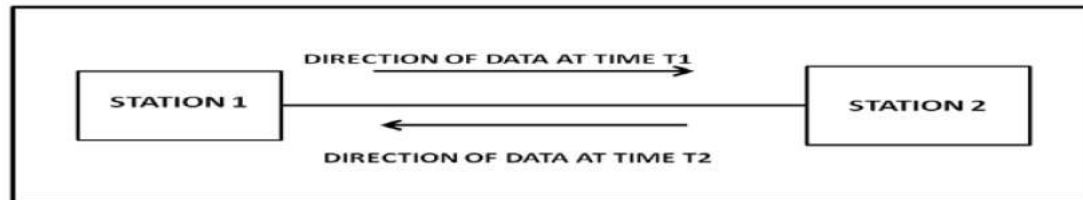
Fig(2): Simplex mode of communication

- **In Simplex**, communication is unidirectional

=====Course One=====

- Only one of the devices sends the data and the other one only receives the data.
- Example: in the above diagram: a cpu send data while a monitor only receives data.

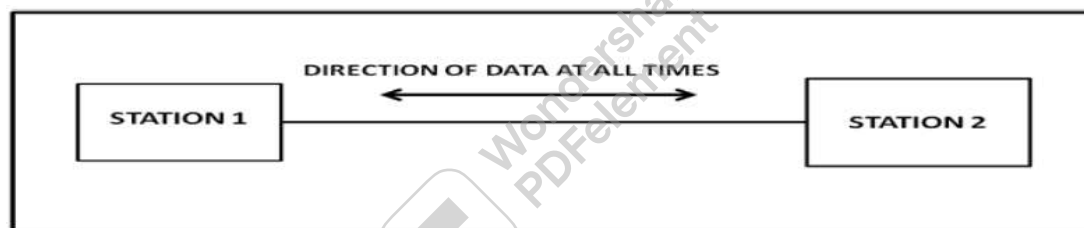
1.5.2 Half Duplex



Fig(3) Half Duplex Mode of Communication

- **In half duplex** both the stations can transmit as well as receive but not at the same time.
- When one device is sending other can only receive and vice-versa (as shown in figure above.)
- Example: A walkie-talkie.

1.5.3 Full Duplex



Fig(4): Full Duplex

- **In Full duplex mode**, both stations can transmit and receive at the same time.
- Example: mobile phones

1.6 COMPUTER NETWORK (Criteria of Network)

- Computer Networks are used for data communications
- **Definition:** A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.
- A Compute network should ensure
 - ✓ **reliability** of the data communication process
 - ✓ **security** of the data
 - ✓ **performance** by achieving higher throughput and smaller delay times

1.6.1 Categories of Network

Networks are categorized on the basis of their size. The three basic categories of computer networks are:

- Local Area Networks (LAN)** is usually limited to a few kilometers of area. It may be privately owned and could be a network inside an office on one of the floor of a

=====Course One=====

building or a LAN could be a network consisting of the computers in a entire building.

- B. **Wide Area Network (WAN)** is made of all the networks in a (geographically) large area. The network in the entire state of Maharashtra could be a WAN.
- C. **Metropolitan Area Network (MAN)** is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.

1.7 PROTOCOL

- **A Protocol** is defined as a set of rules that governs data communications.
- A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

1.7.1 Elements of a Protocol

There are three key elements of a protocol:

- A. **Syntax:**
 - It means the structure or format of the data.
 - It is the arrangement of data in a particular order.
- B. **Semantics :**
 - It tells the meaning of each section of bits and indicates the interpretation of each section.
 - It also tells what action/decision is to be taken based on the interpretation.
- C. **Timing**
 - It tells the sender about the readiness of the receiver to receive the data
 - It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

1. Data Communication & Networking – Behrouz Forouzan

1. Data Communications (More Details)

- 1.1 Data Communication Model
- 1.2 Signal Conversions
- 1.3 Analog signal
- 1.4 Waveforms of different parameters
- 1.5 Bandwidth
- 1.6 Noise
- 1.7 Channel Capacity
- 1.8 Types Of Communications
- 1.9 Modes of transmission
- 1.10 Multiplexing
- 1.11 Network Models

1. Data Communications

Communication is defined as transfer of information, such as thoughts and messages between two entities. The invention of telegraph, radio, telephone, and television made possible instantaneous communication over long distances.

In the context of computers and information technology (IT), the data are represented by **binary digit** or **bit** has only two values 0s and 1s. In fact anything the computer deals with are 0s and 1s only. Due to this it is called discrete or digital. In the digital world messages, thoughts, numbers.. etc can be represented in different streams of 0s and 1s.

Data communications concerns itself with the transmission (sending and receiving) of information between two locations by means of electrical signals. The two types of electrical signals are analog and digital. Data communication is the name given to the communication where exchange of information takes place in the form of 0s and 1s over some kind of media such as wire or wireless. The subject-Data Communications deals with the technology, tools, products and equipment to make this happen.

Entire data communication system revolves around three fundamental concepts.

- **Destiny:** The system should transmit the message to the correct intended destination. The destination can be another user or another computer.
- **Reliability:** The system should deliver the data to the destiny faithfully. Any unwanted signals (noise) added along with the original data may play havoc!
- **Fast:** The system should transmit the data as fast as possible within the technological constraints. In case of audio and video data they must be received in the same order as they are produced without adding any significant delays.

1.1 Data Communication model

The figure 1.1(a) shows the block diagram of a typical communication model. The communication model has five sub systems viz., user, transmitter, communication channel, receiver and destiny.

- **User:** There will be a source that generates the message and a transducer that converts the message into an electrical signal. The source can be a person in front of a microphone or a computer itself sending a file. The user terminal is known as Data Terminal Equipment (DTE).
- **Transmitter:** Can be a radio frequency modulator combining the signal coming out of the data equipment terminal. Here the radio frequency is acting as the carrier for the data signal. Or in case of direct digital transmission the transmitter can be Manchester encoder transmitting digital signals directly.
- **Communication channel:** Can be **guided media** (twisted pair, coaxial cable, fiber optic.) or **unguided media** (air, water ..). In both the cases communication is in the form of electromagnetic waves. With guided media the electromagnetic waves are guided along a physical path. **Unguided media** also called wireless the transmitting electromagnetic waves are not guided along with a physical path. They are radiated through air/vacuum/water., etc.
- **Receiver:** The receiver amplifies the received signals removes any unwanted signals (noise) introduced by the communication channel during propagation of the signal and feeds to the destiny.

=====Course One=====

- **Destiny:** The user at the other end finally receives the message through the data terminal equipment stationed at the other side.

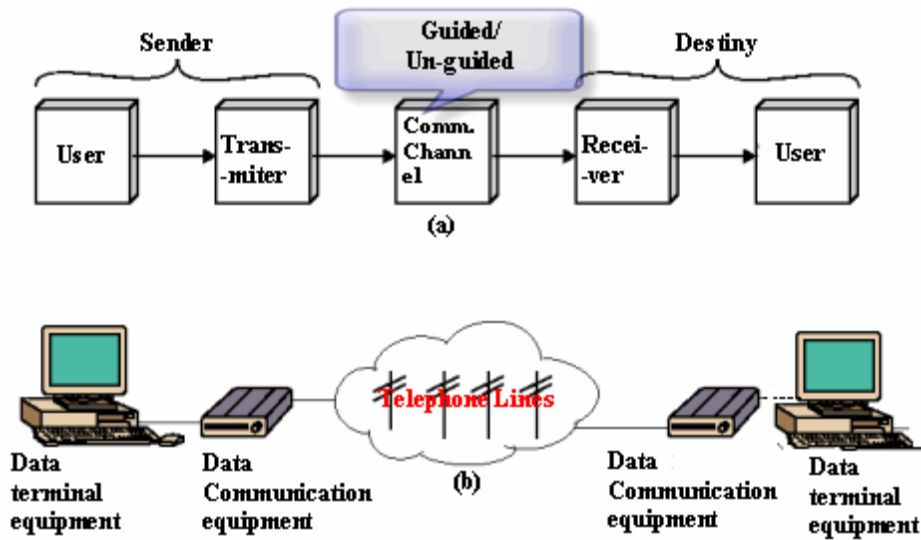


Fig 1.1 (a) The block diagram of a data communication model
 (b) A typical dial-up network

Fig 1.1 (b) shows a typical dial-up network setup.

1.2 Signal conversions

There are two types of signals analog and digital. All naturally available signals are analog in nature. In data communications these signals are converted into digital form by means of A-to-D converters (analog to digital converters).

The following figure illustrates the analog output of microphone and subsequent conversion into its digital counter part by A-to-D converter.

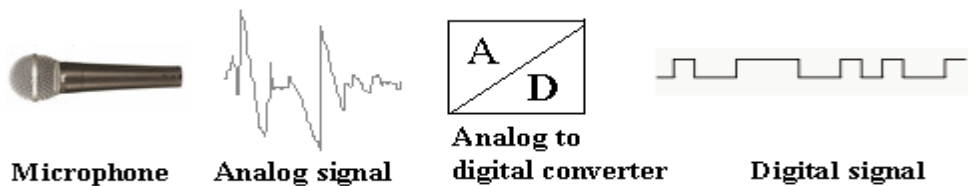


Fig 1.2.1 Example of analog and digital signal

1.3 Analog signal.

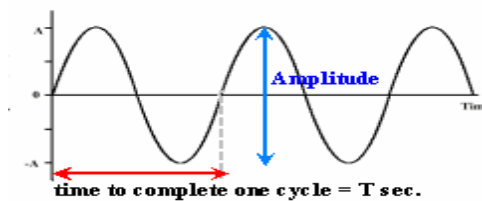


Fig 1.3.1 A simple sine wave and its parameters.

The sine wave is the simplest form of an analog signal. **It has three parameters.** Amplitude, frequency and phase. Normally amplitude in volts is denoted on Y-axis

=====Course One=====

and time period is on X-axis. The time taken to complete one cycle is called time period and measured in seconds.

The reciprocal of time period is frequency and its unit is cycles per second(c/s) or Hz (Hertz).(See Fig.1.2).

1.4 Wave forms of different parameters

The following figures show the signals with different parameters and their inter-relationship

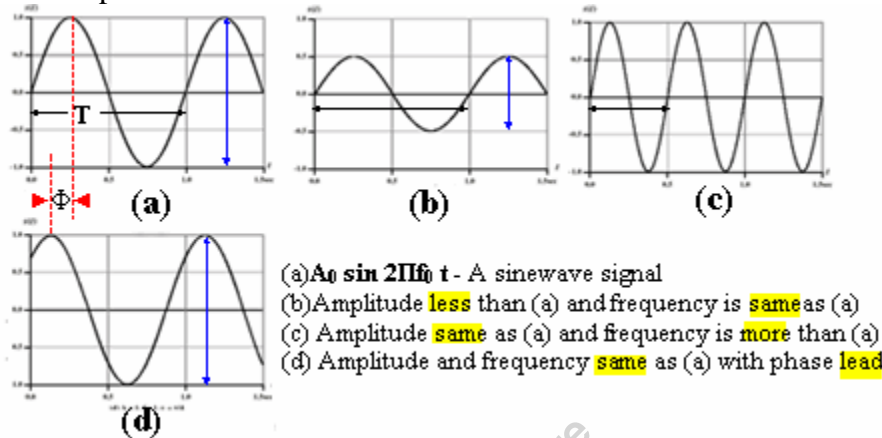


Fig 1.4.1 Different wave forms with different parameters

1.5 Bandwidth

Mathematically it can be shown that any complex waveform is a made of sine waveforms of different amplitudes and frequencies with varying phase relationships amongst each other.

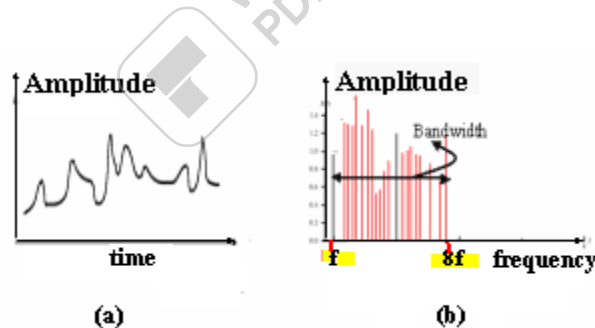


Fig 1.5.1 (a) An analog signal(b) Its various frequency components.

In the above figure the analog signal in fig 1.5(a) has several frequency components of different amplitude as shown in fig 1.5(b). Thus the analog signal encompasses a wide range of frequency spectrum. In analog systems the difference between highest frequency to lowest frequency component is called **bandwidth** (here it is $8f - f = 7f$).

Bandwidth merely (مجرد) specifies a range of frequencies, from the lowest to the highest, that the channel can carry or that are present in the signal. It is one way of describing the maximum amount of information that the channel can carry.

Bandwidth is expressed differently for analog and digital circuits. In analog technology, the bandwidth of a circuit is the difference between the lowest and highest frequencies that can pass through the channel. Engineers measure analog bandwidth in kilohertz or megahertz.

=====Course One=====

Rate of transmission = (bits per second)

1kbps = 1000bps

1Mbps = 10^6 bps

1Gbps = 10^9 bps

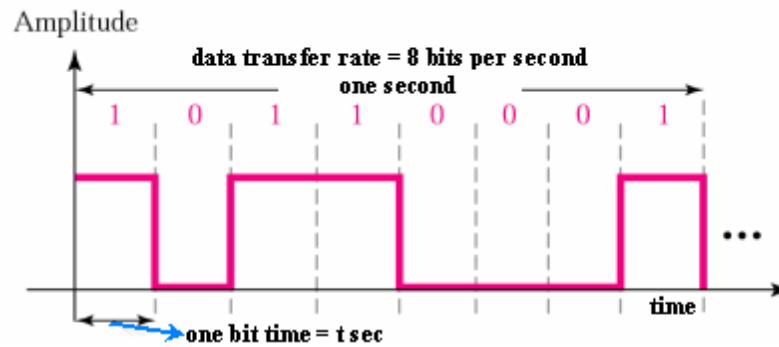


Fig 1.5.2 Relation between bit time and rate

In data communication, the bandwidth is the amount of information that can pass through the channel or medium. Engineers measure digital bandwidth in bits, kilobits, or megabits per second. The kilohertz of an analog bandwidth and the kilobits per second of digital bandwidth for the same circuit are not necessarily the same and often differ greatly.

In principle digital signals require a large bandwidth (theoretically infinite!). The medium has to be of better quality to send digital signals. Most LANs use Manchester encoding because of its self-synchronizing property. Otherwise separate clock signals were to be transmitted along with data in order to inform about sender's transmission clock. In Manchester encoding there is a transition in each bit interval and this property serves as clock also.

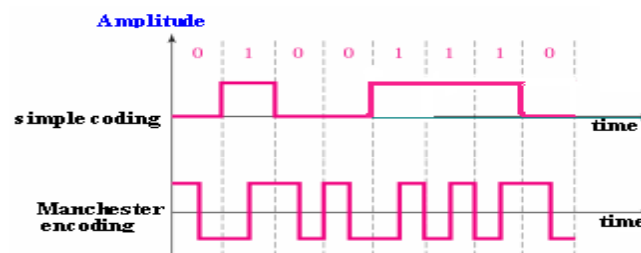


Fig 1.5.3 Manchester encoding

1.6 Noise

In any type of communication, noise is the biggest impairment (ضعف, اختلال). The received signal at the receiver end will consist of transmitted message plus additional unwanted signal that are inserted somewhere between transmitter and receiver distorting the message.

There are several types of noise sources, which can abruptly (بشكل مفاجئ) affect the quality of reception signal. The following are some of them

- **Thermal noise:** Due to thermal agitation (هياج) of electrons. Present in all electronic devices and is the function of temperature.

=====Course One=====

- **Impulse noise:** Due to electromagnetic interference (EMI). They may be present in power lines, or in nature (lightning.. etc)
- **Delay distortion:** Due to non-uniform velocities(سرع) of signals of different frequencies traveling in a guided media. Various frequencies of a message signal will arrive at different delays resulting in distortion.

1.7 Channel capacity

The maximum rate at which data can be transmitted over a communication channel under given conditions is referred as the channel capacity.

There are four parameters involved in the evaluation of channel capacity.

- **Data rate:** The rate at which data can be transmitted. Measured in bits per second
- **Bandwidth:** The bandwidth of the transmitted signal. Measured in cycles per second (Hz).
- **Noise:** The average level of unwanted signals over communication path. Expressed as the ratio between signal and noise.
- **Error rate:** The rate at which error can occur.

Then the channel capacity

(in cycles per second) according to **Shannon's** theorem is given by:

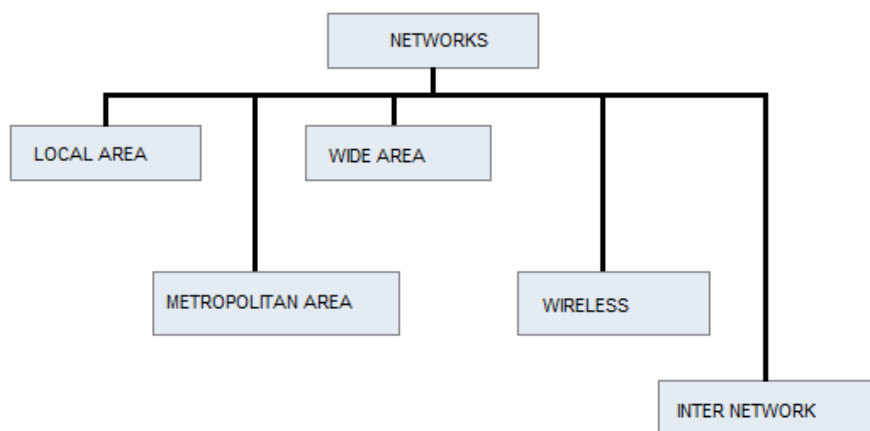
$$C = B \log_2 (1+SNR)$$

Where

- **C** in Cycles per second and this is error free capacity
- **B** is the bandwidth in Hertz.
- **SNR** = $10 \log_{10}$ (Signal power/Noise power)

Normally this theorem represents maximum channel capacity. Actual values may be much less than as given by the formula. One reason for this is the SNR ratio. The SNR ratio assumes only white noise (thermal noise) where as other noise like impulse noise, attenuation noise and delay noise are not taken into account.

3. Types of Communication Networks



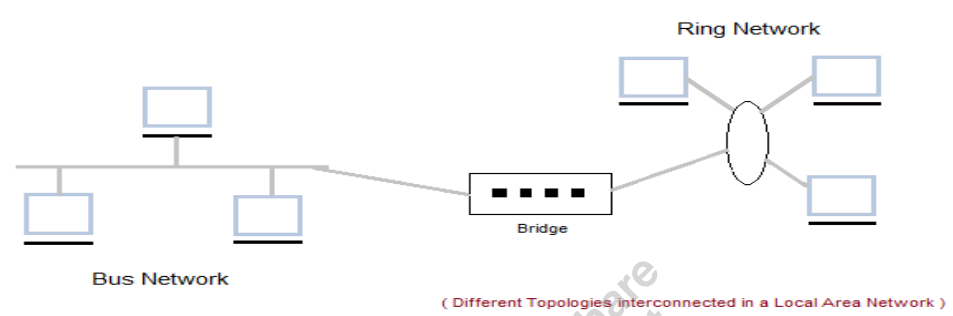
=====Course One=====

1. Local Area Network (LAN)

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

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

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

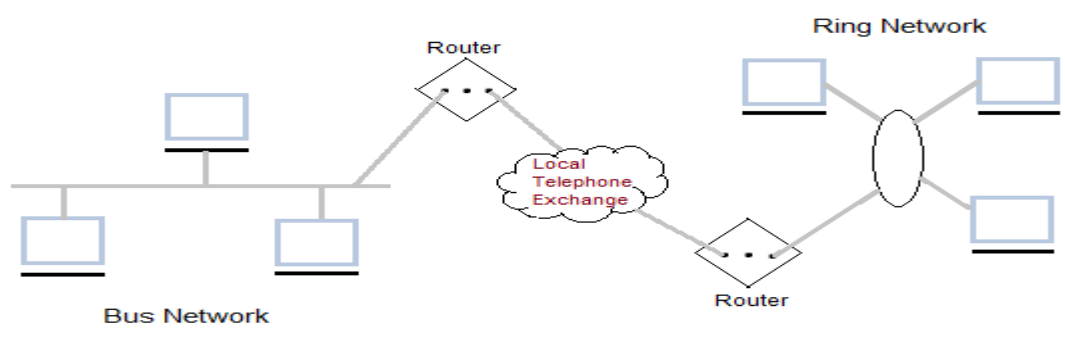


3.1 Applications of LAN

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

2. Metropolitan Area Network (MAN)

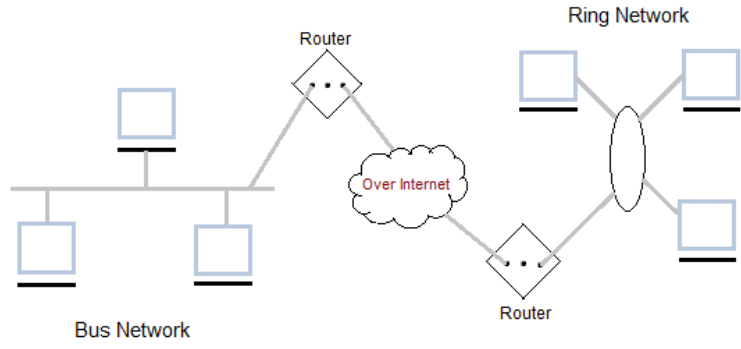
It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company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



=====Course One=====

3. Wide Area Network (WAN)

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



4. Wireless Network

It is the fastest growing segment of computer. They are becoming very important in our daily life because wireless connections are not possible in cars or aeroplane. We can access Internet at any place avoiding wire related troubles. These can be used also when the telephone systems gets destroyed due to some calamity/disaster. WANs are really important now-a-days.



5. Inter Network(InterNet)

When we connect two or more networks then they are called internetwork or internet. We can join two or more individual networks to form an internetwork through devices like routers gateways or bridges.

1.8 Modes of transmission

When we talk of data communication we are primarily concerned with serial transmission although other types of transmission does exists. In serial transmission the data is transmitted bit by bit as a stream of 0s and 1s.

The following key factors have to be observed regarding serial transmission:

=====Course One=====

- **Timing problem:** There should be some mechanism to know when the bit has arrived and at what rate the next bit is going to arrive at the serial input terminal of the receiver. We will see this can be accomplished in two ways.
- **Error detection:** Provision should be made (during transmission itself) to verify the integrity of the received data. Like parity, checksum bits.
- **Error correction:** Ability to correct the data in case of corrupted data reception.

