3rd Class

2017-2018

Computer Networks

شبكات الحاسوب

أستاذ المادة : د. رحيم عبد الصاحب

المحاضر
د. رحيم عبد الصاحب الربيعي
المادة : شبكات الحاسوب ومقدمة للاتصالات
الملزمة الأولى
2017-2018

1. Data Communications and Networking

Data Communications and Networking

NETWORKING FUNDAMENTALS

Unit Structure

1.0 OBJECTIVES:

- Introduce the readers to data communication and its fundamentals
- Define networks.
- Define protocols .
- Standards in networking.
- 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 is 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.

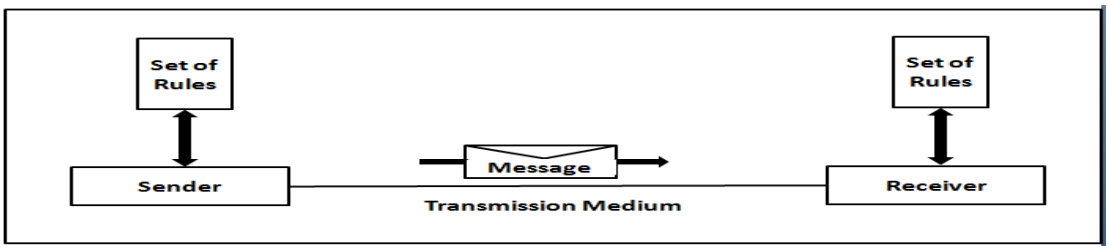
1.3.1 Characteristics of Data Communication

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

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**
    - An image is worth a thousand words‖ is a very famous saying. In computers images are digitally stored.
    - A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements.
    - The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel.
    - The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel.
    - Example: if an image is purely black and white (two color) each pixel can be represented by a value either 0 or 1, so an image made up of 10 x 10 pixel elements would require only 100 bits in memory to be stored.
    - On the other hand an image that includes gray may require 2 bits to represent every pixel value (00 - black, 01 – dark gray, 10 light gray, 11 white). So the same 10 x 10 pixel image would now require 200 bits of memory to be stored.
    - Commonly used Image formats : jpg, png, bmp, etc

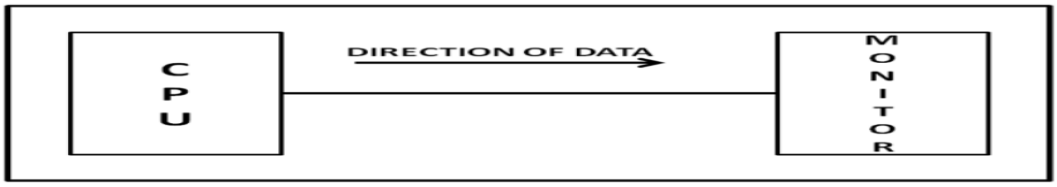
4. **Audio:** Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information.
   Audio data is continuous, not discrete.
5. **Video: Video** refers to broadcasting of data in form of picture or movie

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

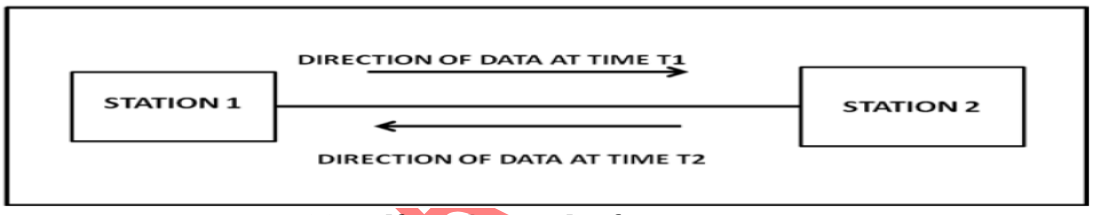
1.5.1 Simplex



Fig(2): Simplex mode of communication

- **In Simplex**, communication is unidirectional
- 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.