Timing problems require a mechanism to synchronize the transmitter and receiver.

1.10 Multiplexing

By **Multiplexing** different message signals can share a single transmission media (The media can be guided or unguided). All they need is they should either differ in their frequency slot or wavelength slot or in time slot.

1.10.1 Frequency Domain Multiplexing (FDM)

In this each message signal is modulated by different radio frequency signals called RF carriers. At the receiving end filters are used to separate the individual message signals. Then they are demodulated (removing the RF carrier) to retrieve back the original messages.

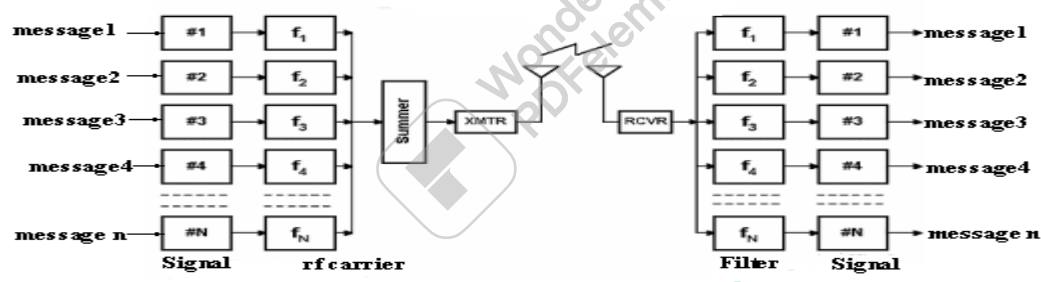


Fig 1.10.1 Frequency domain multiplexing

The Radio /TV broadcasting are the best examples for frequency domain multiplexing. Several individual stations broadcast their programs in their own allotted frequency band sharing the same unguided media. The receiver tunes his set according to his choice. The cable TV network is another example of Frequency domain multiplexing employing guided media.

1.10.2 Wavelength Division Multiplexing (WDM)

Wavelength division multiplexing is a type of FDM scheme used in fiber optical communications where various wavelengths of infrared light are combined over strands of fiber. Optical communication with few exceptions are digital since light transmitters and receivers are usually poorly suited for analog modulation.

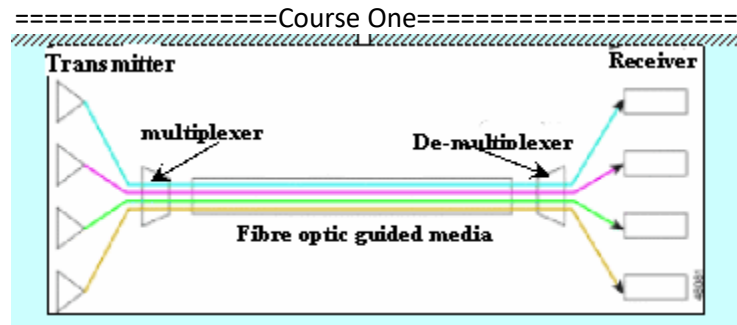


Fig 1.10.2 A Typical wavelength division multiplexer

1.10.3 Time Domain Multiplexing (TDM)

A type of multiplexing where two or more channels of information are transmitted over the same media by allocating a different time interval ("slot" or "slice") for the transmission of each channel. The channels take turns to use the media. Some kind of periodic synchronizing signal or distinguishing identifier is usually required so that the receiver can tell which channel is which.

A typical practical setup combines a set of low-bit-rate streams, each with a fixed and pre-defined bit rate, into a single high-speed bit stream that can be transmitted over a single channel.

The main reason to use TDM is to take advantage of existing transmission lines. It would be very expensive if each low-bit-rate stream were assigned a costly physical channel (say, an entire fiber optic line) that extended over a long distance.

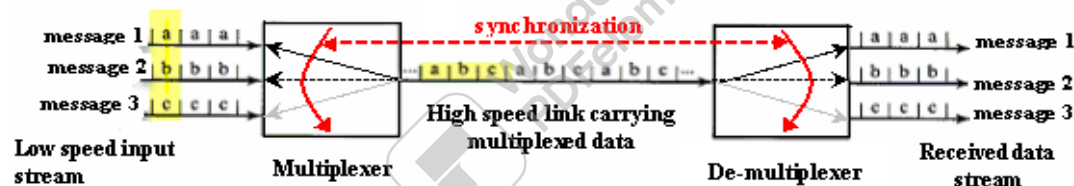


Fig. 1.10.3 Time division multiplexing.

1.11 Network Models

When people to people, machines to machines started communicating with each other the networking technology started picking up. In order to communicate systems with heterogeneous configurations there was a need for standardization.

TCP/IP(Transmission Control Protocol / Internet Protocol) is the oldest one and has become defacto standard for all networks. OSI model is much more refined and let us hope all future models will be based on this.

Each layer takes input from the upper layer, performs its duty and hands over to the lower layer.

OSI (Open Systems Interconnection) was developed as a theoretical model. Studying OSI model gives better perception of the various intricacies involved in data communication and networking.

1.11.1 The OSI Model

It has seven layers. They are separate but related. Each layer has well defined tasks and provides services to the corresponding lower layer while in transmission. In receiving mode the lower layer provides the necessary services to the upper layer. Any changes in one layer should not require changes in other layers.

=====Course One=====

This kind of standardization allows communication across all types of computers.

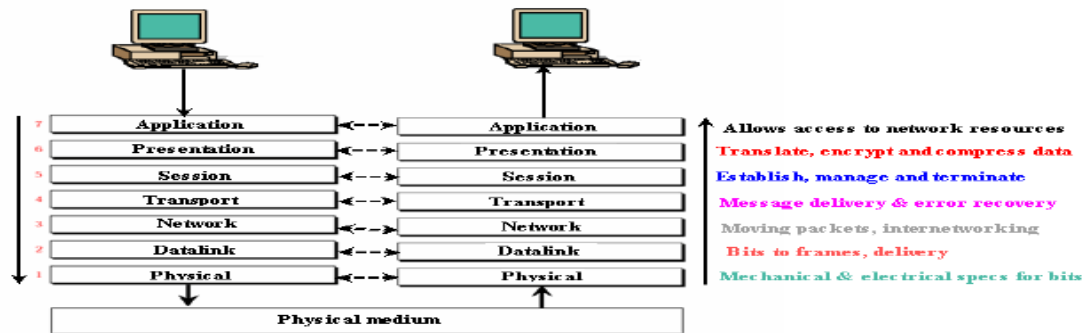


Fig 1.11.1 The OSI Layers and their functions

Easy to remember these layers!.....

Please **Do Not Touch Shiva's Pet Alligator**

The Seven Layers of OSI and their conceptual services -

- **Application - (layer 7)** Allows applications to use the network. The user may want to access the network for various purposes. Like for sending e-mail, transferring a file, surfing the web, accessing remote computer's resources etc.. For every task mentioned above there is a dedicated service.

Services – e-mail, news groups, web applications, file transfer, remote host, directory services, network management, file services

- **Presentation - (layer 6)** Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression. Messages are sent between layers

Services – POP, SMTP (e-mail, Post office protocol, Simple Mail Transfer Protocol), Usenet (for news groups), HTTP (hypertext transfer protocol for web applications), FTP, TFTP (File transfer protocol, trivial FTP for file transfer), Telnet (Terminal Network,

A general purpose program enabling remote login into some other computer and function as if it is directly connected to that remote computer), Domain name server (finding ip addresses for domain names), SNMP (Simple Network Management Protocol).

- **Session - (layer 5)** Allows applications on connecting systems to standard ports & establish a session. Provides synchronization between communicating computers. Messages are sent between layers

Services – Various port numbers are POP(25), USENET(532), HTTP(80), FTP(20/21), Telnet(23), DNS(53), SNMP(161/162) etc..

- **Transport - (layer 4)** Responsible for packet handling. Ensures error-free delivery. Repackages messages (while receiving), divides messages into smaller packets (while transmitting), and handles error handling. segments of message fragments are sent between layers

Services - TCP - connection-oriented communication for applications to ensure error free delivery;

UDP - connectionless communications and does not guarantee packet delivery between transfer points

=====Course One=====

- **Network - (layer 3)** Translates system names into addresses. Responsible for addressing, determining routes for sending, managing network traffic problems, packet switching, routing, data congestion, and reassembling data. Datagrams are sent between layers.

Services - Software & hardware addresses and packet routing between hosts and networks (IP). Two versions IP4(32 bits) & IP6(128 bits)

- **Data link - (layer 2)** Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. Data frames are sent between layers

Services – SLIP/PPP, 802.2 SNAP, Ethernet

- **Physical - (layer 1)** Transmits data over a physical medium. Defines cables, cards, and physical aspects. Data bits are sent.

Services - ISDN, ADSL, ATM, FDDI, CAT 1-5, Coaxial cable

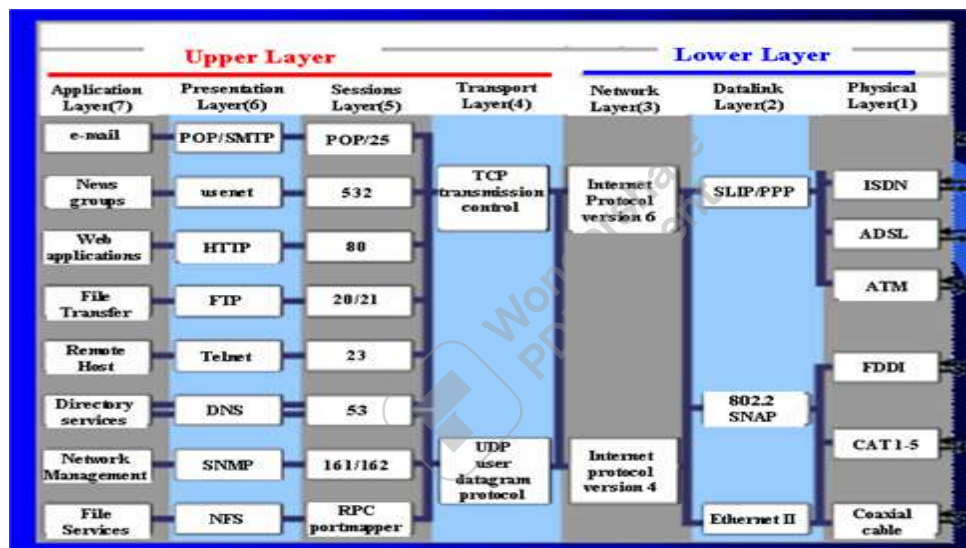


Fig 1.11.2 The OSI Model and their example services

1.11.2 The Internet model

There are four layers in this model. They are:

- I) Application Layer
- II) Transport Layer
- III) Network Layer
- IV) Data Link & Physical Layer.

1. **Application Layer:** Most of the responsibilities of the three top most layers of OSI model are in application layer of Internet model. The services are as depicted in the fig(1.14).
2. **Transport Layer:** It has two protocols. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is a reliable protocol that allows two application layers to converse with (التحدث مع) each other. While transmitting it

=====Course One=====

divides the stream of characters into manageable segments. While receiving it creates stream of characters for application layer from received segments of network layer. Its function is much more than as depicted in OSI model. fast delivery of packets is needed without worrying much about error control.

3. **Network Layer:** The main protocol is IP (Internet Protocol) is responsible for creating network layer packets called IP datagrams. The datagrams travel network to network or LAN to WAN and the packets may reach out of sequence. It is the responsibility of upper layers to put them into proper order.
4. **Datalink & physical Layer:** The Internet model does not discuss much about these layers making this protocol machine independent to a large extent. It is left to the user to choose the proper standard or protocol according to what they desire.

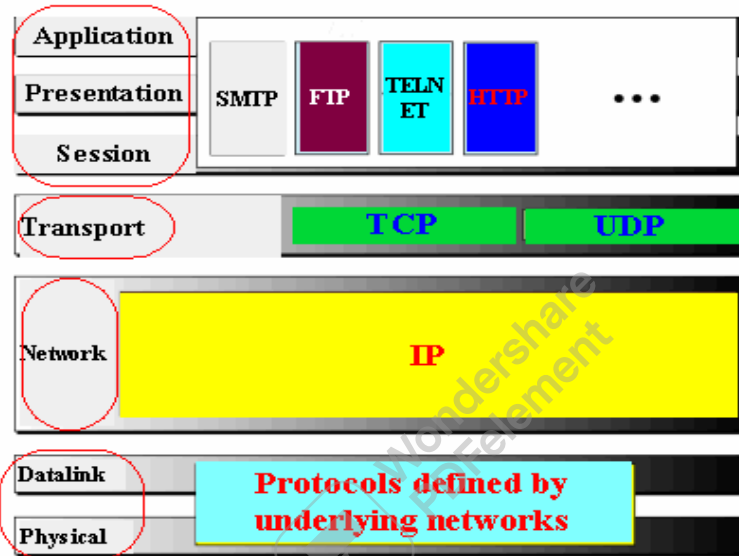


Fig 1.14 The Internet model

4. Network Topologies

4.1 Network Topology

The topology defines how the devices (computers, printers..etc) are connected and how the data flows from one device to another. There are two conventions while representing the topologies. The physical topology defines how the devices are physically wired. The logical topology defines how the data flows from one device to another.

Broadly categorized into

- I) Bus II) Ring III) Star IV) Mesh

=====Course One=====

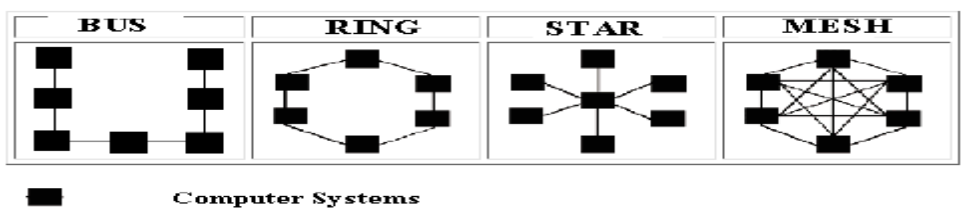


Fig 2.7.1 Outlines of various types of topologies

4.1 Bus topology:

In a bus topology all devices are connected to the transmission medium as backbone. There must be a terminator at each end of the bus to avoid signal reflections, which may distort the original signal. Signal is sent in both directions, but some buses are unidirectional. Good for small networks. Can be used for 10BASE5 (thick net), 10BASE2(thin net) or 10BROAD36 (broad band) co-axial bus standards.

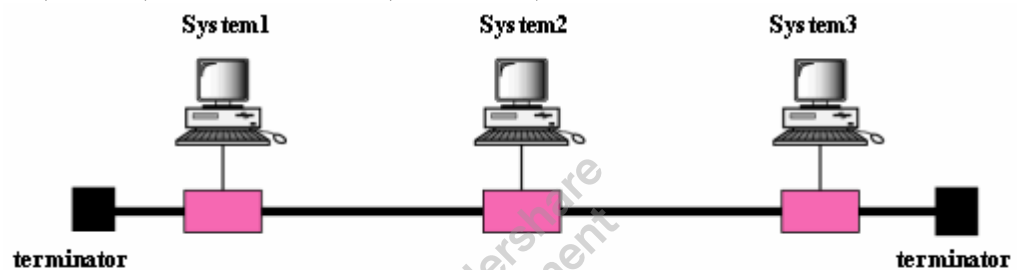


Fig 2.7.2 Physical topology of bus topology.

The main problem with the bus topology is failure of the medium will seriously affect the whole network. Any small break in the media the signal will reflect back and cause errors. The whole network must be shutdown and repaired. In such situations it is difficult to troubleshoot and locate where the break in the cable is or which machine is causing the fault; when one device fails the rest of the LAN fails.

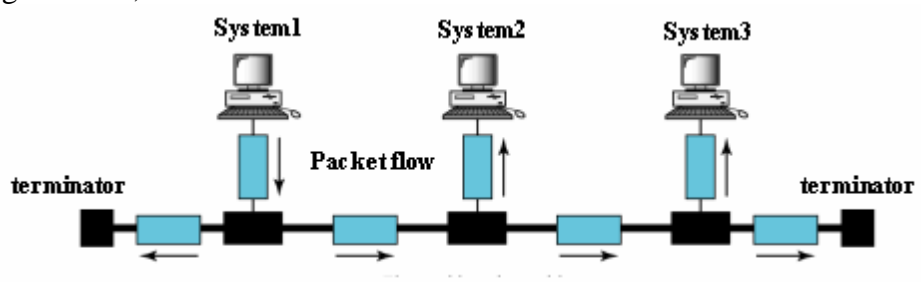


Fig 4.1 Logical topology illustration of bus topology.

4.2 Ring Topology

Ring topology was in the beginning of LAN area. In a ring topology, each system is connected to the next as shown in the following picture.

=====Course One=====

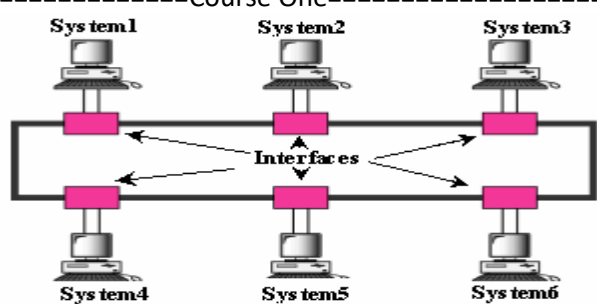


Fig. 4.2 Ring topology illustration.

Each device has a transceiver which behaves like a repeater which moves the signal around the ring; ideal for token passing access methods.

In this topology signal degeneration is low; only the device that holds the token can transmit which reduces collisions. If you see its negative aspect it is difficult to locate a problem cable segment; expensive hardware.

4.3 Star topology

In a star topology each station is connected to a central node. The central node can be either a hub or a switch. The star topology does not have the problem as seen in bus topology. The failure of a media does not affect the entire network. Other stations can continue to operate until the damaged segment is repaired.

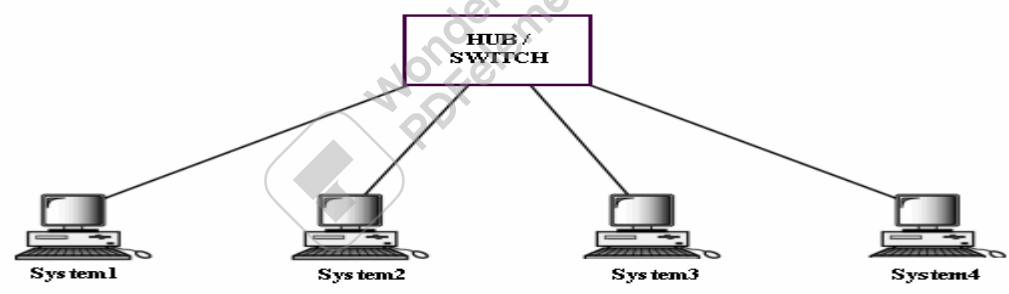


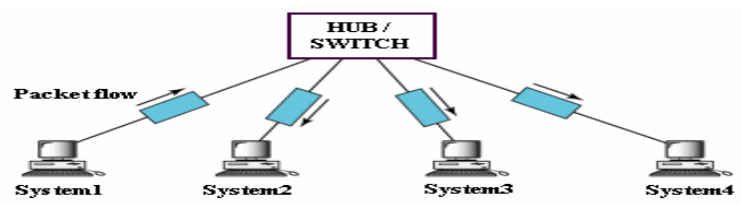
Fig 4.3. Physical topology of Star topology.

Commonly used for 10BASE5, 10BASE-T or 100BASE-TX types.

The advantages are cabling is inexpensive, easy to wire, more reliable and easier to manage because of the use of hubs which allow defective cable segments to be routed around; locating and repairing bad cables is easier because of the concentrators; network growth is easier.

The disadvantages are all nodes receive the same signal therefore dividing bandwidth; Maximum computers are 1,024 on a LAN.

Maximum UTP (Un shielded twisted pair) length is 100 meters; distance between computers is 2.5 meters.



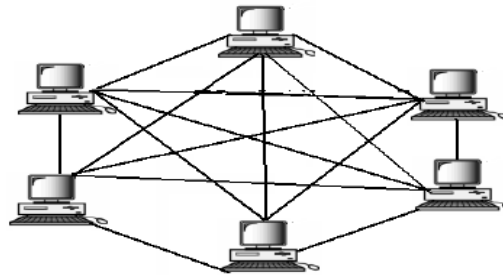
=====Course One=====

Fig 4.4 Logical topology of Star topology.

This topology is the dominant physical topology today.

4.5 Mesh topology

A mesh physical topology is when every device on the network is connected to every device on the network; most commonly used in WAN configurations Helps find the quickest route on the network; provides redundancy. Very expensive and not easy to set up.

**Fig 4.5** Physical topology of Mesh topology.

4.6 Hybrid topology

A hybrid topology is a combination of any two or more network topologies in such a way that the resulting network does not have one of the standard forms. For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit hybrid network topologies. A hybrid topology is always produced when two different basic network topologies are connected.

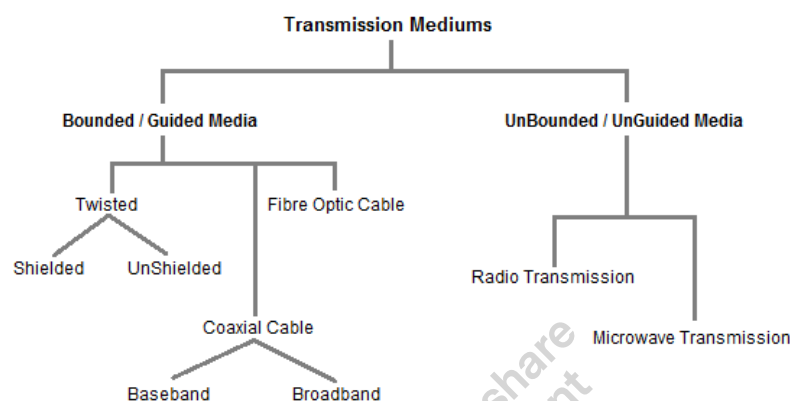
Why networking?

- **Sharing of hardware:** Computer hardware resources (Disks, Printers..)
- **Sharing of software:** Multiple single user licenses are more expensive than multi-user license. Easy maintenance of software
- **Sharing of information:** Several individuals can interact with each other Working in groups can be formed.
- **Communication:** (e-mail, internet telephony, audio conferencing video conferencing
- **Scalability:** Individual subsystems can be created and combine it into a main system to enhance the overall performance.
- **Distributed systems:** In a networked environment computers can distribute the workload among themselves keeping transparency to the end user.