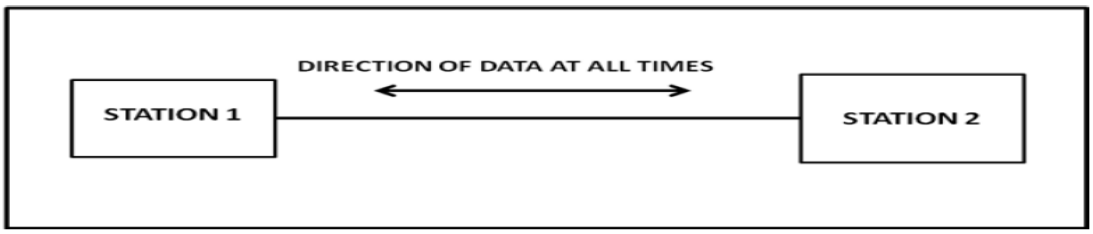
1.5.2 Half Duplex



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

- 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:

A. **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 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 one of the components of a data communications system. Without protocol communication cannot occur. The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly.
- When the sender sends a message it may consist of text, number, images, etc. which are converted into bits and grouped into blocks to be transmitted and often certain additional information called control information is also added to help the receiver interpret the data.
- For successful communication to occur, the sender and receiver must agree upon certain rules called 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.

1.7 STANDARDS IN NETWORKING

- Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.
- Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

1.7.1 Concept of Standard

- Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.
- Data communications standards are classified into two categories:

1. De facto Standard

- These are the standards that have been traditionally used and mean **by fact** or **by convention.**
- These standards are not approved by any organized body but are adopted by widespread use.

2. De jure standard

- It means by **law** or **by regulation.**
  - These standards are legislated and approved by a body that is officially recognized.

1.7.2 Standard Organizations in field of Networking

- Standards are created by standards creation committees, forums, and government regulatory agencies.
- **Examples of Standard Creation Committees** :
  1. International Organization for Standardization(ISO)
  2. International Telecommunications Union Telecommunications Standard (ITU-T)
  3. American National Standards Institute (ANSI)
  4. Institute of Electrical & Electronics Engineers (IEEE)
  5. Electronic Industries Associates (EIA)

o **Examples of Forums**

1. ATM Forum
2. MPLS Forum
3. Frame Relay Forum

Examples of Regulatory Agencies:

1. Federal Communications Committee (FCC)

1.9 REFERENCES

1. Data Communication & Networking – Behrouz Forouzan

2. Data Communications (More Details)

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 **bi**nary digi**t** 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: C**an 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.
- **Destiny:** The user at the other end finally receives the message through the data terminal equipment stationed at the other side.

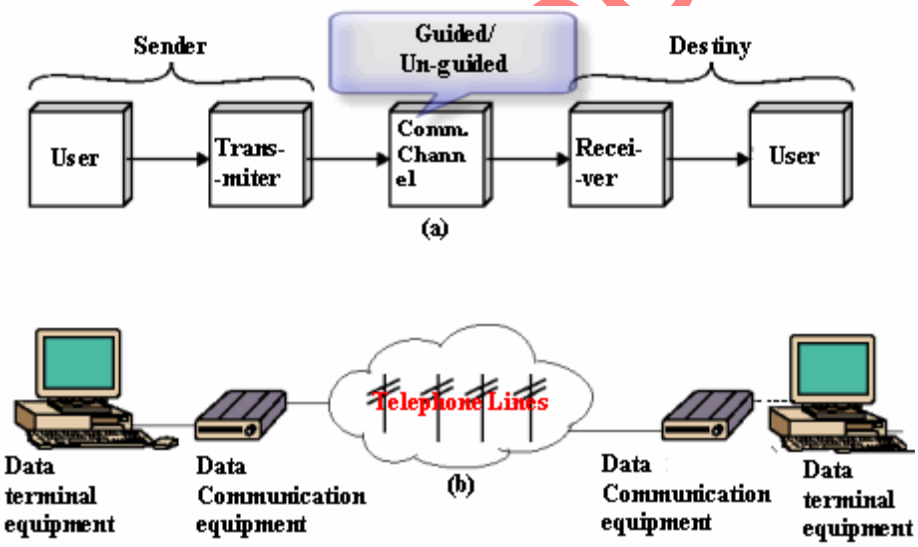


Fig 1.1 (a) The block diagram of a data communication model
(b) A typical dial-up network

Fig 1.1 (b) shows a typical dial-up network setup. The Data Communication Equipment (DCE) at the transmitting end converts the digital signals into audio tones (modulation) so that the voice grade telephone lines can be used as guided media during transmission. At the far end the receiving audio tones, they are converted back to digital signals (Demodulation) by the *data communication equipment* (DCE) and fed to the far end data terminal equipment (DTE).

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).