=====Course One=====

5. Transmission Mediums in Computer Networks

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to travel between one point to another (from source to receiver). Transmission medium is the means through which we send our data from one place to another.



Factors to be considered while choosing Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

6.1. Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of **Bounded/ Guided** are discussed below.

A. Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points:

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μ s/km.
- Repeater spacing is 2km.

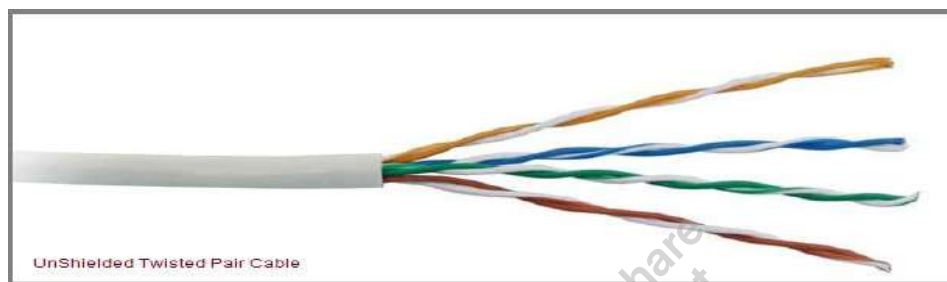
Twisted Pair is of two types :

a.Unshielded Twisted Pair (UTP)

b.Shielded Twisted Pair (STP)

a.Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ11** connector and 4 pair cable use **RJ-45** connector.



Advantages :

- Installation is easy, Flexible, Cheap, It has high speed capacity, 100 meter limit and Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages :

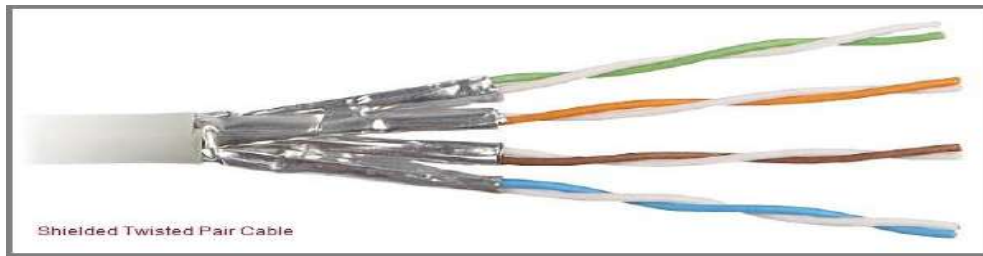
- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

b.Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

=====Course One=====



Advantages :

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages :

- Difficult to manufacture
- Heavy

B.Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

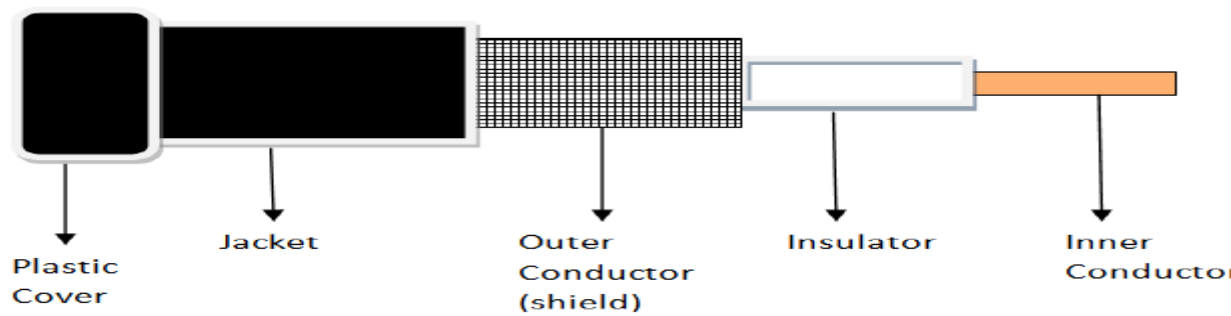
Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath.

The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.

=====Course One=====



There are two types of Coaxial cables :

A.BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

B.BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages :

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages :

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

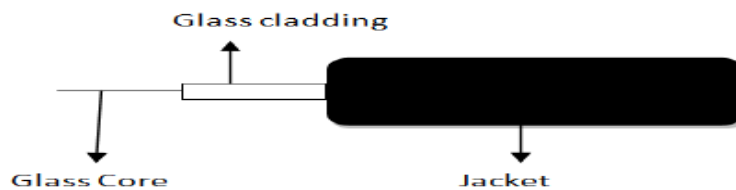
C.Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

=====Course One=====

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield. Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**



Advantages :

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages :

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

2.UnBounded/UnGuided Transmission Media

Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them. Types of unguided/ unbounded media are discussed below :

- Radio Transmission
- MicroWave Transmission

a.Radio Transmission

Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications.

Types of Propagation

Radio Transmission utilizes different types of propagation :

=====Course One=====

- **Troposphere** : The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet planes, wind is found here.
- **Ionosphere** : The layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

b.Microwave Transmission

It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.

There are 2 types of Microwave Transmission:

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

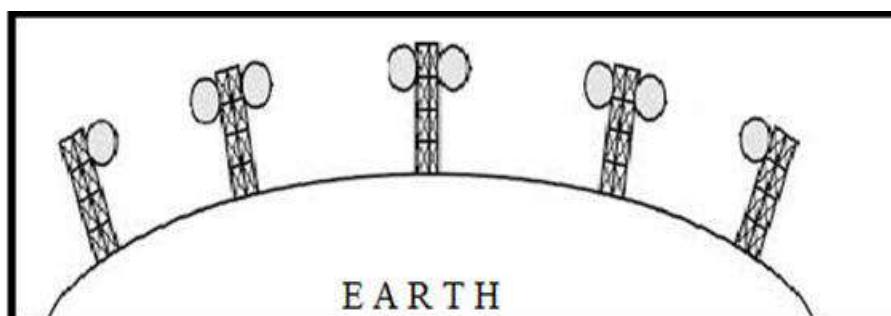
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly.

C.Terrestrial Microwave

For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world

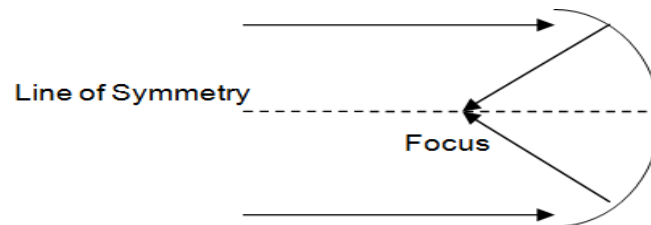


=====Course One=====

There are two types of antennas used for terrestrial microwave communication :

1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



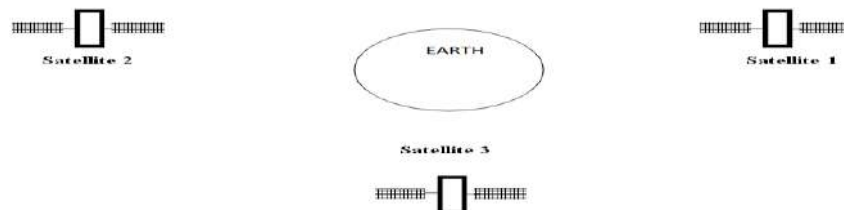
2. Horn Antenna

It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.

d.Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000KM above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave:

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave :

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave :

=====Course One=====

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

Part 2

FTP, SMTP, Telnet, HTTP,...
TCP, UDP
IP, ARP, ICMP
Network Interface

Reference: Charles L. Hedrick, "Introduction to the Internet Protocols", Rutgers University, <http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/>

A. What is TCP/IP?

- **TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network**
- **TCP stands for "Transmission Control Protocol"**
- **IP stands for "Internet Protocol"**
- **They are Transport layer and Network layer protocols respectively of the protocol suite**
- **The most well known network that adopted TCP/IP is Internet – the biggest WAN in the world**

What is a protocol?

- **A protocol is a collection of rules and procedures for two computers to exchange information**
- **Protocol also defines the format of data that is being exchanged**

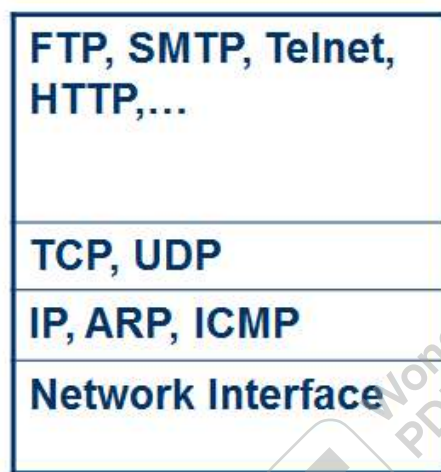
Why TCP/IP is so popular?

- **TCP/IP was developed very early**
- **Technologies were widely discussed and circulated in documents called "Request for Comments" (RFC) – free of charge**
- **Supported by UNIX operating system**

TCP/IP Mode

- Because TCP/IP was developed earlier than the OSI 7-layer mode, it does not have 7 layers but only 4 layers

TCP/IP Protocol Suite



OSI 7-layer

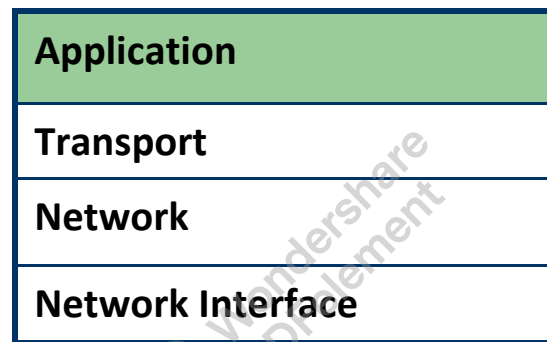


- Application layer protocols define the rules when implementing specific network applications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
 - FTP – File Transfer Protocol
 - For file transfer
 - Telnet – Remote terminal protocol
 - For remote login on any other computer on the network
 - SMTP – Simple Mail Transfer Protocol
 - For mail transfer
 - HTTP – Hypertext Transfer Protocol
 - For Web browsing
- TCP/IP is built on “connectionless” technology, each datagram finds its own way to its destination
- Transport Layer protocols define the rules of
 - Dividing a chunk of data into segments
 - Reassemble segments into the original chunk
- Typical protocols:
 - TCP – Transmission Control Protocol
 - Provide further the functions such as reordering and data resend
 - UDP – User Datagram Service
 - Use when the message to be sent fit exactly into a datagram
 - Use also when a more simplified data format is required

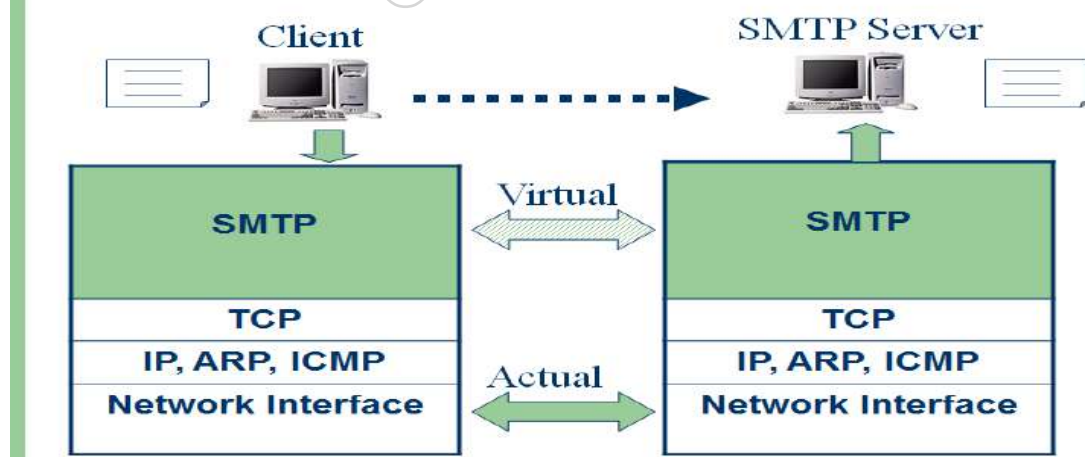
=====Course One=====

- **Network layer protocols define the rules of how to find the routes for a packet to the destination**
- **It only gives best effort delivery. Packets can be delayed, corrupted, lost, duplicated, out-of-order**
- **Typical protocols:**
 - **IP – Internet Protocol**
 - Provide packet delivery
 - **ARP – Address Resolution Protocol**
 - Define the procedures of network address / MAC address translation
 - **ICMP – Internet Control Message Protocol**
 - Define the procedures of error message transfer

Application Layer



B. Example: SMTP



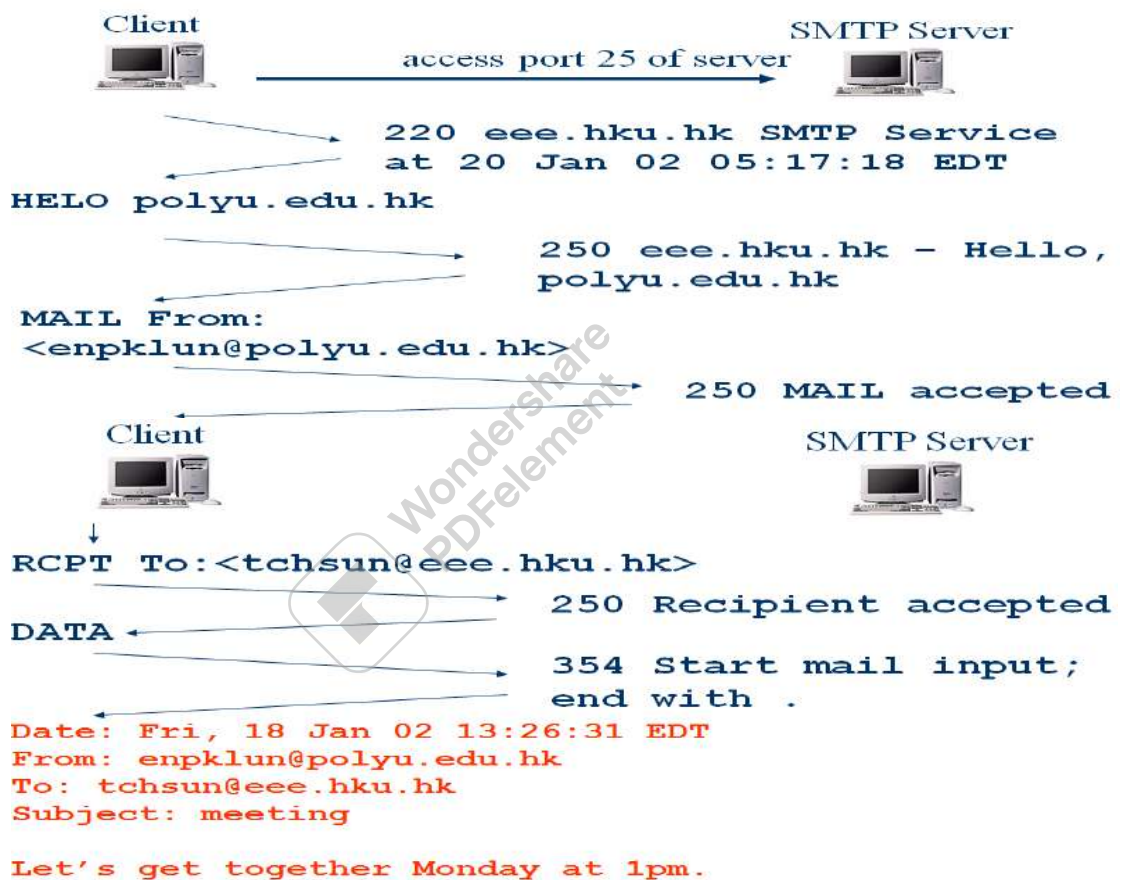
- The underlying layers have guaranteed accurate data delivery
- We need to make a lot of agreements with the server in application layer before sending mail
- Agree on how data is represented
 - Binary or ASCII
- Ensure the right recipient
 - There may be 1000 users served by the server

=====Course One=====

- Ensure the client has the right to send mail
 - Some clients are not welcome
- How to tell the server it is the end of the message
 - All mail looks the same :

Example: SMTP

The following mail is to be sent:
 Date: Fri, 18 Jan 02 13:26:31 EDT
 From: enpklun@polyu.edu.hk
 To: tchsun@eee.hku.hk
 Subject: meeting
 Let's get together Monday at 1pm.



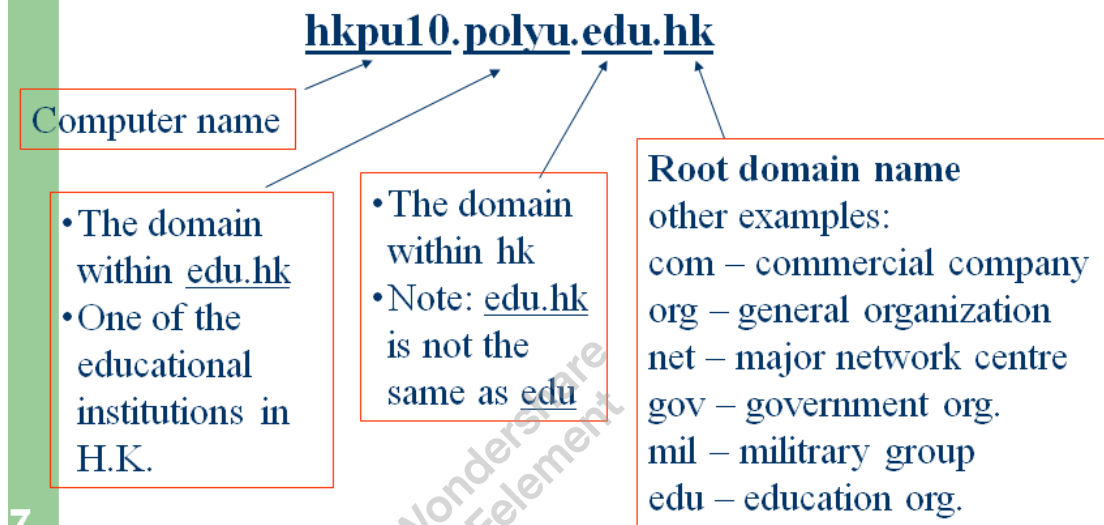
- The agreement made in the SMTP protocol
 - All messages use normal text
 - All ASCII characters
 - The responses all begin with numbers
 - To indicate the status when receiving the command
 - Some words are reserved words
 - HELO, MAIL, RCPT...
 - Mail ends with a line that contains only a period
- The information passed with the SMTP messages
 - The recipient name
 - The sender name
 - The mail

=====Course One=====

C. Domain Name:

- Every computer has a network address
 - e.g. 158.132.161.99
- To access a computer, we need to specify its network address
- Human beings are weak in memorizing numbers
- We prefer computer name or domain name
 - e.g. hkpu10.polyu.edu.hk
- Need a machine on the Internet to convert name to number

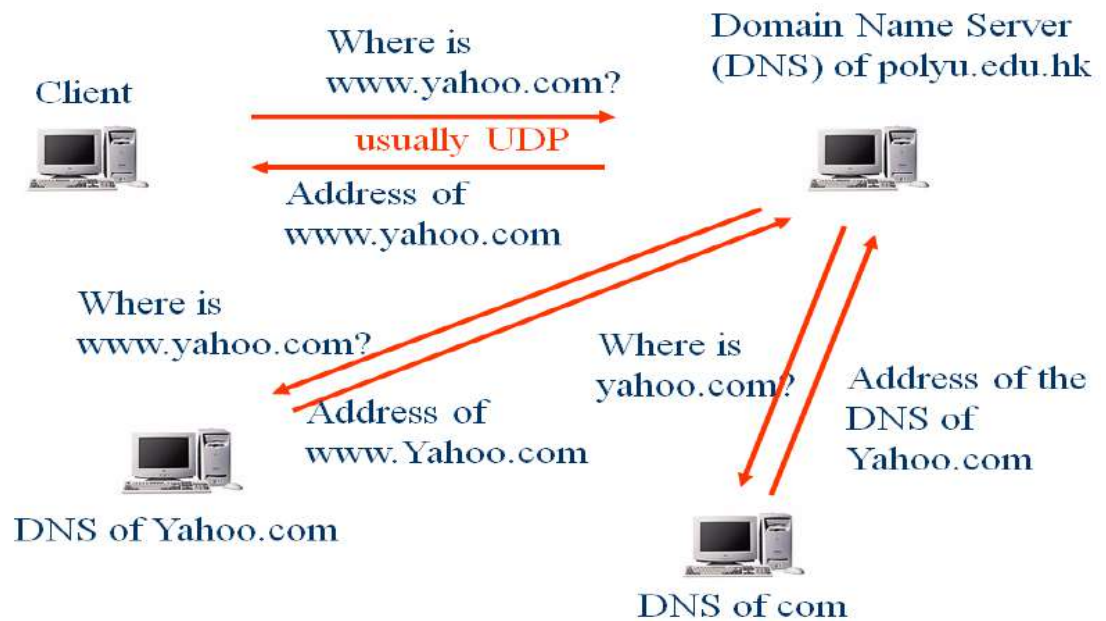
Example:



- An organization needs to **register its domain name**
 - e.g. **PolyU** has registered its name to the domain of **edu.hk**
- Once a domain name is assigned, the organization **is free to assign other names** belong to its domain
 - e.g. we can have

hkpu10.polyu.edu.hk
 smtp.polyu.edu.hk
 mail.polyu.edu.hk

=====Course One=====



- Nevertheless, such a complicated procedure **needs not perform** in most cases
- Client computers usually **remember** the answers that it got before
- It reduces the loading to the root DNS
- To further reduce loading, there can be many root DNS on the Internet
 - e.g. there are a few "com" root DNS