==========Sheet N0. One==========

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

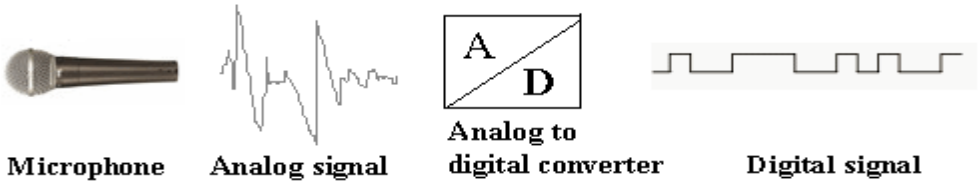


Fig 1.2.1 Example of analog and digital signal

1.3 Analog signal.

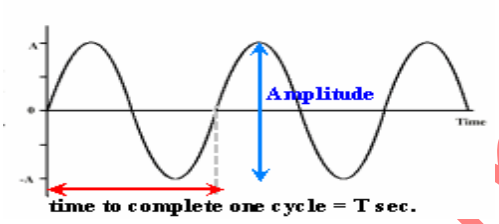


Fig 1.3.1 A simple sine wave and its parameters.

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 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

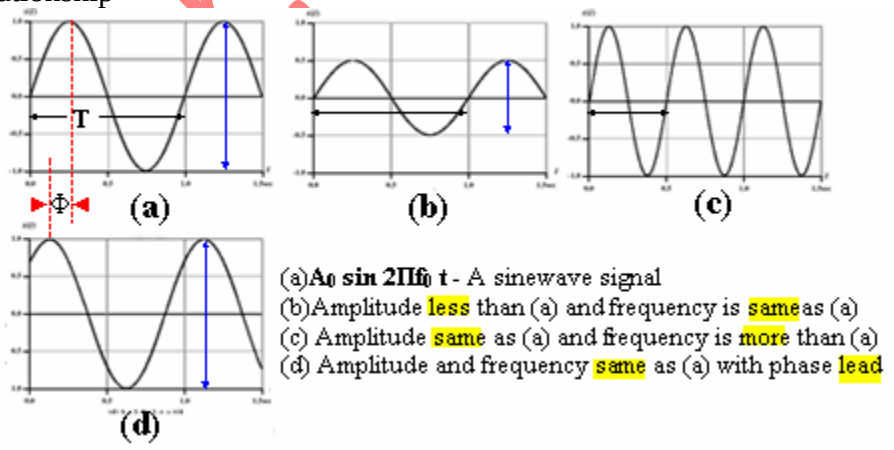


Fig 1.4.1 Different wave forms with different parameters

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.

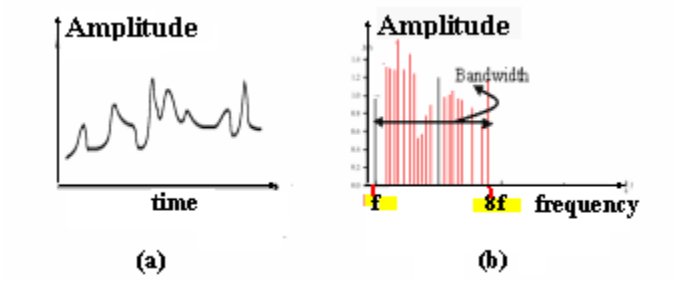


Fig 1.5.1 (a) An analog signal(b) Its various frequency components.

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.

Rate of transmission = (bits per second)

1kbps = 1000bps
1Mbps = 10^6 bps
1Gbps = 10^9 bps

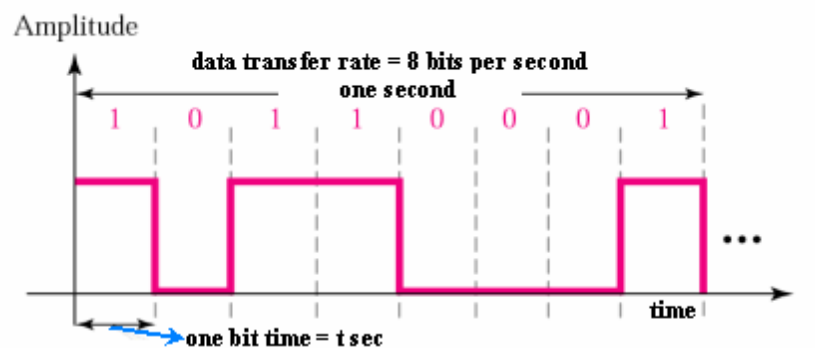


Fig 1.5.2 Relation between bit time and rate

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.

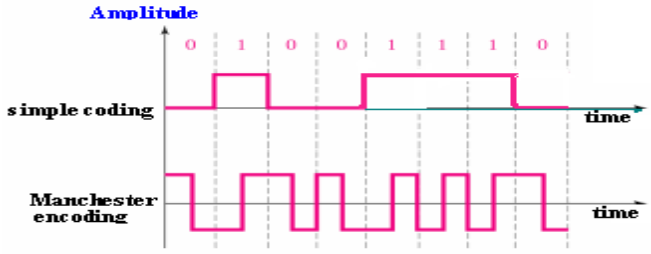


Fig 1.5.3 Manchester encoding

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.
- **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.

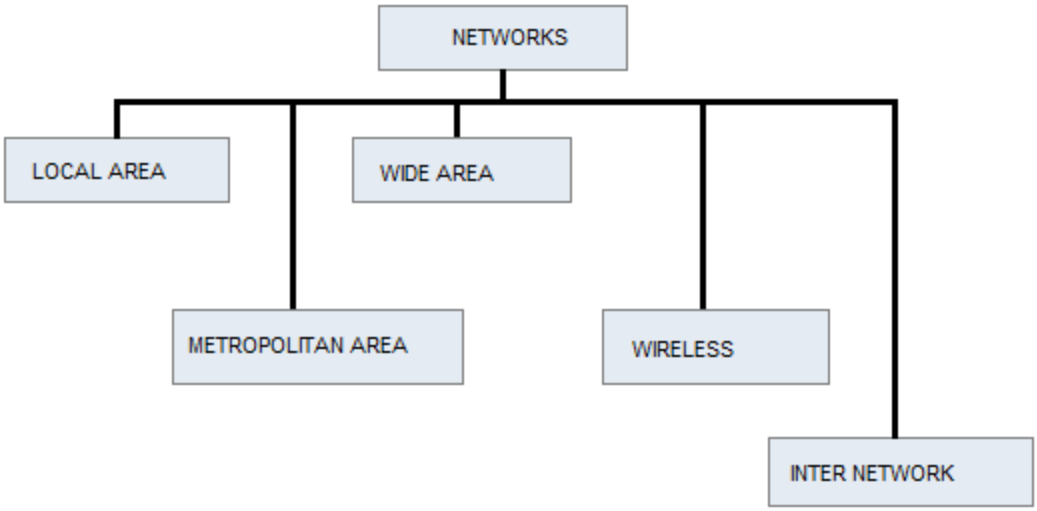
Then the channel capacity
(in cycles per second) according to **Shannon's** theorem is given by:

$$\mathbf{C = B \log_2 (1+SNR)}$$

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

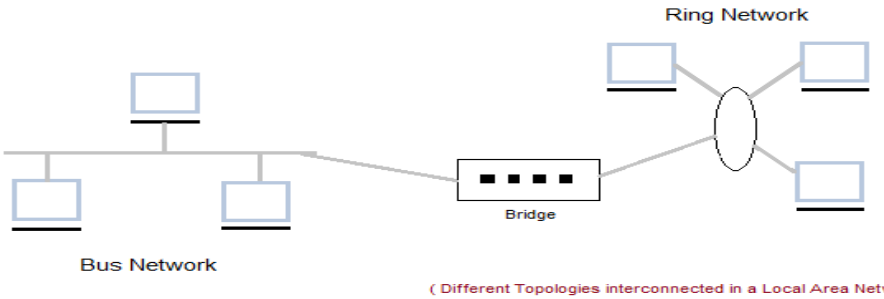


1.Local Area Network (LAN)

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.



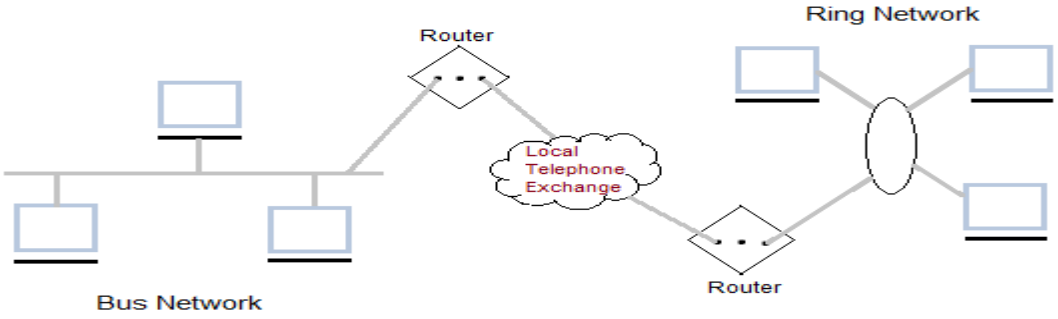
(Different Topologies interconnected in a Local Area Network)

3.1Applications 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.