Transport Layer

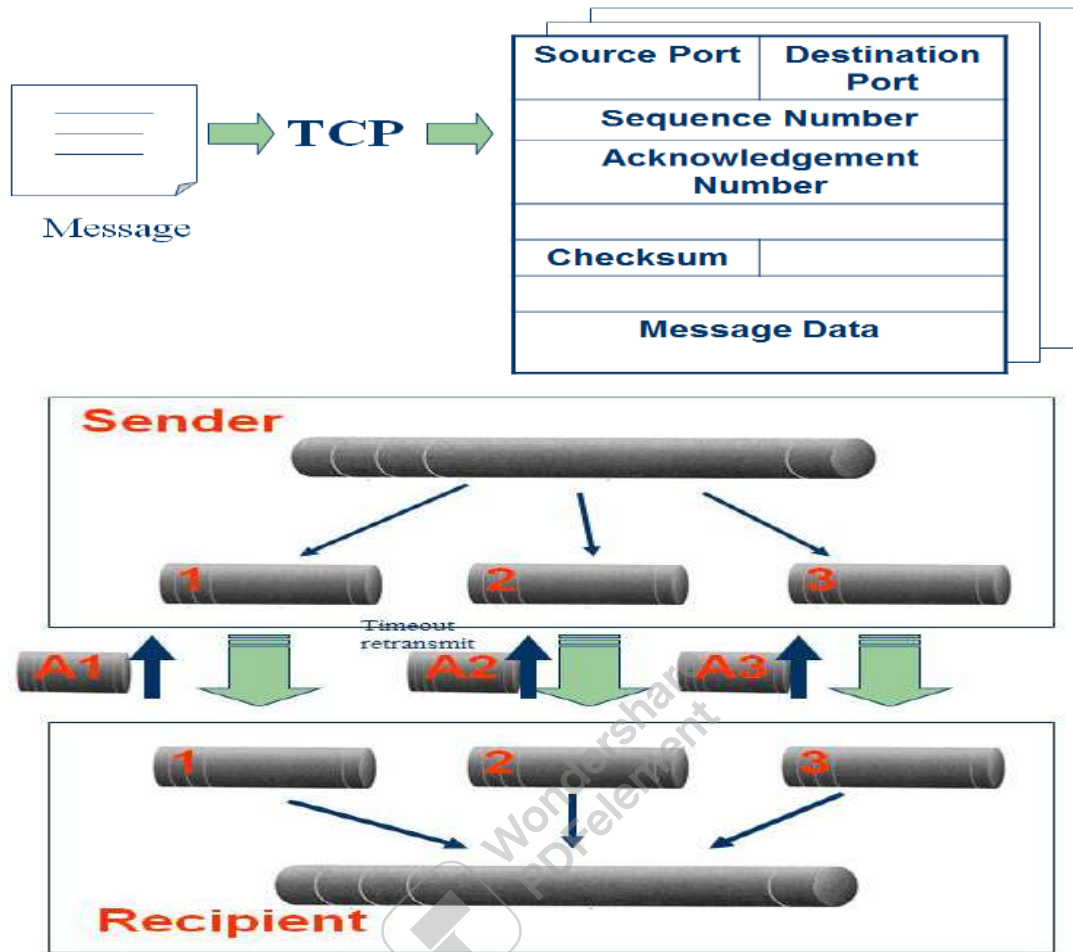
D. TCP and UDP

TCP – Transmission Control Protocol

- TCP is a **connection-oriented protocol**
 - Does not mean it has a physical connection between sender and receiver
 - TCP provides the function to allow a connection virtually exists – also called virtual circuit
- TCP provides the functions:
 - **Dividing a chunk of data into segments**
 - **Reassembly segments into the original chunk**
 - **Provide further the functions such as reordering and data resend**
- Offering a **reliable byte-stream delivery service**

=====Course One=====

Dividing and Reassembly



A Typical Procedure

- **Sender**
 - TCP divides a message into segments
 - Add sequence no.
 - Send the segments in sequence and wait for acknowledgement
 - If an acknowledgement for a segment is not received for a certain period of time, resend it until an acknowledgement is received
- **Recipient**
 - When receiving segments, send the acknowledgement with correct number
 - Reassembly the segments back to the message

Port Multiplexing

- A computer may perform a number of network applications at the same time
 - FTP + SMTP + HTTP, etc.
- Each computer has only one network address, how can it serve so many applications at the same time?

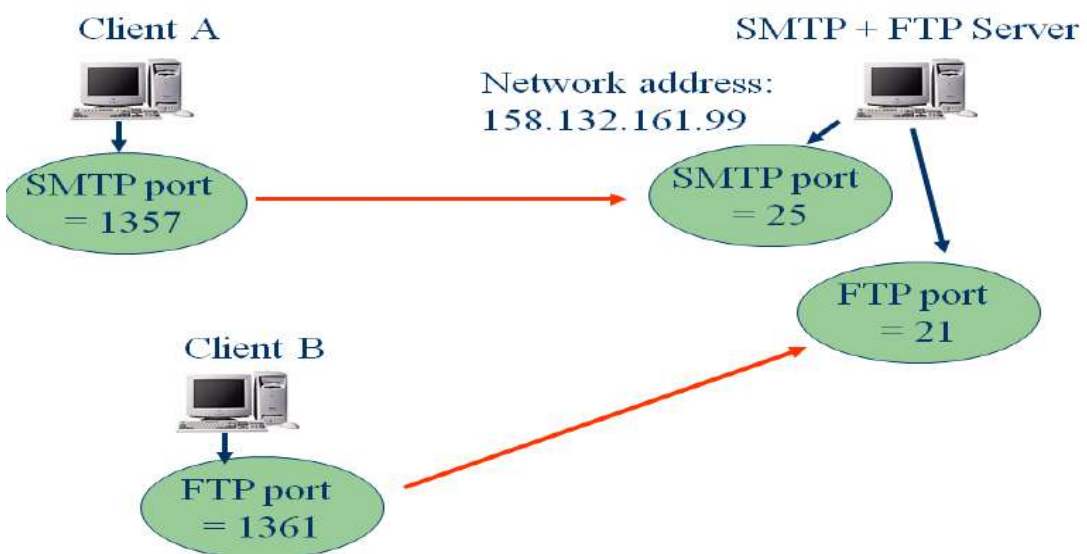
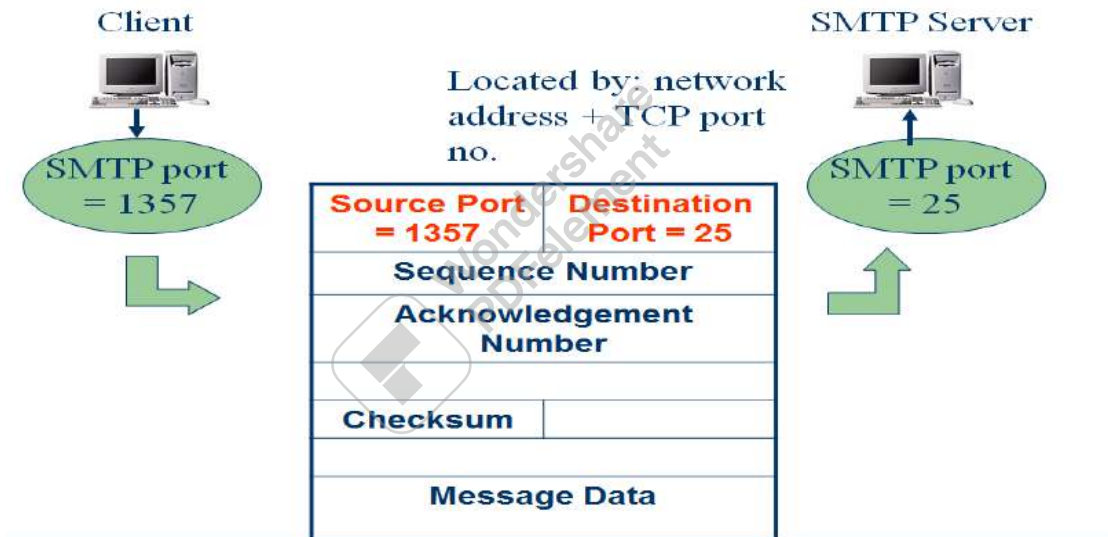
=====Course One=====

⇒ **by port multiplexing**



Well-known Port Numbers

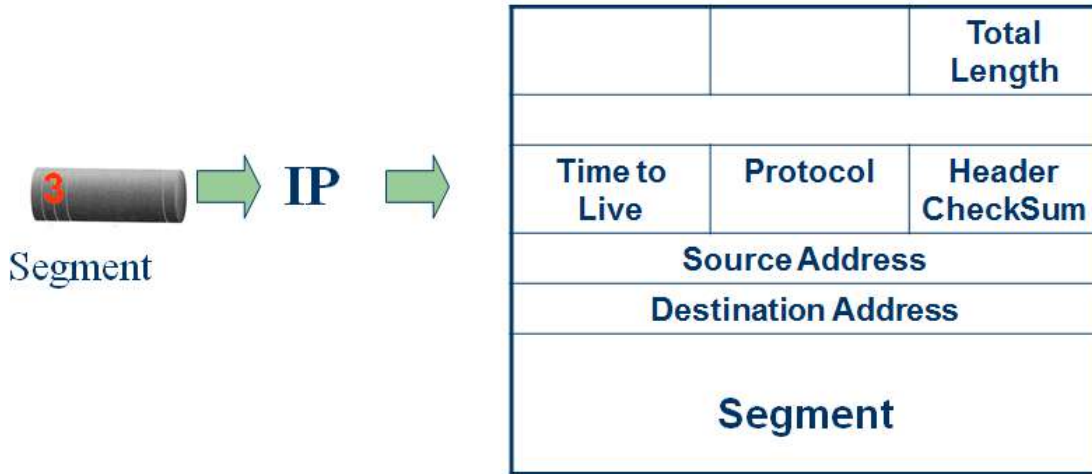
- Some port numbers are reserved for some purposes
 - Port 21: FTP – file transfer
 - Port 25: SMTP – mail transfer
 - Port 23: TELNET – remote login
 - Port 80: HTTP – Web access
- These port numbers are well known to all computers in the network
- E.g. whenever a client access port 25 of the server, it means the client needs SMTP service



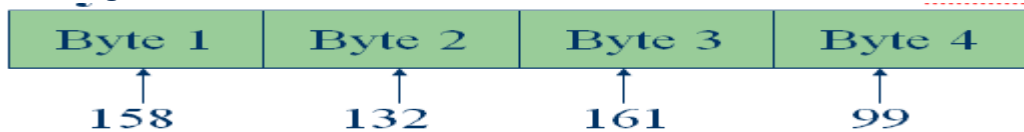
=====Course One=====

E. Network Addresses and Subnets

- A header is added to each segment in the Network layer



- **Total Length** – Total length of a packet (up to 65535 bytes)
- **Time to Live** – How many times this packet can be routed on the network (up to 255)
- **Protocol** – The transport layer protocol that the packet belongs to
 - TCP: 6
 - UDP: 17
 - ICMP: 1
- **Source address** – the network address of the computer that sends the data
- **Destination address** – the network address of the computer that the data is sending to
- Each computer (**host**) must have a unique network address (**or IP address for TCP/IP suite**)
- **Each IP address** is 32-bit long (four bytes)
- The four-byte address is written out as a.b.c.d
 - e.g.



- IP addresses are hierarchical
 - **network I.D.** and **host I.D.**
- Each Network I.D. on the Internet needs to be **registered** to the **Internet Assigned Number Authority**

Class A – for very large network

=====Course One=====



- Only 2^7 (63) networks can belong to this class
- Each network, there are 2^{24} hosts or computers
- Very few class A networks in the world
 - e.g. **Arpanet** – the earliest packet switched WAN (started 40 years ago)

Class B – for medium size network



- 2^{14} (16384) networks can belong to this class
- Each network, there are 2^{16} (65536) hosts or computers
- Polyu’s address belongs to this group
 - e.g. 158.132.14.1



Class C – for small network



- 2^{21} networks can belong to this class
- Each network, there are only 2^8 (256) hosts or computers

Class D – for multicast network



- Packets are addressed to a multicast group
- Not often supported on Internet

Special Addresses

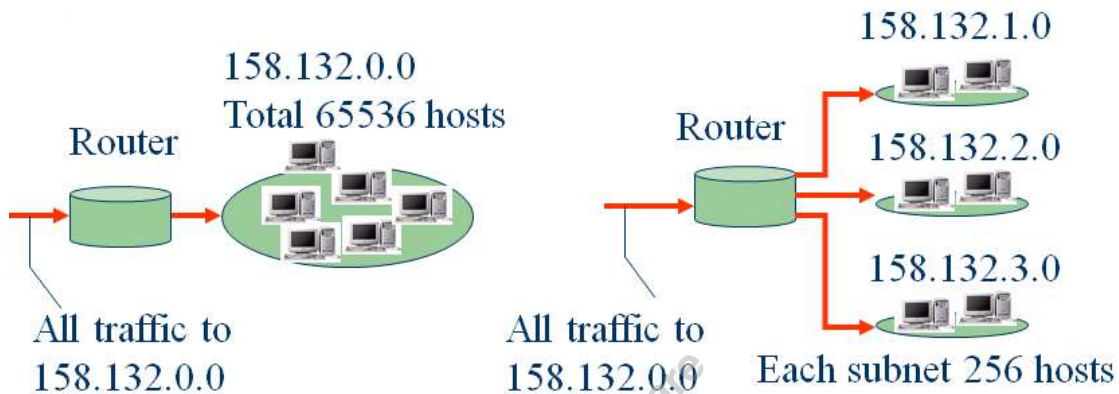
- Host I.D. = all '1's ⇒ Directed broadcast
 “Broadcast to all hosts in the network or subnetwork”, not assigned
- Host I.D. = all '0's ⇒ “This network”, not assigned

=====Course One=====

- **Network I.D. = 127** is reserved for loopback and diagnostic purposes, not assigned
- **Network I.D. + Host I.D. = all '1's** ⇒ Limited broadcast
 "Broadcast to all hosts in the current network", not assigned

Subnets

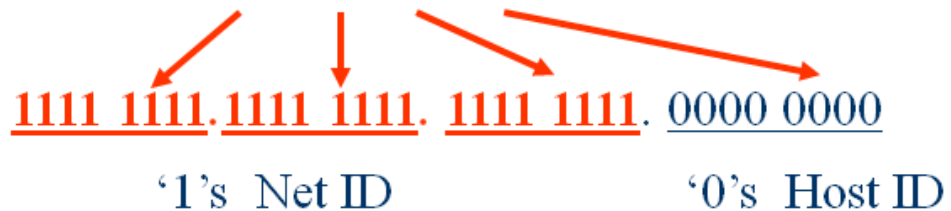
- Difficult to manage
- Usually subdivide into a few small subnets
- Subnetting can **also help to reduce broadcasting traffic**



Subnet Mask

- How does the router know which subnet a packet should go?
- For each interface of the router, a subnet mask is provided to redefine which part of the address is Net ID and which part is Host ID
- Become **classless** addressing

A subnet mask: 255.255.255.0



=====Course One=====

A packet with destination address 158.132.1.10

Routing Table

	S0	S1	S2
Subnet	158.132.1.0	158.132.2.0	158.132.3.0
Mask	255.255.255.0	255.255.255.0	255.255.255.0

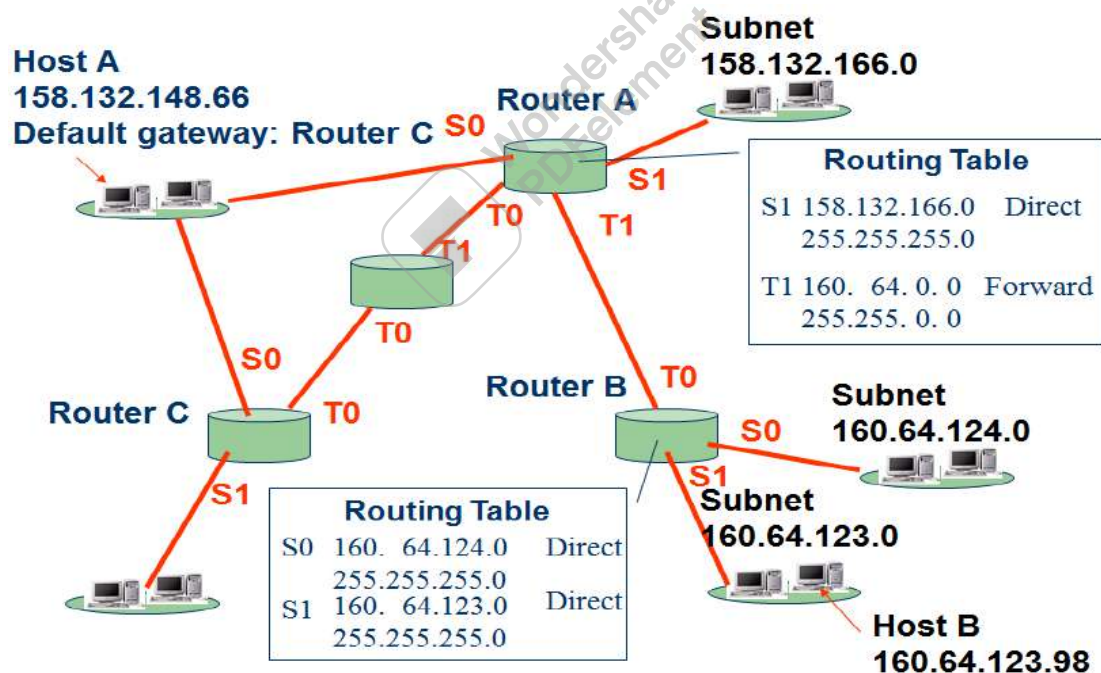
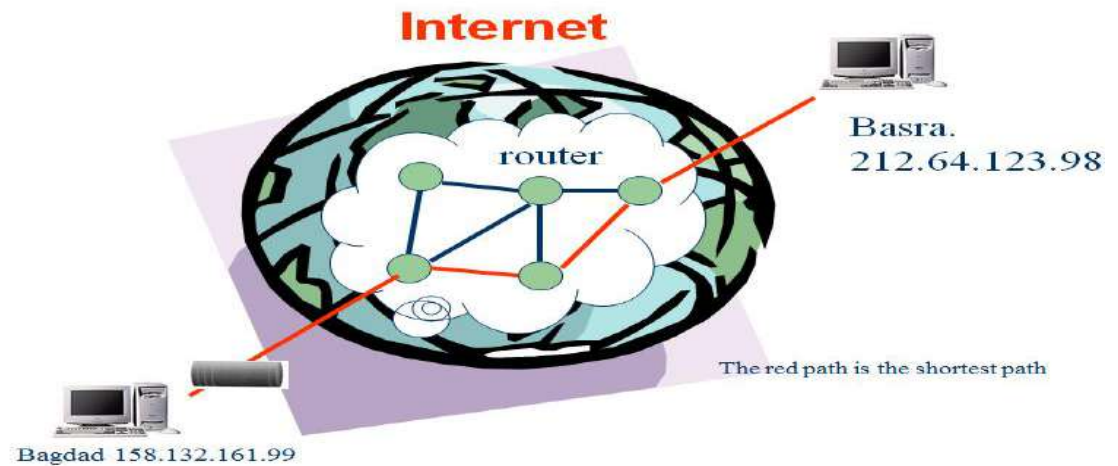
$$\begin{array}{r}
 158.132. 1. 10 \\
 \text{AND } 255.255.255. 0 \\
 \hline
 158.132. 1. 0
 \end{array}
 \qquad
 \begin{array}{r}
 1001 1110.1000 0100.0000 0001.0000 1010 \\
 \text{AND } 1111 1111.1111 1111.1111 1111.0000 0000 \\
 \hline
 1001 1110.1000 0100.0000 0001.0000 0000
 \end{array}$$

Advantage: easy to compute

F. Routing

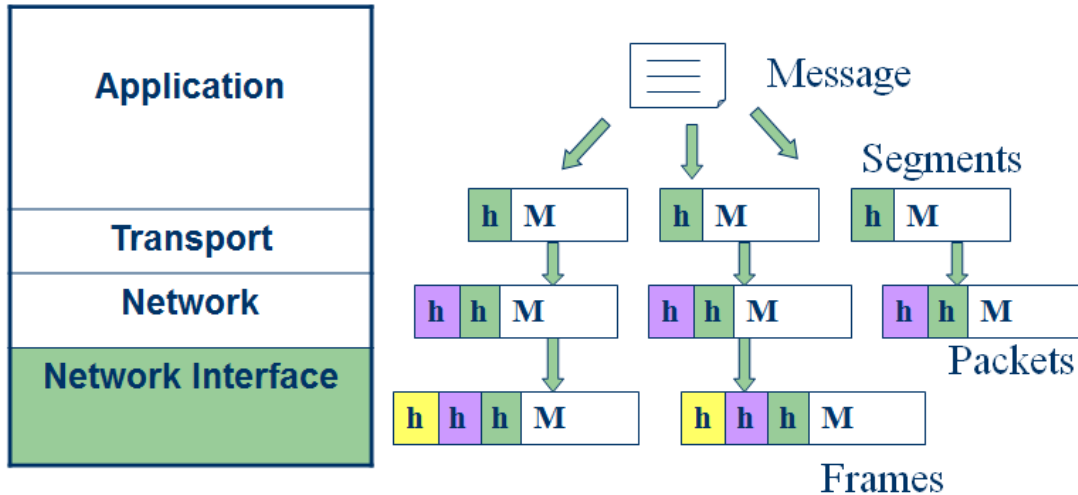
- How a packet finds its way to a computer in a network?
 - **By using Routers**
- **Routing** is the selection of a path to guide a packet from the source to the destination
- Criteria in selecting a path may be:
 - Shortest path
 - Quickest path
 - Cheapest path
- Each router has a **table** that records the estimated distance to all other routers
- If a router knows the entire network topology, the **shortest path** can be calculated
- To achieve this, routers broadcast Link State Advertisement to all other routers periodically
 - By means of **routing protocol**
- Each router knows the exact topology, and then calculates the shortest path
- In practice, it is not possible for a router to all paths. **Only the nearer ones are kept**
 - Hence can give **wrong estimation**

=====Course One=====



1. Host A wants to send a packet to Host B with address 160.64.123.98
2. Host A checks that 160.64.123.98 is not in the same network
3. Send packet to default gateway (Router C)
4. Default gateway finds that it cannot provide the best route for the packet, inform Host A to send the packet to Router A next time
5. Router C sends the packet to Router A
6. Router A checks from the table the packet should forward to Router B
7. Router B receives the packet and checks in its table the packet should directly deliver to subnet 160.64.123.0
8. Host B (160.64.123.98) receives the packet