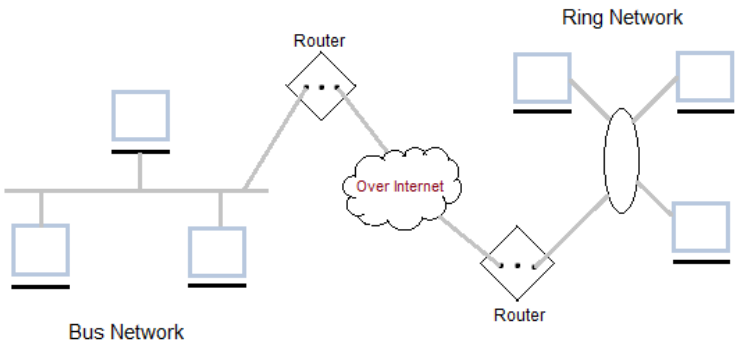
2.Metropolitan Area Network (MAN)

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.



3.Wide Area Network (WAN)

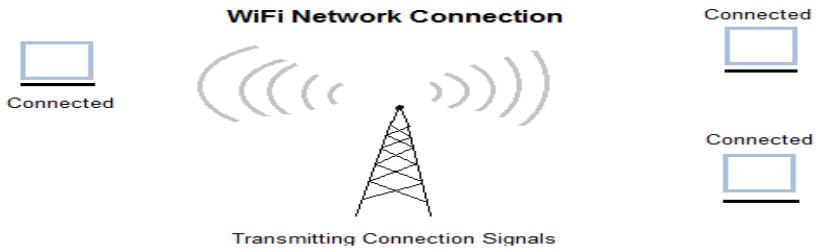
It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



4.Wireless Network

It is the fastest growing segment of computer. They are becoming very important in our daily life because wind 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 Types of communication

Based on the requirements, the communications can be of different types:

- **Point- to-point communication:** In this type, communication takes place between two end points. For instance, in the case of voice communication using telephones, there is one calling party and one called party. Hence the communication is point-to-point.
- **Point-to-multipoint communication:** In this type of communication, there is one sender and multiple recipients. For example, in voice conferencing, one person will be talking but many others can listen. The message from the sender has to be *multicast* to many others. Location from which information is sent to many recipients, as in the case of audio or video broadcasting. In a broadcasting system, the listeners are passive, and there is no reverse communication path.
- **Simplex communication:** In simplex communication, communication is possible only in one direction. There is one sender and one receiver; the sender and receiver cannot change roles.
- **Half-duplex communication:** Half-duplex communication is possible in both directions between two entities (computers or persons), but one at a time. A walkie-talkie uses this approach. The person who wants to talk presses a talk button on his handset to start talking, and the other person's handset will be in receive mode. When the sender finishes, he terminates it with an over message. The other person can press the talk button and start talking. These types of systems require limited channel bandwidth, so they are low cost systems.
- **Full-duplex communication:** In a full-duplex communication system, the two parties the caller and the called can communicate simultaneously, as in a telephone system. However, note that the communication system allows simultaneous transmission of data, but when two persons talk simultaneously, there is no effective communication! The ability of the communication system to transport data in both directions defines the system as full duplex.

Depending on the type of information transmitted, we have voice communication, data communication, fax communication, and video communication systems. When various types of information are clubbed together, we talk of multimedia communications. Even a few years ago, different information media such as voice, data, video, etc. were transmitted separately by using their own respective methods of transmission. With the advent of digital communication and "convergence technologies," this distinction is slowly disappearing, and multimedia communication is becoming the order of the day.

1.9 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. **Protocols** are implemented for these types of transmissions so that the communication takes place in a well-defined manner. Protocols are mutually(تبادليا) agreed set of(متفق عليه) rules and are necessary because the format of transmission should be understood by the receiver

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

- **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. There are two approaches regarding transmission of serial data.

- **Asynchronous transmission**
- **Synchronous transmission**

1.9.1 Asynchronous transmission

In asynchronous transmission data is transferred character by character and each character (frame by frame i.e. each character is an asynchronous frame in asynchronous transmission) and can be 5 to 8 bits long. The term "Asynchronous" means it is asynchronous at frame level. The bits are still synchronized at bit level during reception.