Data Link and Physical Layers



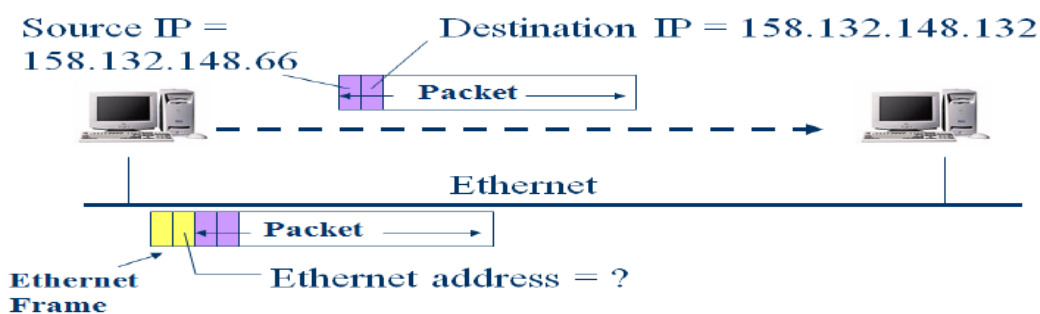
G. Ethernet Encapsulation and ARP

- An IP packet should be **encapsulated** into a frame for transmission by data link layer
- e.g. if Ethernet (or **IEEE 802.3**) is used:

Preamble	Des. Add	Sour. Add	Length	IP Packet	FCS
7 Bytes	1 Byte	2/6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

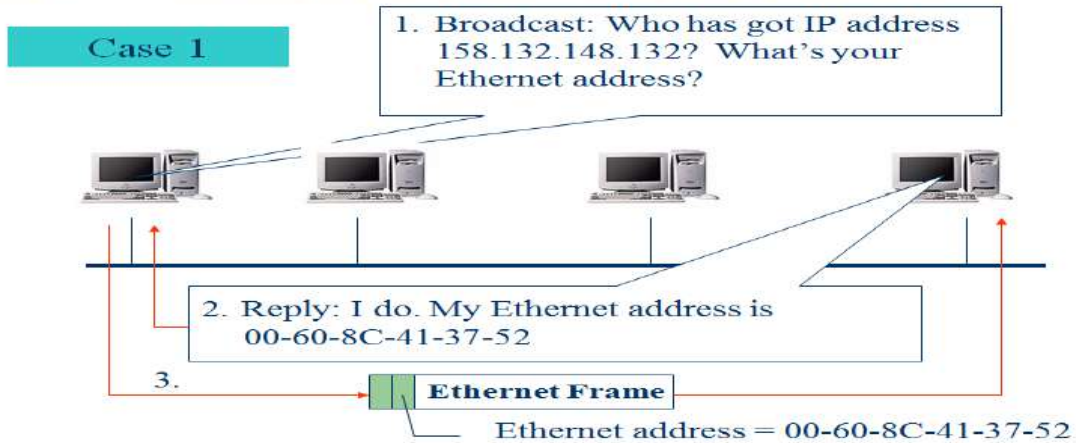
IEEE 802.3 Frame

- **Only the hardware address (MAC address) is unique to a host**
- **Need to convert a network address to MAC address**

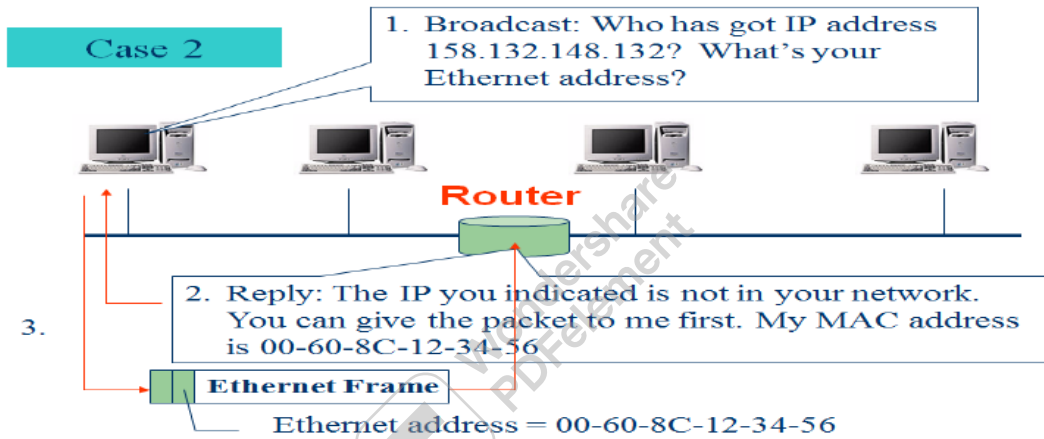


=====Course One=====

ARP – Address Resolution Protocol



ARP – Address Resolution Protocol



ARP Cache

- Will have a **heavy traffic** if so many ARP broadcast messages are generated
- Each host will have a **cache** to store the mappings (from IP to MAC address) that were obtained before

IP Address	MAC Address
158.132.148.80	00-60-8C-27-35-9A
158.132.148.28	02-60-8C-1A-37-49

- An entry will only be kept in the cache for a limited amount of time (say, 2 minutes)

Network Devices

Functions of network devices

- Separating (connecting) networks or expanding network
 - e.g. repeaters, hubs, bridges, routers, brouters, switches, gateways
- Remote access
 - e.g. 56K Modems and ADSL modems

A. Expanding Network

Networks cannot be made larger by simply adding new computers and more cables

- Less efficient !!

Can install components to

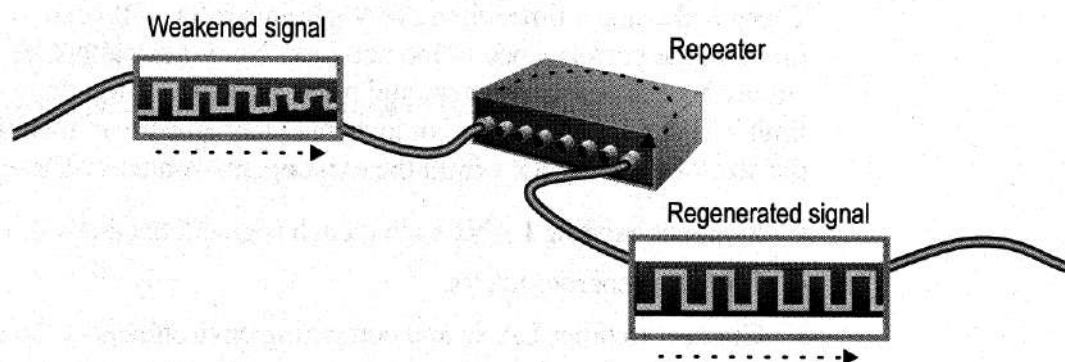
- segment (divide) large LAN to form smaller LANs
- connect LANs

Required components

- **Repeaters, bridges, routers, brouters, switches or gateways**

a. Repeaters and Hubs

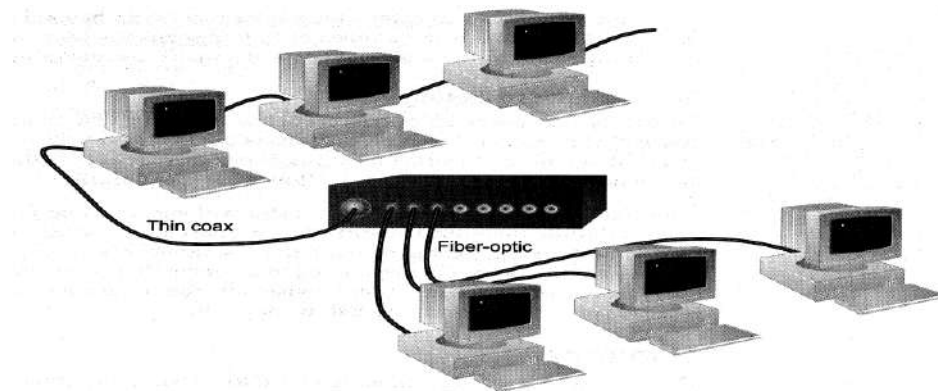
- Repeaters or hubs work at the OSI **physical layer** to **regenerate the network's signal** and resend them to other segments
- Primitive hub can be viewed as a multiport repeater
 - It regenerates data and broadcasts them to all ports



Limitations and Features

- Cannot link unlike segments
- Cannot join segments with different access methods (e.g. CSMA/CD and token passing)
- Do not isolate and filter packets
- Can connect different types of media
- The most economic way of expanding networks

=====Course One=====

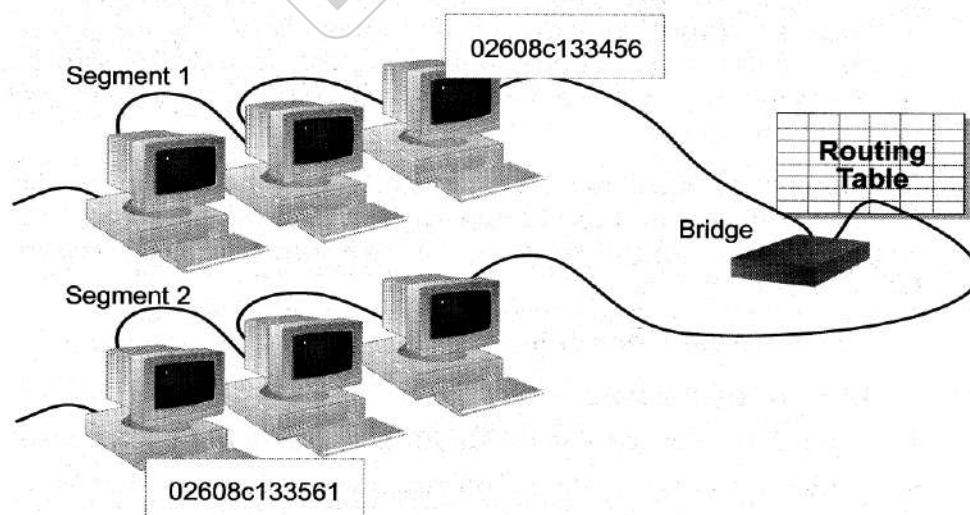


b. Bridges

- Has one input and one output
- Used to isolate network traffic and computers
- Has the intelligent to examine incoming packet source and destination addresses
- But cannot interpret higher-level information
- Hence cannot filter packet according to its protocol

How Bridges Work

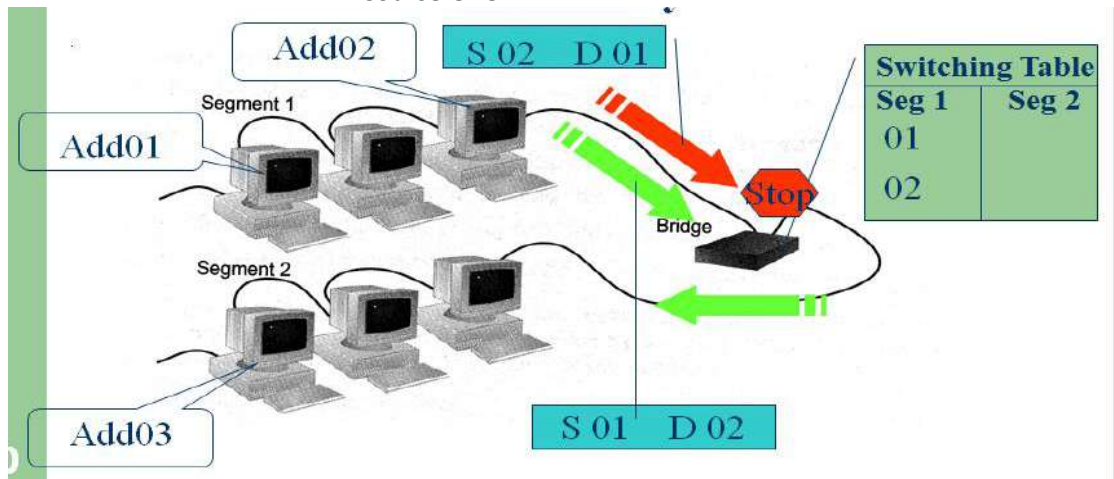
- Bridges work at the **Media Access Control Sub-layer** of the OSI model
- Routing table is built to record the segment no. of address
- If destination address is in the same segment as the source address, stop transmit
- Otherwise, forward to the other segment



Creating a Switching Table

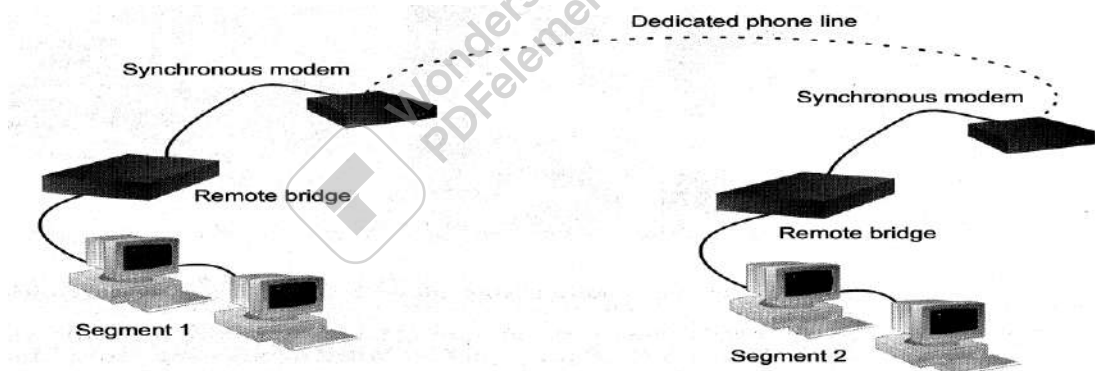
- Based on the addresses of the sending computers
- New addresses are added if they are not in the table

=====Course One=====



Remote Bridges

- Bridges are often used in large networks that have widely dispersed segments
- Remote bridges can be used to connect remote segments via data-grade telephone line

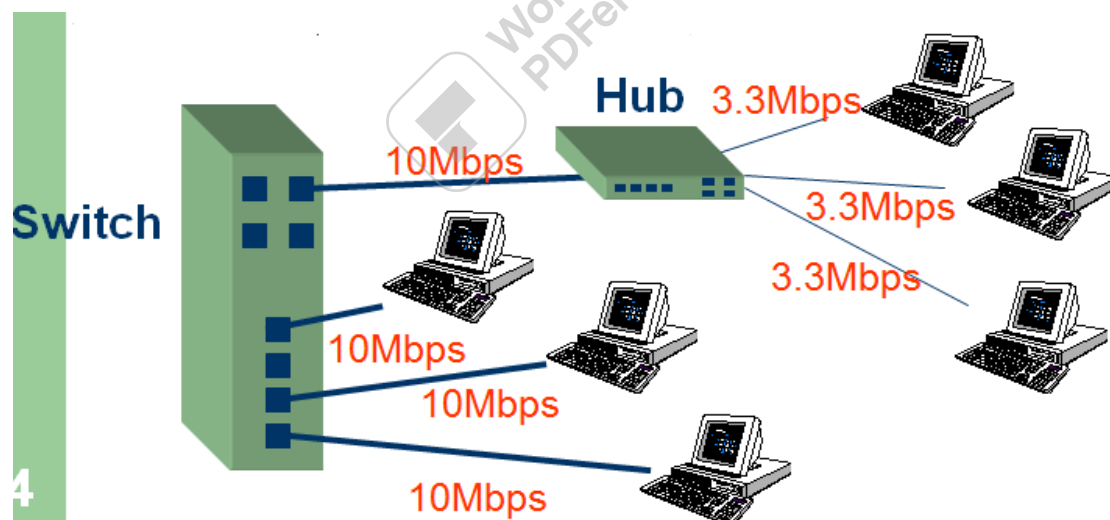
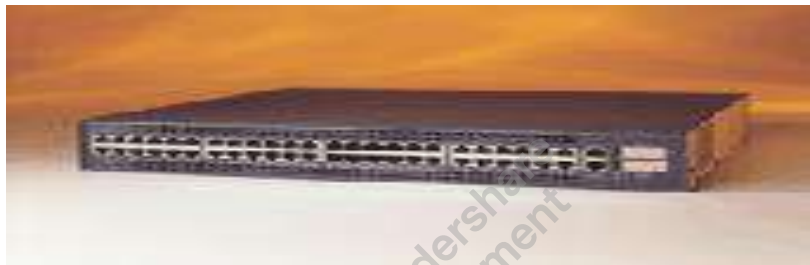


Differences between Bridges and Repeaters

	<i>Repeaters</i>	<i>Bridges</i>
<i>OSI layer</i>	Physical layer	Data link layer
<i>Data regeneration</i>	Regenerate data at the signal level	Regenerate data at the packet level
<i>Reduce network traffic</i>	No	Yes

c. Switches

- Switches operate at the **Data Link layer** (layer 2) of the OSI model
- Can interpret address information
- Switches resemble bridges and can be considered **as multiport bridges**
- By having multiports, can better use limited bandwidth and prove more cost-effective than bridge
- Switches divide a network into several isolated channels
- Packets sending from 1 channel will not go to another if not specify
- Each channel has its own capacity and need not be shared with other channels



Advantages of Switches

- Switches divide a network into several isolated channels (**or collision domains**)
 - **Reduce the possibility of collision**

=====Course One=====

- Collision only occurs when two devices try to get access to one channel
- Can be solved by buffering one of them for later access
- **Each channel has its own network capacity**
 - Suitable for real-time applications, e.g. video conferencing
- **Since isolated, hence secure**
 - Data will only go to the destination, but not others

Limitations of Switches

- Although contains buffers to accommodate bursts of traffic, can become overwhelmed by heavy traffic
 - **Device cannot detect collision when buffer full**
 - CSMA/CD scheme will not work since the data channels are isolated, not the case as in Ethernet
 - Some higher level protocols do not detect error
 - E.g. UDP
 - Those data packets are continuously pumped to the switch and introduce more problems

Method of Switching - Cut Through Mode

Preamble	Des. Add	Sour. Add	Length	Data	FCS
7 Bytes	1 Byte	2/6 Bytes	2/6 Bytes	46 - 1500 Bytes	4 Bytes

- Read the first 14 bytes of each packet, then transmit
- Much faster
- Cannot detect corrupt packets
- Can propagate the corrupt packets to the network
- Best suited to small workgroups

Method of Switching - Store and Forward Mode

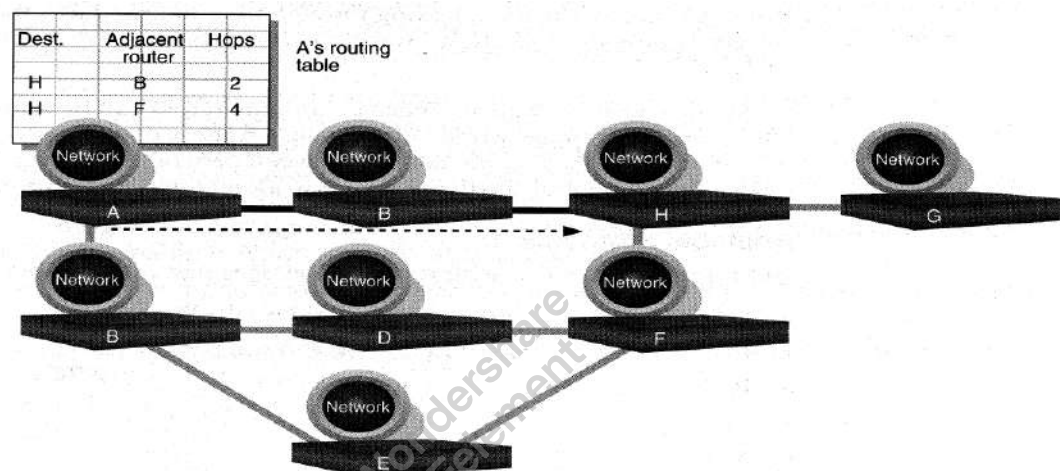
- Read the whole packet before transmit
- Slower than the cut-through mode
- More accurate since corrupt packets can be detected using the FCS

=====Course One=====

- **More suit to large LAN since they will not propagate error packets**
- **Facilitate data transfer between segments of different speed**

d. Routers

- **Layer 2 Switches cannot take advantage of multiple paths**
- **Routers work at the OSI layer 3 (network layer)**
- **They use the “logical address” of packets and routing tables to determine the best path for data delivery**

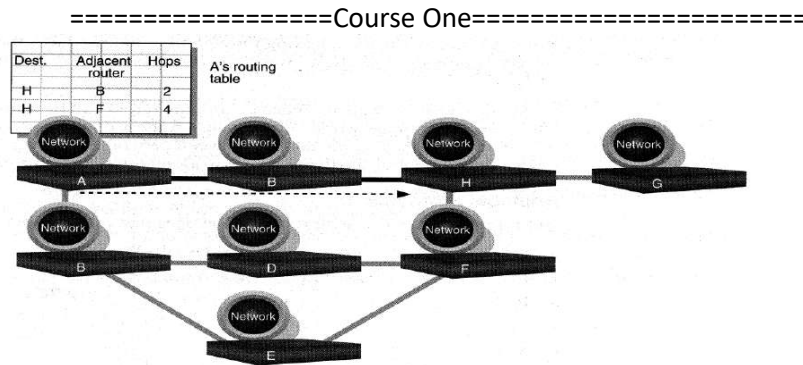


How Routers Work

- As packets are passed from routers to routers, Data Link layer source and destination addresses are stripped off and then recreated
- Enables a router to route a packet from a TCP/IP Ethernet network to a TCP/IP token ring network
- **Only packets with known network addresses will be passed - hence reduce traffic**
- Routers can listen to a network and identify its busiest part
- **Will select the most cost effective path for transmitting packets**

How Routing Table is formed

- Routing table is formed based on communications between routers using “Routing Protocols”
 - Routing Protocols \neq Routable Protocol
- Routing Protocols collect data about current network status and contribute to selection of the best path



Routing Protocol Example - RIP for IP Routing

- **RIP (Routing Information Protocol)** — the oldest one
- Use no. of hops between nodes to determine best path
- Does not consider the network congestion condition
- Broadcast every 30 sec the routing table to neighbouring routers to convey routing information
- RIP is limited to interpreting a maximum of 16 hops
- Not suitable for large network (e.g. Internet)
- Can create excessive network traffic due to broadcasting
- May take a long time to reach the far reaches

Routing Protocol Example - OSPF for IP

- **OSPF - Open Shortest Path First**
- Make up the limitations of RIP - can coexist with RIP
- In general case, best path refers to the shortest path
- In case of traffic congestion, can go a longer path
- Each router maintains a database of other router's links
- If link failure notice is received, router can rapidly compute an alternate path
- Require more memory and CPU power

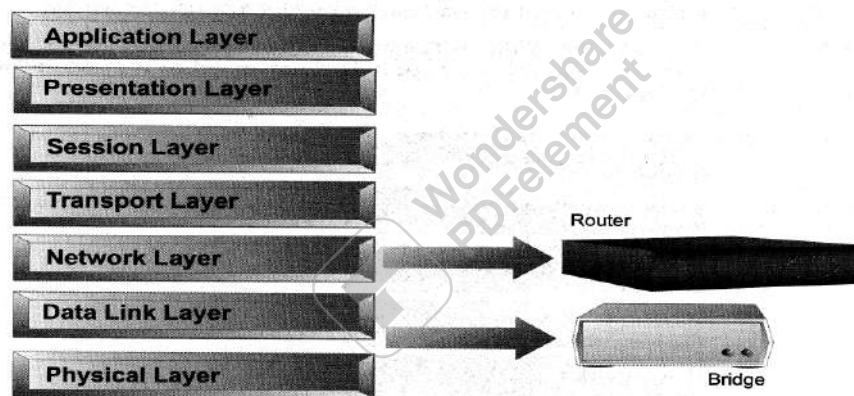
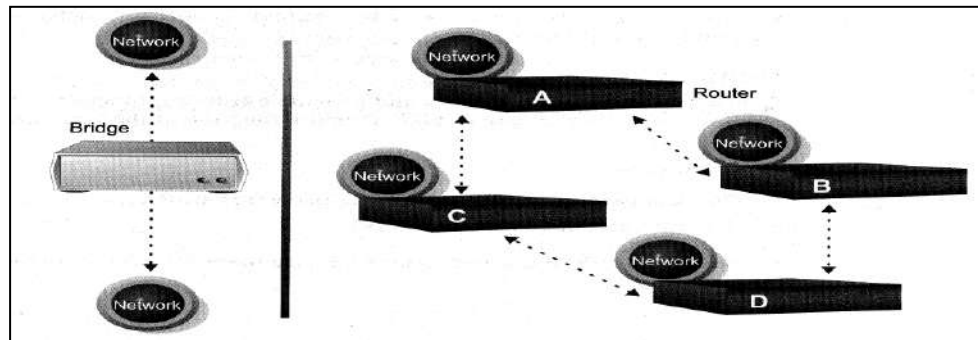
Static and Dynamic Routers

<i>Static Routers</i>	<i>Dynamic Routers</i>
Manual configuration of routes	Manual configuration of the first route. Automatic discovery of new routes
Always use the same route	Can select the best route
More secure	Need manual configuration to improve security

=====Course One=====

Distinguishing Between Bridges and Routers

- Bridges forward everything they don't recognize
- Routers select the best path
- **Routers are layer 3** devices which recognize network address
- **Bridges are layer 2** devices which look at the MAC sublayer node address



Layer-3 Switches

- Layer-3 switches operate in both layer 2 (data link layer) and 3 (network layer)
- Can perform both MAC switching and IP routing
- A combination of switch and router but much faster and easier to configure than router

Why Layer-3 switches?