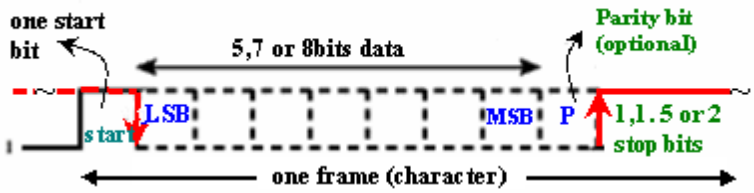


Fig 1.9.1 Asynchronous data format

- In a steady stream, interval between characters is uniform (length of stop element can be 1,1.5 or 2 stop bits - as programmed earlier)
- In idle state, receiver looks for transition 1 to 0 (start signal)
- Then samples next five, seven or eight intervals (as programmed earlier) Timing only needs maintaining within each frame (bit level).
- Looks for parity (if programmed earlier)
- Then looks for next 1 to 0 for next frame
- Simple
- Cheap. Minimum hardware & software requirement to impliment.
- Overhead of 2 or 3 bits per frame (~20%)
- Good for data with large gaps in between each frame (keyboard, low speed data..)

1.9.2 Synchronous transmission

In Synchronous transmission a block of data in the form of bits stream is transferred without start / stop bits. The block can be of any arbitrary length. In order to establish synchronization with remote computer the transmitter transmits synch pulses initially. When the receiver locks to the transmitter's clock frequency a block of data gets transmitted. See fig.1.9.2

The Characteristics are as follows

- Block of data transmitted without start or stop bits
- Initially synch pulses are transmitted (Clocks must be synchronized)
- Can use separate clock line (In that case synch pulses are not needed!)
- Good over short distances
- Subject to impairments
- Embed clock signal in data (Manchester encoding)
- Carrier frequency (analog) is used
- Need to indicate start and end of block
- Use preamble and post amble (to leave sufficient space between blocks)
- More efficient (lower overhead) than asynchronous transmission.

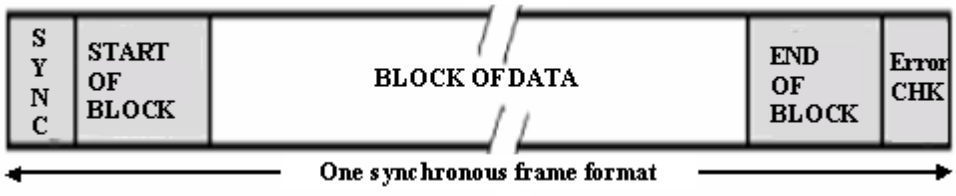


Fig 1.9.2 The synchronous frame format

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.

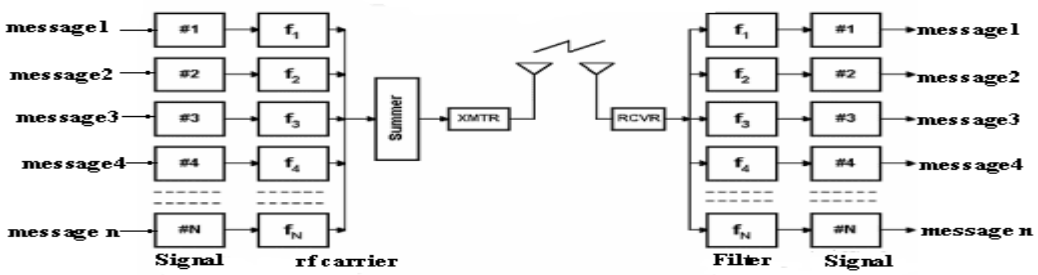


Fig 1.10.1 Frequency domain multiplexing

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.

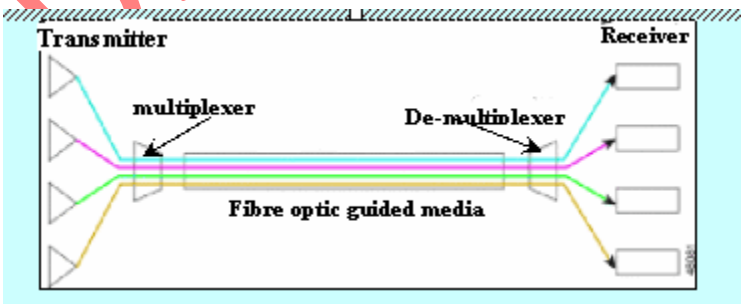


Fig 1.10.2 A Typical wavelength division multiplexer

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.