- Traffic of LAN is no longer local
- Speed of LAN is much faster
- Need a much faster router, however, very expensive

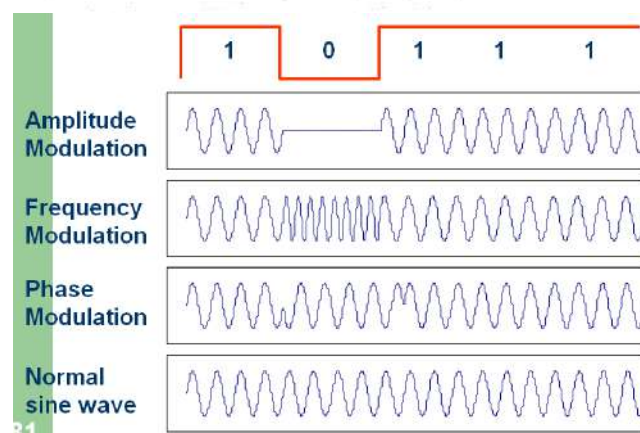
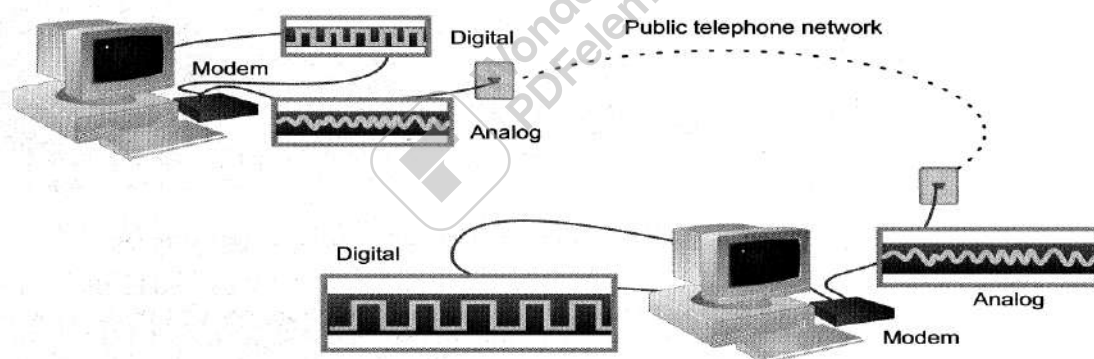
Summary

- **Repeaters** are the least expensive way to expand a network, but they are limited to connecting two segments
- **Bridges** function similar to repeaters, but can understand the node addresses
- **Switches** can be considered as multiport bridges, can divide a network into some logical channels
- **Routers** interconnect networks and provide filtering functions. They can determine the best route

B. Remote Access Devices

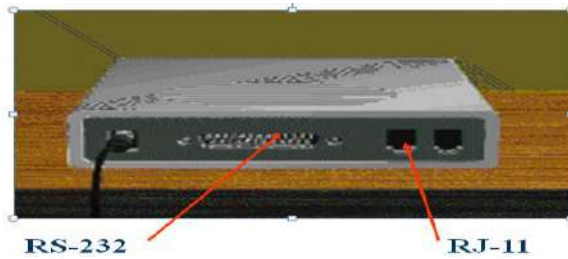
1. Modems

- Allow computers to communicate over a telephone line
- Enable communication between networks or connecting to the world beyond the LAN
- Cannot send digital signal directly to telephone line
- Sending end: MODulate the computer's digital signal into analog signal and transmits
- Receiving end: DEModulate the analog signal back into digital form



- Modems typically have the following I/O interface:
 - A serial RS-232 communication interface
 - An RJ-11 telephone-line interface (a telephone plug)

=====Course One=====



Modem Performance Measures

- Baud rate - the number of symbol change per second on the transmission line
- Bit per second (bps) - number of bits transmitted per second
- In the past, they are identical
- With compression technique, a change of signal can mean more than one bits 28.8kbaud can mean 115.2kbps when using V.42bis

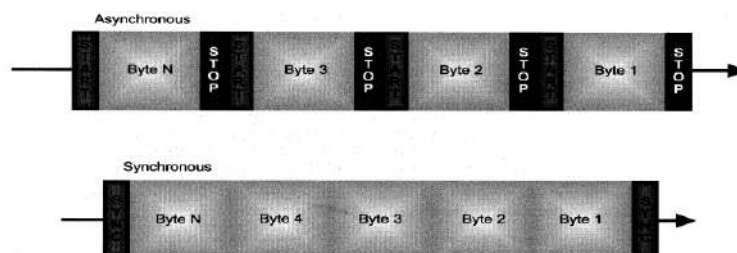
Types of Modem - Asynchronous Modems

- No clocking devices
- Commonly used in telephone networks
- Data is transmitted in a serial stream. Each character is turned into a string of 8 bits
- Each of these characters is separated by one start bit and one or two stop bits



Types of Modem - Synchronous Modems

- Need clocking devices
- Data are transmitted in blocks
- Used in digital networks

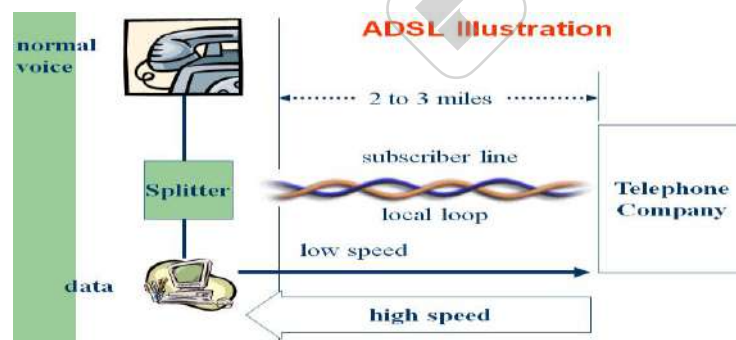


Comparison

- **Asynchronous modems** are relatively simple and economic
 - Large overhead - can be up to 20 to 27% of the data traffic
 - Error control is done by using parity bit or higher layer protocols, e.g. MNP, V.42
- **Synchronous modems** are relatively complicated and expensive
 - Seldom use in home market
 - Less overhead means higher efficiency
 - More sophisticated error control protocol is required

2. ADSL

- ADSL stands for **Asymmetric Digital Subscriber Line**
- Particularly suitable for high speed multimedia communications, general Internet applications
- **Asymmetric** - downstream 1.5 to 6.1Mbps
upstream 16 to 640kbps
- **Digital** - mainly for transmitting digital data
still require modulation and demodulation
- **Subscriber line** - make use of the analog connection between household and CO



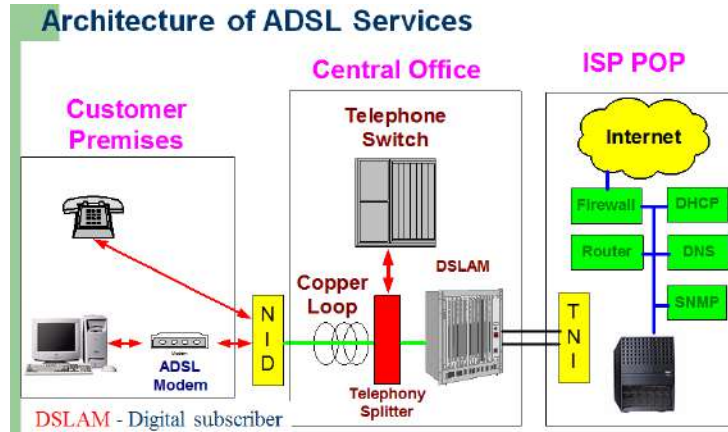
Why Asymmetric?

- In general Internet applications, downstream often requires a higher data rate than upstream
 - Downstream - file download, video playback
 - Upstream - click a link, send a form
- Reducing the resource for upstream can provide more resource for downstream

Why Subscriber Line?

=====Course One=====

- **By better controlling the length and quality of the analog connection between household and CO, a higher data rate can be achieved**



3. Dynamic Addresses for Different Purposes

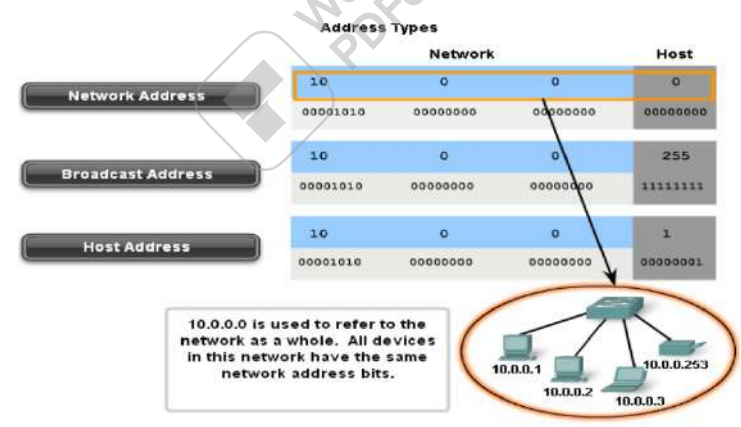
3.1 Types of Address in an IPv4 Network

Within the address range of each IPv4 network, we have three types of addresses:

- Network address** - The address by which we refer to the network
- Broadcast address** - A special address used to send data to all hosts in the network
- Host addresses** - The addresses assigned to the end devices in the network

3.1 .1 Network Address

The network address is a standard way to refer to a network. For example, we could refer to the network shown in the figure as "the **10.0.0** network." This is a much more convenient and descriptive way to refer to the network than using a term like "the first network." All hosts in the **10.0.0** network will have the same network bits. Within the IPv4 address range of a network, the lowest address is reserved for the network address. This address has a 0 for each host bit in the host portion of the address.

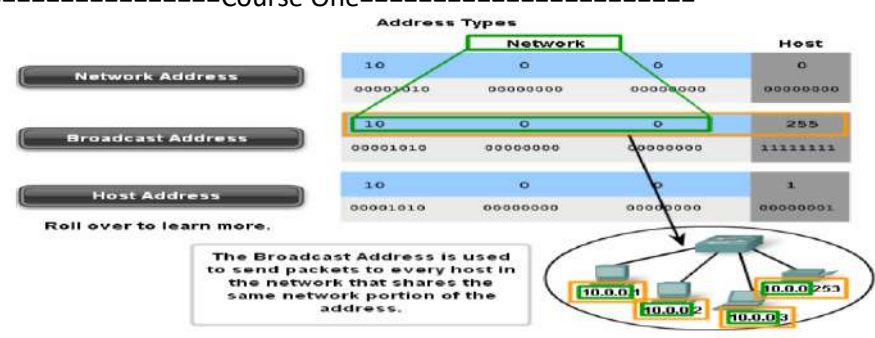


3.1.2 Broadcast Address

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

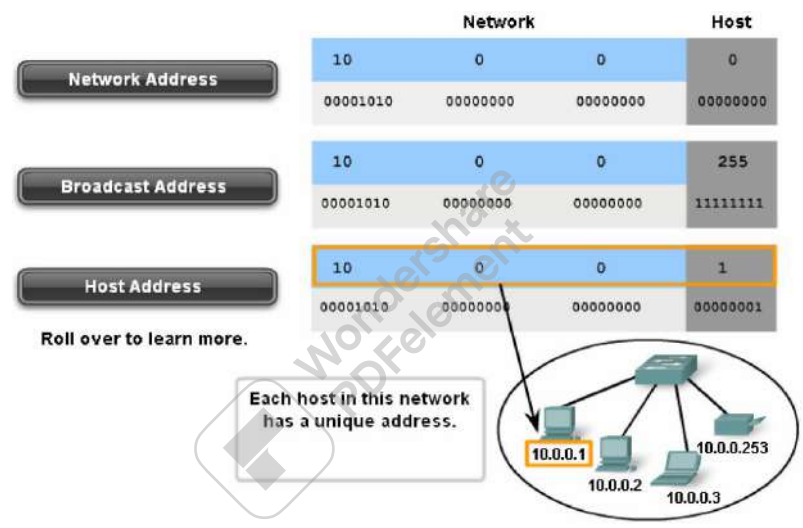
The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s. For the network **10.0.0.0** with 24 network bits, the broadcast address would be **10.0.0.255**. This address is also referred to as the directed broadcast.

=====Course One=====



3.1.3 Host Addresses

Every end device requires a unique address to deliver a packet to that host. In IPv4 addresses, we assign the values between the network address and the broadcast address to the devices in that network.



3.1.4 Network Prefixes

An important question is: How do we know how many bits represent the network portion and how many bits represent the host portion? When we express an IPv4 network address, we add a prefix length to the network address. The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address. This leaves the remaining 8 bits, the last octet, as the host portion.

The subnet mask consists of 32 bits, just as the address does, and uses 1s and 0s to indicate which bits of the address are network bits and which bits are hosts bits.

Networks are not always assigned a /24 prefix. Depending on the number of hosts on the network, the prefix assigned may be different. Having a different prefix number changes the host range and broadcast address for each network. Roll over the addresses in the figure to view the results of using different prefixes on an address.

Notice that the network address could remain the same, but the host range and the broadcast address are different for the different prefix lengths. In this figure you can also see that the number of hosts that can be addressed on the network changes as well.

=====Course One=====

Using Different Prefixes for the 172.16.4.0 Network

Network	Network address	Host range	Broadcast address
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

SAME NETWORK ADDRESS
ALL PREFIXES

DIFFERENT BROADCAST
ADDRESS EACH PREFIX

3.2 Calculating Network, Hosts and Broadcast addresses

At this point, you may be wondering: How do we calculate these addresses? This calculation process requires us to look at these addresses in binary. In the example network divisions, we need to look at the octet of the address where the prefix divides the network portion from the host portion. In all of these examples, it is the last octet. While this is common, the prefix can also divide any of the octets.

To get started understanding this process of determining the address assignments, let's break some examples down into binary.

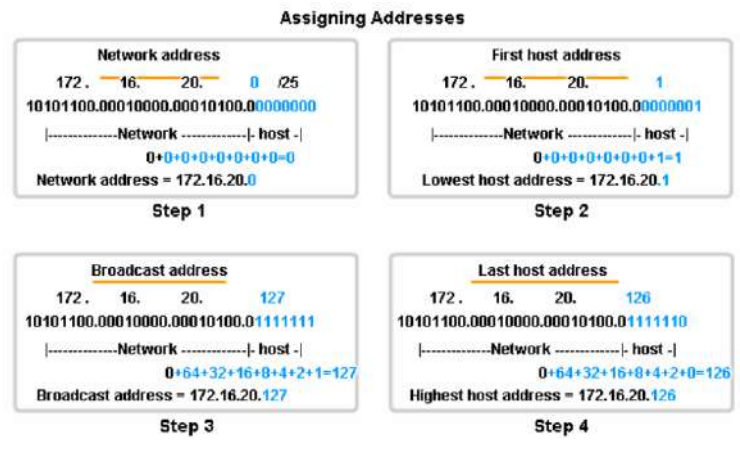
In the first box, we see the representation of the network address. With a 25 bit prefix, the last 7 bits are host bits. To represent the network address, all of these host bits are '0'. This makes the last octet of the address 0. This makes the network address 172.16.20.0 /25.

In the second box, we see the calculation of the lowest host address. This is always one greater than the network address. In this case, the last of the seven host bits becomes a '1'. With the lowest bit of host address set to a 1, the lowest host address is 172.16.20.1. The third box shows the calculation of the broadcast address of the network. Therefore, all seven host bits used in this network are all '1s'. From the calculation, we get 127 in the last octet. This gives us a broadcast address of 172.16.20.127.

The fourth box presents the calculation of the highest host address. The highest host address for a network is always one less than the broadcast. This means the lowest host bit is a '0 and all other host bits as "1s". As seen, this makes the highest host address in this network 172.16.20.126.

Although for this example we expanded all of the octets, we only need to examine the content of the divided octet.

=====**Course One**=====



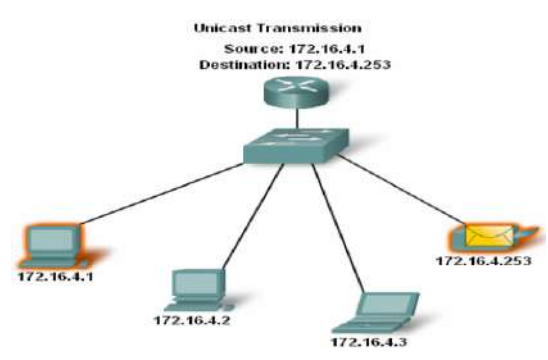
3.3 Unicast, Broadcast, Multicast-Types of communication

In an IPv4 network, the hosts can communicate one of three different ways:

- Unicast** - the process of sending a packet from one host to an individual host
 - Broadcast** - the process of sending a packet from one host to all hosts in the network
 - Multicast** - the process of sending a packet from one host to a selected group of hosts
- These three types of communication are used for different purposes in the data networks. In all three cases, the IPv4 address of the originating host is placed in the packet header as the source address.

3.3.1 Unicast Traffic

Unicast communication is used for the normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the host address of the destination device as the destination address and can be routed through an internetwork. Broadcast and multicast, however, use special addresses as the destination address. Using these special addresses, broadcasts are generally restricted to the local network. The scope of multicast traffic also may be limited to the local network or routed through an internetwork.



In an IPv4 network, the unicast address applied to an end device is referred to as the host address. For unicast communication, the host addresses assigned to the two end devices are used as the source and destination IPv4 addresses. During the encapsulation process, the source host places its IPv4 address in the unicast packet header as the source host address and the IPv4 address of the destination host in the

=====Course One=====

packet header as the destination address. The communication using a unicast packet can be forwarded through an internetwork using the same addresses.

3.3.2 Broadcast Transmission

Because broadcast traffic is used to send packets to all hosts in the network, a packet uses a special broadcast address. When a host receives a packet with the broadcast address as the destination, it processes the packet as it would a packet to its unicast address.

Broadcast transmission is used for the location of special services/devices for which the address is not known or when a host needs to provide information to all the hosts on the network.

Some examples for using broadcast transmission are:

- Mapping upper layer addresses to lower layer addresses
- Requesting an address
- Exchanging routing information by routing protocols

When a host needs information, the host sends a request, called a query, to the broadcast address. All hosts in the network receive and process this query. One or more of the hosts with the requested information will respond, typically using unicast.

Similarly, when a host needs to send information to the hosts on a network, it creates and sends a broadcast packet with the information.

Unlike unicast, where the packets can be routed throughout the internetwork, broadcast packets are usually restricted to the local network. This restriction is dependent on the configuration of the router that borders the network and the type of broadcast. There are two types of broadcasts: **directed broadcast** and **limited broadcast**.

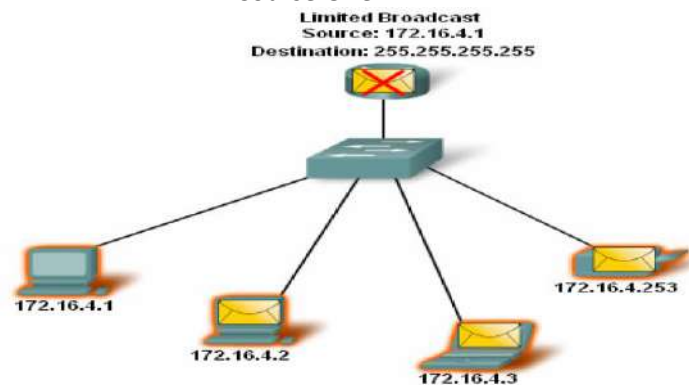
3.3.2.1 Directed Broadcast

A directed broadcast is sent to all hosts on a specific network. This type of broadcast is useful for sending a broadcast to all hosts on a non-local network

3.3.2.2 Limited Broadcast

The limited broadcast is used for communication that is limited to the hosts on the local network. These packets use a destination IPv4 address **255.255.255.255**.