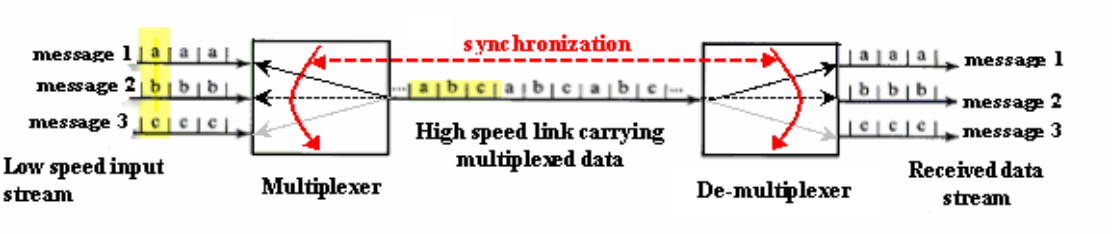


Fig. 1.10.3 Time division multiplexing.

1.11 Network Models

When people to people, machines to machines started communicating with each other the networking technology started picking up. Different vendors started manufacturing their proprietary configurations. 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.

Especially in data communications the way data traverses from the user to the destiny is a complex task that can be broken into several sub tasks, built one over the other like layers. Each layer takes input from the upper layer, performs its duty and hands over to the lower layer.

Several models were suggested out of which the Internet model is widely accepted. Later 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.
This kind of standardization allows communication across all types of computers.

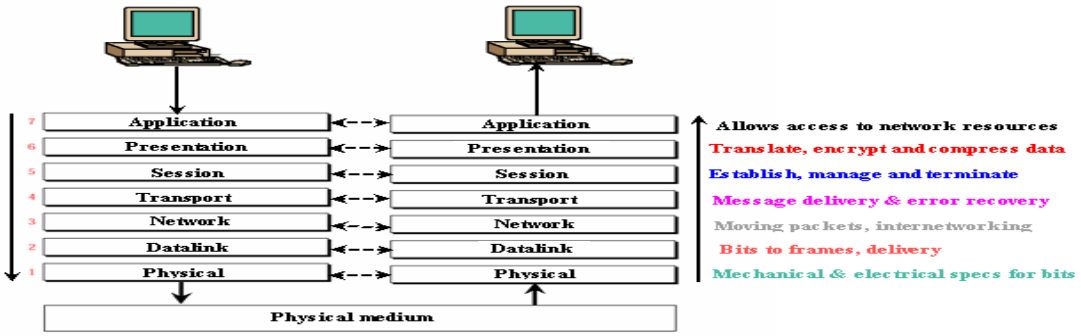


Fig 1.11.1 The OSI Layers and their functions

==========Sheet N0. One==========

Easy to remember these layers!……
Please **D**o **N**ot **T**ouch **S**hiva's **P**et **A**lligator

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

- **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

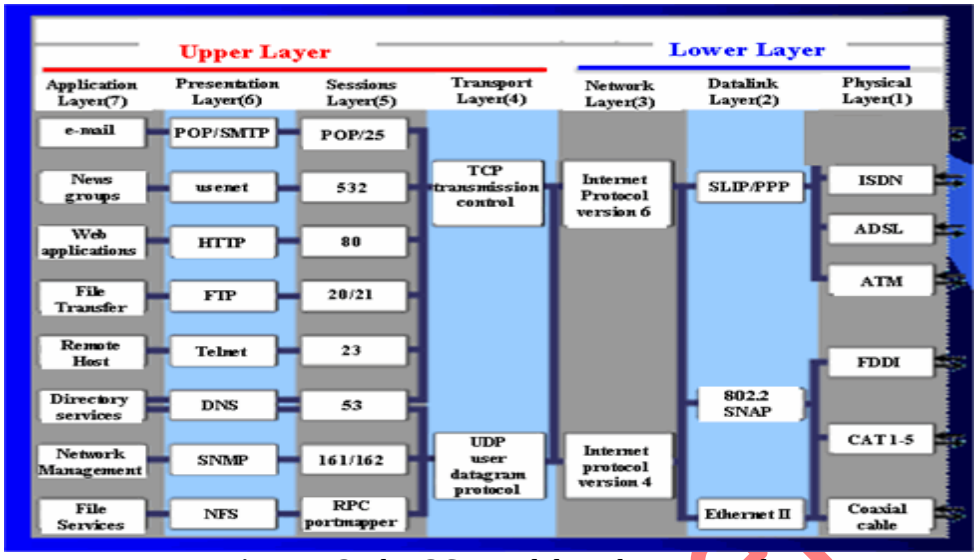


Fig 1.11.2 The OSI Model an their example services

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) IV) Data Link
V) & 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 divides the stream of characters into manageable segments. While receiving it creates stream of characters for application layer from received segments from network layer. Its function is much more than as depicted in OSI model. Some of the responsibilities of OSI's session layer are dissolved into Internet model's transport layer. The other protocol UDP is a simpler protocol. It ignores (يتجاهل) some of the duties of the transport layer defined in OSI model. It is used when 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.