=====Course One=====



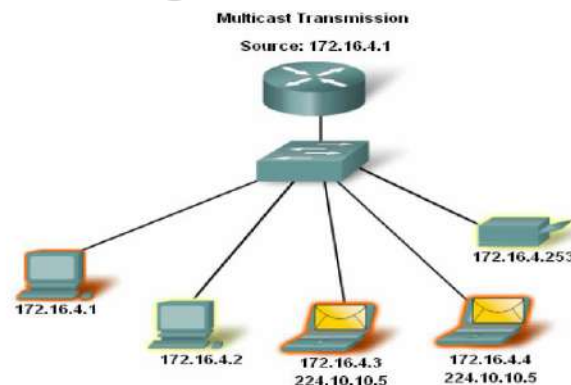
As you learned earlier, when a packet is broadcast, it uses resources on the network and also forces every host on the network that receives it to process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect performance of the network or devices. Because routers separate broadcast domains, subdividing networks with excessive broadcast traffic can improve network performance.

3.3.4 Multicast Transmission

Multicast transmission is designed to conserve the bandwidth of the IPv4 network. It reduces traffic by allowing a host to send a single packet to a selected set of hosts.

3.3.5 Multicast Clients

Hosts that wish to receive particular multicast data are called multicast clients. The multicast clients use services initiated by a client program to subscribe to the multicast group.



3.4 Reserved IPv4 Address Range

Expressed in dotted decimal format, the IPv4 address range is **0.0.0.0** to **255.255.255.255**. As you have already seen, not all of these addresses can be used as host addresses for unicast communication.

3.4.1 Experimental Addresses

One major block of addresses reserved for special purposes is the IPv4 experimental address range **240.0.0.0** to **255.255.255.254**. Currently, these addresses are listed as reserved for future use (RFC 3330). This suggests that they could be converted to usable addresses. Currently, they cannot be used in IPv4 networks. However, these addresses could be used for research or experimentation.

3.4.2 Multicast Addresses

As previously shown, another major block of addresses reserved for special purposes is the IPv4 multicast addresses range **224.0.0.0** to **239.255.255.255**. Additionally, the multicast address range is subdivided into different types of addresses: reserved link local addresses and globally scoped addresses, as shown in the graphic. One additional type of multicast address is the administratively scoped addresses, also called limited scope addresses.

devices.

3.4.3 Host Addresses

After accounting for the ranges reserved for experimental addresses and multicast addresses, this leaves an address range of **0.0.0.0** to **223.255.255.255** that could be used for IPv4 hosts. However, within this range are many addresses that are already reserved for special purposes. Although we have previously covered some of these addresses, the major reserved addresses are discussed in the next section.

Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	<ul style="list-style-type: none"> • used for research or experimentation • cannot currently be used for hosts in IPv4 networks 	240.0.0.0 to 255.255.255.254	1700 3330

3.5 Public And private Addresses

Although most IPv4 host addresses are public addresses designated for use in networks that are accessible on the Internet, there are blocks of addresses that are used in networks that require limited or no Internet access. These addresses are called private addresses.

=====Course One=====

3.5.1 Private Addresses

The private address blocks are:

10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
 172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

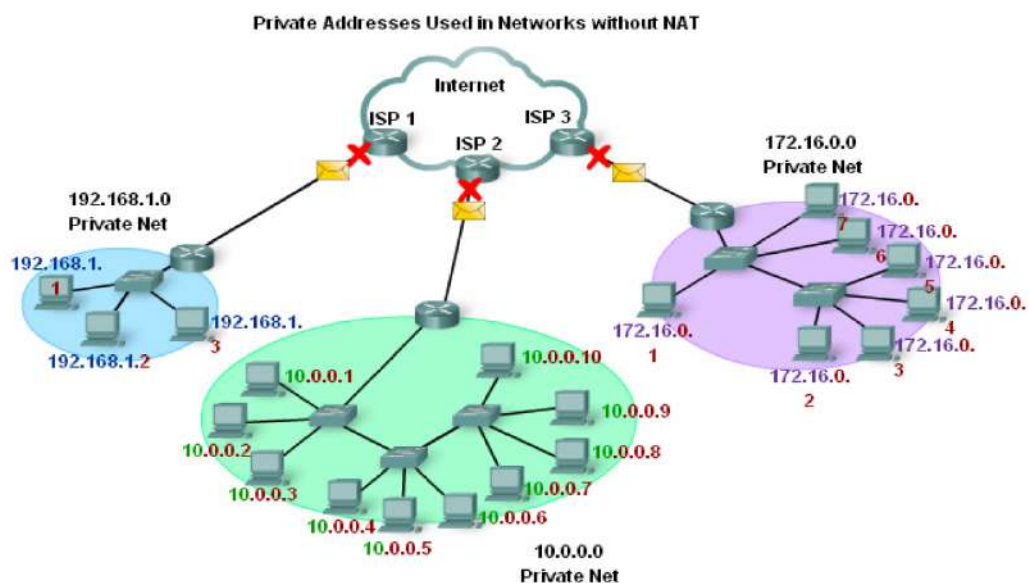
Private space address blocks, as shown in the figure, are set aside for use in private networks. The use of these addresses need not be unique among outside networks. Hosts that do not require access to the Internet at large may make unrestricted use of private addresses. However, the internal networks still must design network address schemes to ensure that the hosts in the private networks use IP addresses that are unique within their networking environment.

3.5.2 Network Address Translation (NAT)

NAT allows the hosts in the network to "borrow" a public address for communicating to outside networks. While there are some limitations and performance issues with NAT, clients for most applications can access services over the Internet without noticeable problems.

3.5.1 Public Addresses

The vast majority of the addresses in the IPv4 unicast host range are public addresses. These addresses are designed to be used in the hosts that are publicly accessible from the Internet. Even within these address blocks, there are many addresses that are designated for other special purposes.



IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2 ⁷) 16,777,214 hosts per net (2 ²⁴⁻²)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2 ¹⁴) 65,534 hosts per net (2 ¹⁶⁻²)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2 ²¹) 254 hosts per net (2 ⁸⁻²)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

3.8 Planning to Address the Network

The allocation of Network layer address space within the corporate network needs to be well designed. Network administrators should not randomly select the addresses used in their networks. Nor should address assignment within the network be random.

The allocation of these addresses inside the networks should be planned and documented for the purpose of:

- Preventing duplication of addresses
- Providing and controlling access
- Monitoring security and performance

3.8 .1 Preventing Duplication of Addresses

As you already know, each host in an internetwork must have a unique address. Without the proper planning and documentation of these network allocations, we could easily assign an address to more than one host.

3.8 .2 Providing and Controlling Access

Some hosts provide resources to the internal network as well as to the external network. One example of these devices is servers. Access to these resources can be controlled by the Layer 3 address. If the addresses for these resources are not planned and documented, the security and accessibility of the devices are not easily controlled. For example, if a server has a random address assigned, blocking access to its address is difficult and clients may not be able to locate this resource.

3.8 .3 Monitoring Security and Performance

Similarly, we need to monitor the security and performance of the network hosts and the network as a whole. As part of the monitoring process, we examine network traffic looking for addresses that are generating or receiving excessive packets. If we have proper planning and documentation of the network addressing, we can identify the device on the network that has a problematic address.

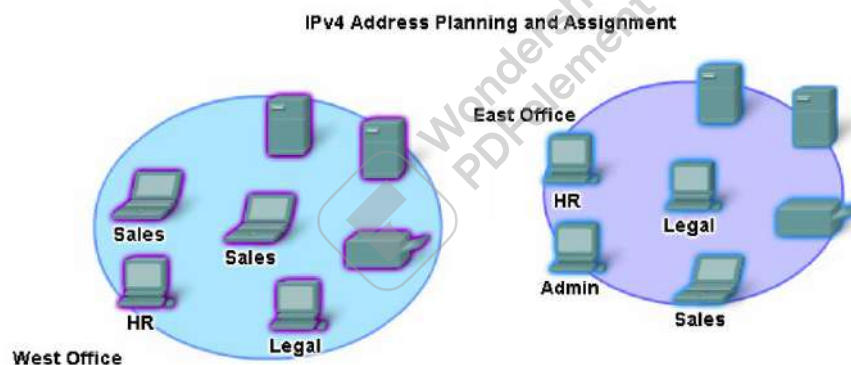
3.8 .4 Assigning Addresses within a Network

As you have already learned, hosts are associated with an IPv4 network by a common network portion of the address. Within a network, there are different types of hosts.

Some examples of different types of hosts are:

- End devices for users
- Servers and peripherals
- Hosts that are accessible from the Internet
- Intermediary devices

Each of these different device types should be allocated to a logical block of addresses within the address range of the network.



3.9 Planning to Address the Network

An important part of planning an IPv4 addressing scheme is deciding when private addresses are to be used and where they are to be applied.

Considerations include:

- Will there be more devices connected to the network than public addresses allocated by the network's ISP?
- Will the devices need to be accessed from outside the local network?
- If devices that may be assigned private addresses require access to the Internet, is the network capable of providing a Network Address Translation (NAT) service?

3.10 Static and Dynamic Addressing for End User Devices

=====Course One=====

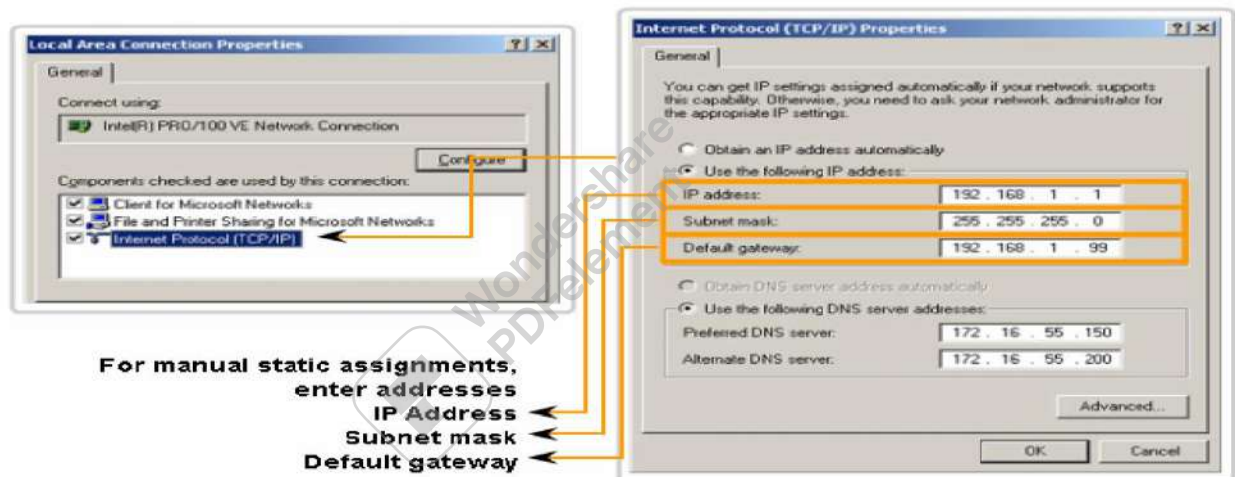
3. 10.2 Static Assignment of Addresses

With a static assignment, the network administrator must manually configure the network information for a host, as shown in the figure. At a minimum, this includes entering the host IP address, subnet mask, and default gateway.

Static addresses have some advantages over dynamic addresses. For instance, they are useful for printers, servers, and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would cause problems if that address changed. Additionally, static assignment of addressing information can provide increased control of network resources. However, it can be time-consuming to enter the information on each host.

When using static IP addressing, it is necessary to maintain an accurate list of the IP address assigned to each device. These are permanent addresses and are not normally reused.

Addressing End Devices



3. 10.3 Dynamic Assignment of Addresses

Because of the challenges associated with static address management, end user devices often have addresses dynamically assigned, using Dynamic Host Configuration Protocol (DHCP), as shown in the figure.

DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. The configuration of the DHCP server requires that a block of addresses, called an address pool, be defined to be assigned to the DHCP clients on a network. Addresses assigned to this pool should be planned so that they exclude any addresses used for the other types of devices.

DHCP is generally the preferred method of assigning IP addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

Another benefit of DHCP is that an address is not permanently assigned to a host but is only "leased" for a period of time. If the host is powered down or taken off the network,

=====Course One=====

the address is returned to the pool for reuse. This feature is especially helpful for mobile users that come and go on a network.

Assigning Dynamic Addresses



This property will set the device to obtain an IP address automatically.

3.12 Who Assigns the Different Addresses?

A company or organization that wishes to have network hosts accessible from the Internet must have a block of public addresses assigned. The use of these public addresses is regulated and the company or organization must have a block of addresses allocated to it. This is true for IPv4, IPv6, and multicast addresses.

3.12.1 Internet Assigned Numbers Authority (IANA)

IANA is the master holder of the IP addresses. The IP multicast addresses and the IPv6 addresses are obtained directly from IANA. Until the mid-1990s, all IPv4 address space was managed directly by the IANA. At that time, the remaining IPv4 address space was allocated to various other registries to manage for particular purposes or for regional areas.

3.12. Overview of IPv6

In the early 1990s, the Internet Engineering Task Force (IETF) grew concerned about the exhaustion of the IPv4 network addresses and began to look for a replacement for this protocol.

This activity led to the development of what is now known as IPv6. Creating expanded addressing capabilities was the initial motivation for developing this new protocol. Other issues were also considered during the development of IPv6, such as:

University of Technology
Department of Computer Science
Date: 2018-2019

Lecturer: Dr. Raheem Abdul Sahib Oglu
Material: computer networks
Branches : Security, Programming ,.....

=====Course One=====

Improved packet handling ,Increased scalability and longevity , QoS mechanisms,
Integrated security

To provide these features, IPv6 offers:

- 128-bit hierarchical addressing - to expand addressing capabilities
- Header format simplification - to improve packet handling
- Improved support for extensions and options - for increased scalability/longevity and improved packet handling
- Flow labeling capability - as QoS mechanisms
- Authentication and privacy capabilities - to integrate security

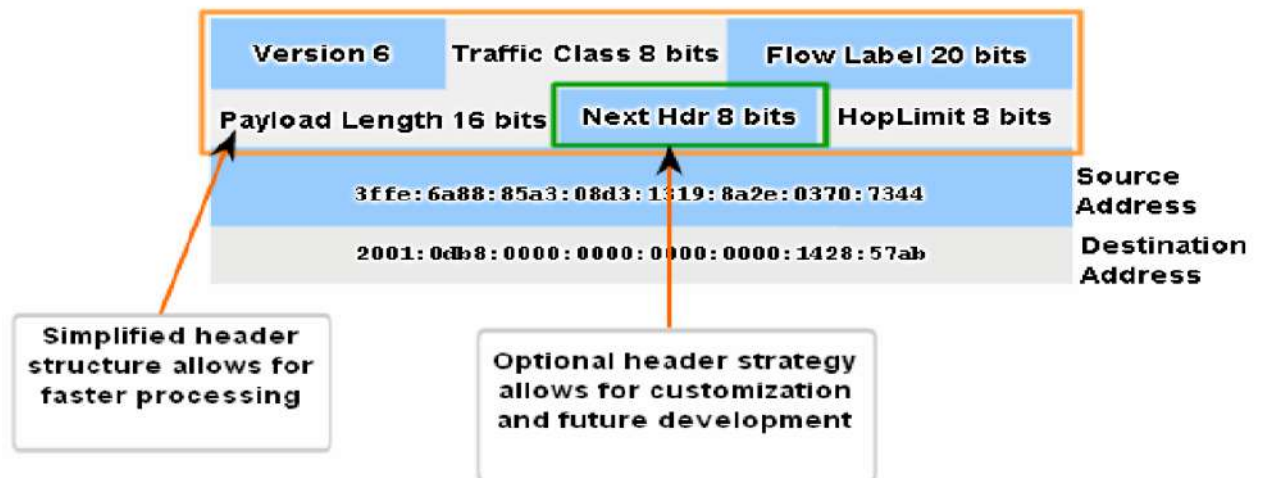
IPv6 is not merely a new Layer 3 protocol - it is a new protocol suite. New protocols at various layers of the stack have been developed to support this new protocol. There is a new messaging protocol (ICMPv6) and new routing protocols. Because of the increased size of the IPv6 header, it also impacts the underlying network infrastructure.

3.12.2 Transition to IPv6

As you can see from this brief introduction, IPv6 has been designed with scalability to allow for years of internetwork growth. However, IPv6 is being implemented slowly and in select networks. Because of better tools, technologies, and address management in the last few years, IPv4 is still very widely used, and likely to remain so for some time into the future. However, IPv6 may eventually replace IPv4 as the dominant Internet protocol.

=====Course One=====

IPv6 Header



IPv6 Header

3.13. Is It on My Network?

3.13.1 The Subnet Mask-Defining the Network and Host Portions

As we learned earlier, an IPv4 address has a network portion and a host portion. We referred to the prefix length as the number of bits in the address giving us the network portion. *The prefix is a way to define the network portion that is human readable.* The data network must also have this network portion of the addresses defined.

To define the network and host portions of an address, the devices use a separate 32-bit pattern called a subnet mask, as shown in the figure. We express the subnet mask in the same dotted decimal format as the IPv4 address. *The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.*

The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

As shown in the figure, a /24 prefix is expressed as a subnet mask as 255.255.255.0 (11111111.11111111.11111111.00000000). The remaining bits (low order) of the subnet mask are zeroes, indicating the host address within the network. The subnet mask is configured on a host in conjunction with the IPv4 address to define the network portion of that address.

For example, let's look at the host 172.16.4.35/27:

Address

172.16.20.35
 10101100.00010000.00010100.00100011

=====Course One=====

Subnet mask

255.255.255.224

11111111.11111111.11111111.11100000

Network address

172.16.20.32

10101100.00010000.00010100.00100000

Because the high order bits of the subnet masks are contiguous 1s, there are only a limited number of subnet values within an octet. You will recall that we only need to expand an octet if the network and host division falls within that octet. Therefore, there are a limited number 8 bit patterns used in address masks.

These patterns are:

00000000 = 0

10000000 = 128

11000000 = 192

11100000 = 224

11110000 = 240

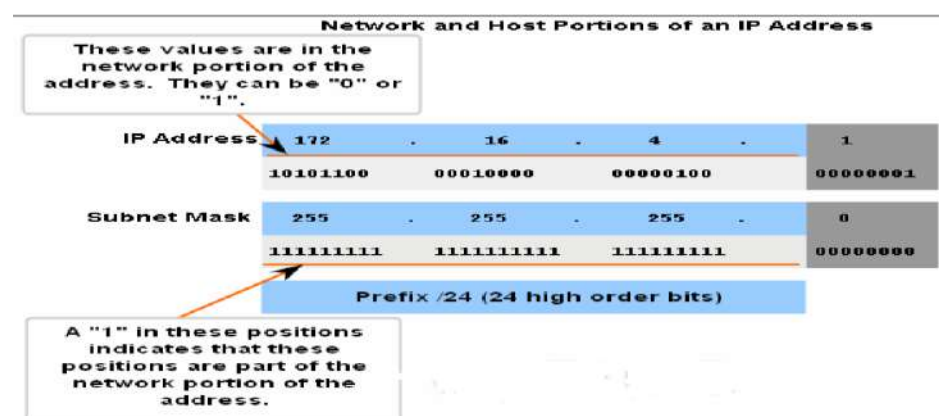
11111000 = 248

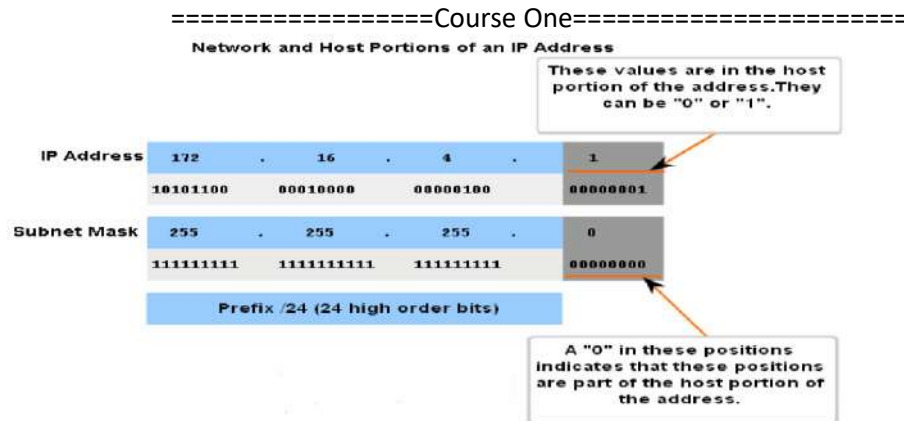
11111100 = 252

11111110 = 254

11111111 = 255

If the subnet mask for an octet is represented by 255, then all the equivalent bits in that octet of the address are network bits. Similarly, if the subnet mask for an octet is represented by 0, then all the equivalent bits in that octet of the address are host bits. In each of these cases, it is not necessary to expand this octet to binary to determine the network and host portions.





3.13.2 ANDing-What Is In Our Network

Inside data network devices, digital logic is applied for their interpretation of the addresses. When an IPv4 packet is created or forwarded, the destination network address must be extracted from the destination address. This is done by a logic called AND.

The IPv4 host address is logically ANDed with its subnet mask to determine the network address to which the host is associated. When this ANDing between the address and the subnet mask is performed, the result yields the network address.

3.13.3 The AND Operation

ANDing is one of three basic binary operations used in digital logic. The other two are OR and NOT. While all three are used in data networks, AND is used in determining the network address. Therefore, our discussion here will be limited to logical AND. Logical AND is the comparison of two bits that yields the following results:

$1 \text{ AND } 1 = 1$, $1 \text{ AND } 0 = 0$, $0 \text{ AND } 1 = 0$, $0 \text{ AND } 0 = 0$

3.13.4 Reasons to Use AND

This ANDing between the host address and subnet mask is performed by devices in a data network for various reasons.

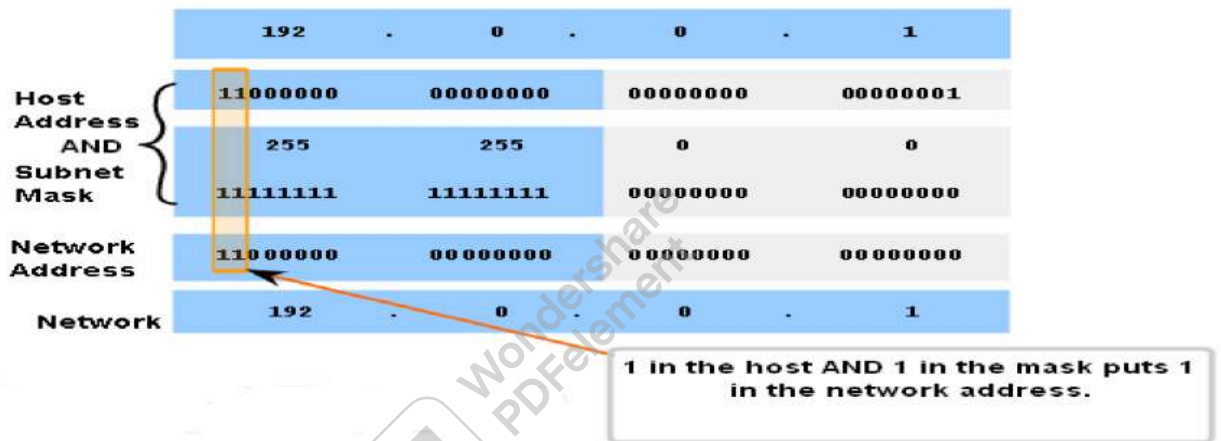
Routers use ANDing to determine an acceptable route for an incoming packet. The router checks the destination address and attempts to associate this address with a next hop. As a packet arrives at a router, the router performs ANDing on the IP destination address in the incoming packet and with the subnet mask of potential routes. This yields a network address that is compared to the route from the routing table whose subnet mask was used.

=====Course One=====

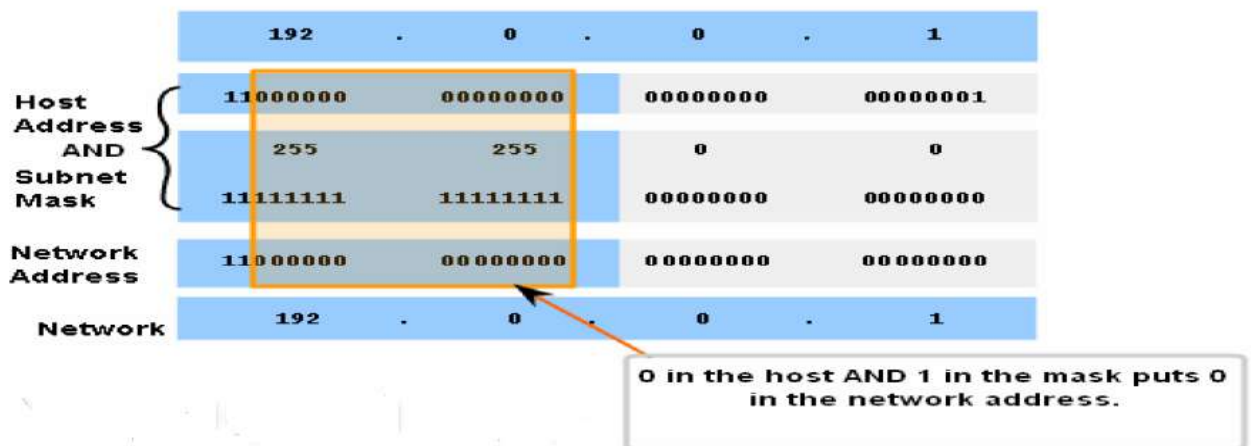
An originating host must determine if a packet should be sent directly to a host in the local network or be directed to the gateway. To make this determination, a host must first know its own network address.

A host extracts its network address by ANDing its address with its subnet mask. A logical AND is also performed by an originating host between the destination address of the packet and the subnet mask of this host. This yields the network address of the destination. If this network address matches the network address of the local host, the packet is sent directly to the destination host. If the two network addresses do not match, the packet is sent to the gateway.

Applying the Subnet Mask
 A device with address 192.0.0.1 belongs to network 192.0.0.0



Applying the Subnet Mask
 A device with address 192.0.0.1 belongs to network 192.0.0.0



Applying the Subnet Mask
 A device with address 192.0.0.1 belongs to network 192.0.0.0

14. Basic Subnetting

Subnetting allows for creating multiple logical networks from a single address block. Since we use a router to connect these networks together, each interface on a router must have a unique network ID. Every node on that link is on the same network. We create the subnets by using one or more of the host bits as network bits. This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits used, the more subnets that can be defined. For each bit borrowed, we double the number of subnetworks available. For example, if we borrow 1 bit, we can define 2 subnets. If we borrow 2 bits, we can have 4 subnets. However, with each bit we borrow, fewer host addresses are available per subnet.

RouterA in the figure has two interfaces to interconnect two networks. Given an address block of 192.168.1.0 /24, we will create two subnets. We borrow one bit from the host portion by using a subnet mask of 255.255.255.128, instead of the original 255.255.255.0 mask. The most significant bit in the last octet is used to distinguish between the two subnets. For one of the subnets, this bit is a "0" and for the other subnet this bit is a "1".

14.1 Formula for calculating subnets

Use this formula to calculate the number of subnets:

2^n where n = the number of bits borrowed

In this example, the calculation looks like this:

$2^1 = 2$ subnets

14.2 The number of hosts

To calculate the number of hosts per network, we use the formula of $2^n - 2$ where n = the number of bits left for hosts.

Applying this formula, ($2^7 - 2 = 126$) shows that each of these subnets can have 126 hosts.

For each subnet, examine the last octet in binary. The values in these octets for the two networks are:

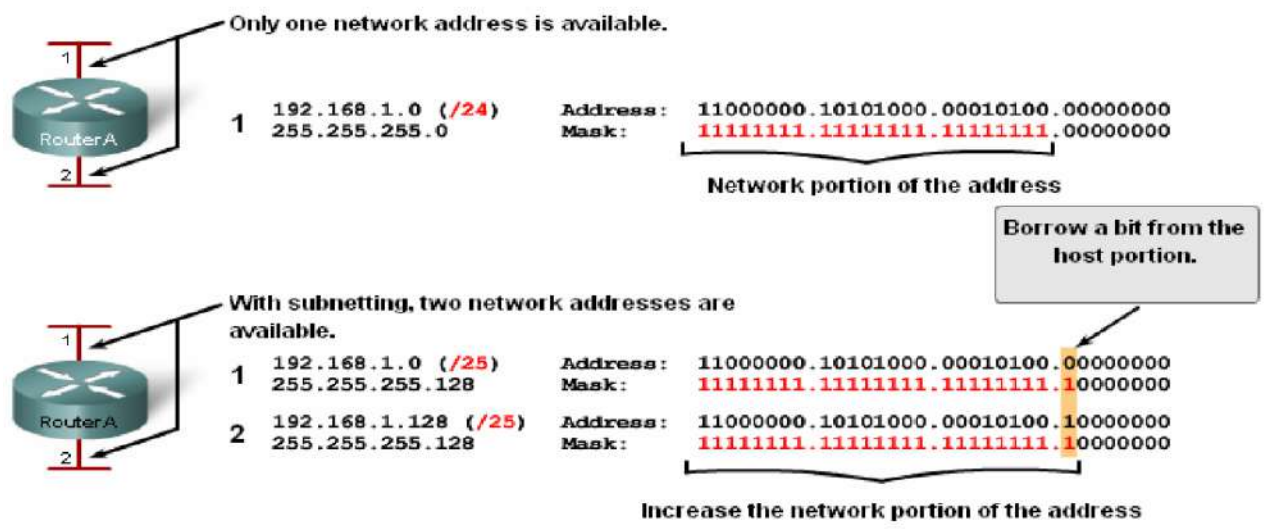
Subnet 1: 00000000 = 0

Subnet 2: 10000000 = 128

See the figure for the addressing scheme for these networks.

=====Course One=====

Borrowing Bits for Subnets



Borrowing Bits for Subnets

Addressing Scheme: Example of 2 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Example with 3 subnets

Next, consider an internetwork that requires three subnets. See the figure. Again we start with the same 192.168.1.0 /24 address block. Borrowing a single bit would only provide two subnets. To provide more networks, we change the subnet mask to 255.255.255.192 and borrow two bits. This will provide four subnets.

Calculate the subnet with this formula:

$2^2 = 4$ subnets

The number of hosts

To calculate the number of hosts, begin by examining the last octet. Notice these subnets.

Subnet 0: 0 = 00000000

Subnet 1: 64 = 01000000

Subnet 2: 128 = 10000000

Subnet 3: 192 = 11000000

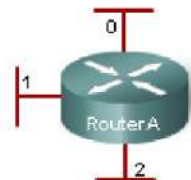
Apply the host calculation formula.

=====Course One=====

$2^6 - 2 = 62$ hosts per subnet

See the figure for the addressing scheme for these networks.

Borrowing Bits for Subnets



	Address	Mask
-	192.168.1.0 (/24) 255.255.255.0	11000000.10101000.00010100.00000000 11111111.11111111.11111111.00000000
0	192.168.1.0 (/26) 255.255.255.192	11000000.10101000.00010100.00000000 11111111.11111111.11111111.11000000
1	192.168.1.64 (/26) 255.255.255.192	11000000.10101000.00010100.01000000 11111111.11111111.11111111.11000000
2	192.168.1.128 (/26) 255.255.255.192	11000000.10101000.00010100.10000000 11111111.11111111.11111111.11000000
3	192.168.1.192 (/26) 255.255.255.192	11000000.10101000.00010100.11000000 11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

More subnets are available, but fewer addresses are available per subnet.

Borrowing Bits for Subnets

Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Example with 6 subnets

Consider this example with five LANs and a WAN for a total of 6 networks. See the figure. To accommodate 6 networks, subnet 192.168.1.0 /24 into address blocks using the formula:

$2^3 = 8$

To get at least 6 subnets, borrow three host bits. A subnet mask of 255.255.255.224 provides the three additional network bits.

The number of hosts

To calculate the number of hosts, begin by examining the last octet. Notice these subnets.

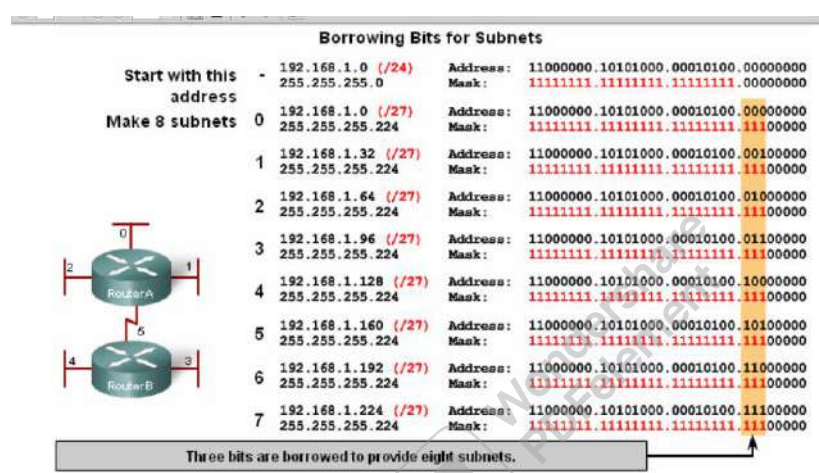
=====Course One=====

- 0 = 00000000
- 32 = 00100000
- 64 = 01000000
- 96 = 01100000
- 128 = 10000000
- 160 = 10100000
- 192 = 11000000
- 224 = 11100000

Apply the host calculation formula:

$2^5 - 2 = 30$ hosts per subnet.

See the figure for the addressing scheme for these networks.



Borrowing Bits for Subnets
Addressing Scheme: Example of 6 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

15. Subnetting-Dividing Networks into Right Sizes

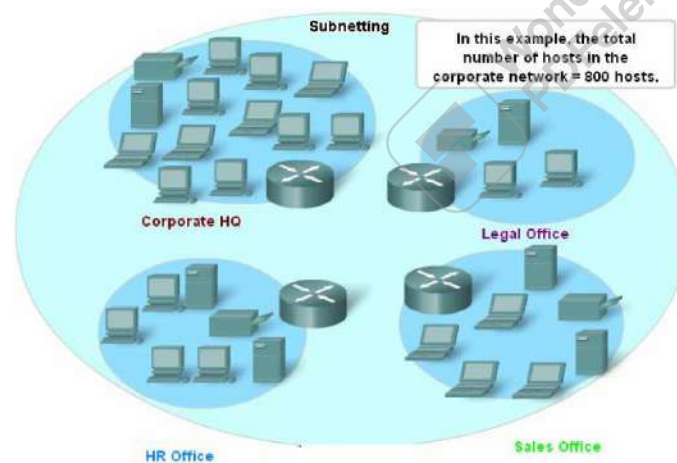
Every network within the internetwork of a corporation or organization is designed to accommodate a finite number of hosts.

Some networks, such as point-to-point WAN links, only require a maximum of two hosts. Other networks, such as a user LAN in a large building or department, may need to accommodate hundreds of hosts. Network administrators need to devise the internetwork addressing scheme to accommodate the maximum number of hosts for each network. The number of hosts in each division should allow for growth in the number of hosts.

15.1 Determine the Total Number of Hosts

First, consider the total number of hosts required by the entire corporate internetwork. We must use a block of addresses that is large enough to accommodate all devices in all the corporate networks. This includes end user devices, servers, intermediate devices, and router interfaces.

See Step 1 of the figure.



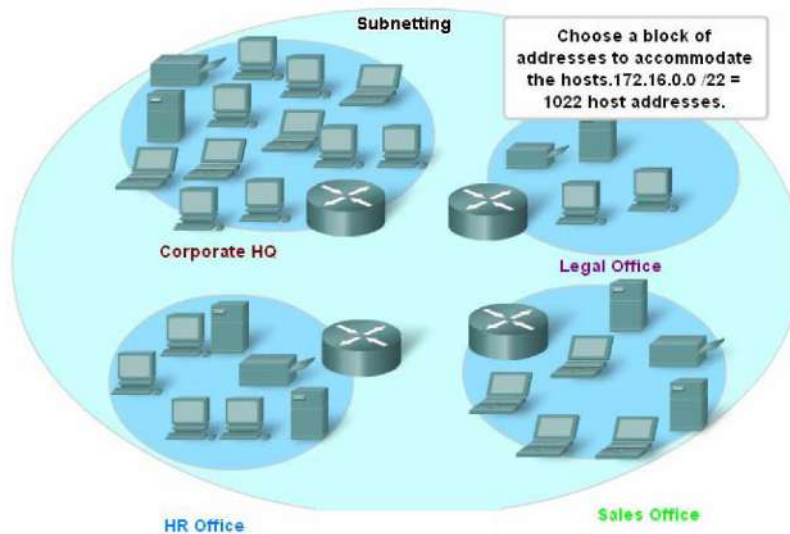
Consider the example of a corporate internetwork that needs to accommodate 800 hosts in its four locations.

15.2 Determine the Number and Size of the Networks

Next, consider the number of networks and the size of each required based on common groupings of hosts.

See Step 2 of the figure.

=====Course One=====



We subnet our network to overcome issues with location, size, and control. In designing the addressing, we consider the factors for grouping the hosts that we discussed previously:

- Grouping based on common geographic location
- Grouping hosts used for specific purposes
- Grouping based on ownership

Each WAN link is a network. We create subnets for the WAN that interconnect different geographic locations. When connecting the different locations, we use a router to account for the hardware differences between the LANs and the WAN.

Although hosts in a common geographic location typically comprise a single block of addresses, we may need to subnet this block to form additional networks at each location. We need to create subnetworks at the different locations that have hosts for common user needs. We may also have other groups of users that require many network resources, or we may have many users that require their own subnetwork. Additionally, we may have subnetworks for special hosts such as servers. Each of these factors needs to be considered in the network count.

We also have to consider any special security or administrative ownership needs that require additional networks.

One useful tool in this address planning process is a network diagram. A diagram allows us to see the networks and make a more accurate count.

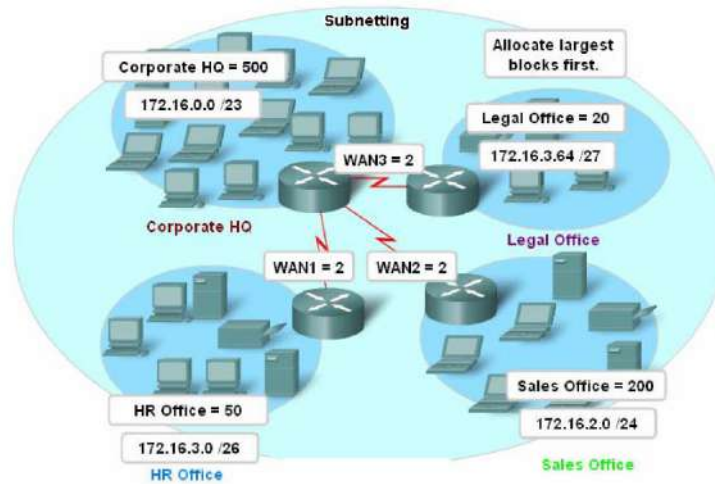
To accommodate 800 hosts in the company's four locations, we use binary arithmetic to allocate a /22 block ($2^{10}-2=1022$).

15.3 Allocating Addresses

Now that we have a count of the networks and the number of hosts for each network, we need to start allocating addresses from our overall block of addresses.

=====Course One=====

See Step 3 of the figure.



This process begins by allocating network addresses for locations of special networks. We start with the locations that require the most hosts and work down to the point-to-point links. This process ensures that large enough blocks of addresses are made available to accommodate the hosts and networks for these locations.

When making the divisions and assignment of available subnets, make sure that there are adequately-sized address blocks available for the larger demands. Also, plan carefully to ensure that the address blocks assigned to the subnet do not overlap.

15.3 The total Number of Usable Hosts

Recall from the previous section that as we divide the address range into subnets, we lose two host addresses for each new network. These are the network address and broadcast address.

The formula for calculating the number of hosts in a network is:

$$\text{Usable hosts} = 2^n - 2$$

Where n is the number of bits remaining to be used for hosts.

16. Subnetting –Subnetting a subnet

Subnetting a subnet, or using Variable Length Subnet Mask (VLSM) was designed to maximize addressing efficiency. When identifying the total number of hosts using traditional subnetting, we allocate the same number of addresses for each subnet. If all the subnets have the same requirements for the number hosts, these fixed size address blocks would be efficient. However, most often that is not the case.

For example, the topology in Figure 1 shows a subnet requirement of seven subnets, one for each of the four LANs and one for each of the three WANs. With the given address of 192.168.20.0, we need to borrow 3 bits from the host bits in the last octet to meet our subnet requirement of seven subnets.

University of Technology
 Department of Computer Science
 Date: 2018-2019

Lecturer: Dr. Raheem Abdul Sahib Oglia
 Material: computer networks
 Branches : Security, Programming ,.....

=====Course One=====

These bits are borrowed bits by changing the corresponding subnet mask bits to "1s" to indicate that these bits are now being used as network bits. The last octet of the mask is then represented in binary by 11100000, which is 224. The new mask of 255.255.255.224 is represented with the /27 notation to represent a total of 27 bits for the mask.

In binary this subnet mask is represented as: 11111111.11111111.11111111.11100000

After borrowing three of the host bits to use as network bits, this leaves five host bits. These five bits will allow up to 30 hosts per subnet.

Although we have accomplished the task of dividing the network into an adequate number of networks, it was done with a significant waste of unused addresses. For example, only two addresses are needed in each subnet for the WAN links. There are 28 unused addresses in each of the three WAN subnets that have been locked into address these address blocks. Further, this limits future growth by reducing the total number of subnets available. This inefficient use of addresses is characteristic of classful addressing.

Applying a standard subnetting scheme to scenario is not very efficient and is wasteful. In fact, this example is a good model for showing how subnetting a subnet can be used to maximize address utilization.

Getting More Subnet for Less Hosts

Recall in previous examples we began with the original subnets and gained additional, smaller, subnets to use for the WAN links. Creating smaller each subnet is able to support 2 hosts leaves the original subnets free to be allotted to other devices and prevents many addresses from being wasted.

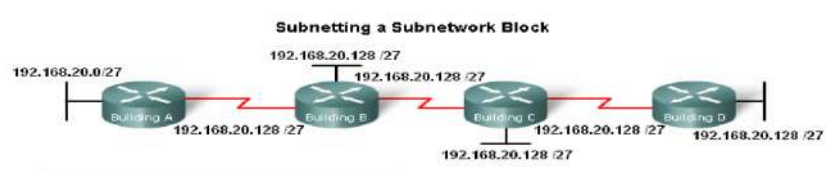
To create these smaller subnets for the WAN links, begin with 192.168.20.192. We can divide this subnet is to many smaller subnets. To provide address blocks for the WANS with two addresses each, we will borrow three additional host bits to be used as network bits.

Address: 192.168.20.192 In Binary: 11000000.10101000.00010100.11000000

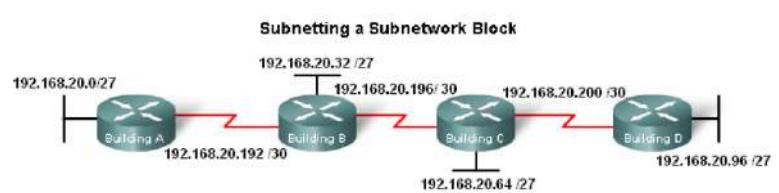
Mask: 255.255.255.252 30 Bits in binary: 11111111.11111111.11111111.11111100

The topology in the figure 2 shows an addressing plan that breaks up the 192.168.20.192 /27 subnets into smaller subnets to provide addresses for the WANs. Doing this reduces the number addresses per subnet to a size appropriate for the WANs. With this addressing, we have subnets 4, 5, and 7 available for future networks, as well as several other subnets available for WANs.

=====Course One=====



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.220/30

based on the number of hosts, including router interfaces and WAN connections. This scenario has the following requirements:

- AtlantaHQ 58 host addresses
- PerthHQ 26 host addresses
- SydneyHQ 10 host addresses
- CorpusHQ 10 host addresses
- WAN links 2 host addresses (each)

It is clear from these requirements that using a standard subnetting scheme would, indeed, be wasteful. In this internetwork, standard subnetting would lock each subnet into blocks of 60 hosts, which would mean a significant waste of potential addresses. This waste is especially evident in figure 2 where we see that the PerthHQ LAN supports 26 users and the SydneyHQ and CorpusHQ LANs routers support only 10 users each.

Therefore, with the given address block of 192.168.15.0 /24, we will begin designing an addressing scheme to meet the requirements and save potential addresses.