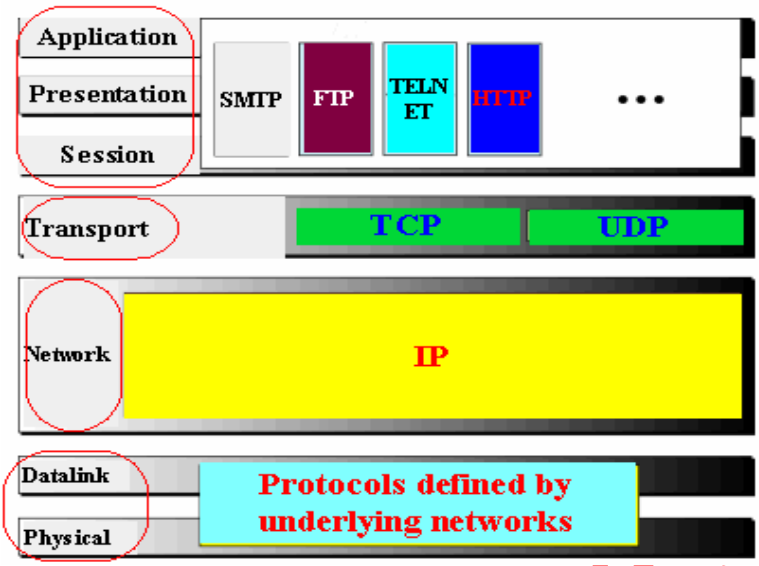


Fig 1.14 The Internet model

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

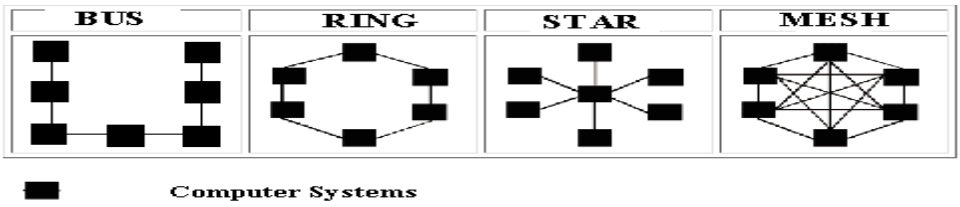


Fig 2.7.1 Outlines of various types of topologies

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.

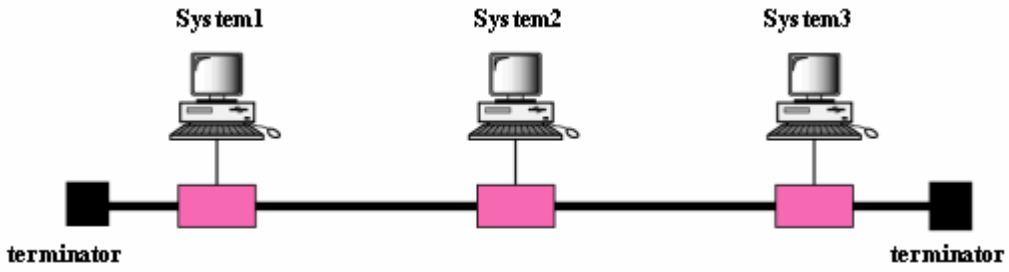


Fig 2.7.2 Physical topology of bus topology.

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.

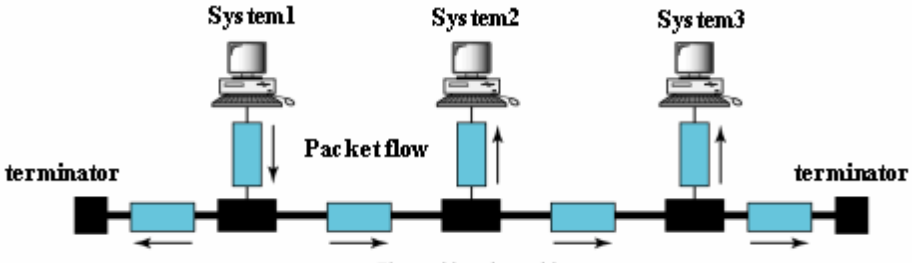


Fig 4.1 Logical topology illustration of bus topology.

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.

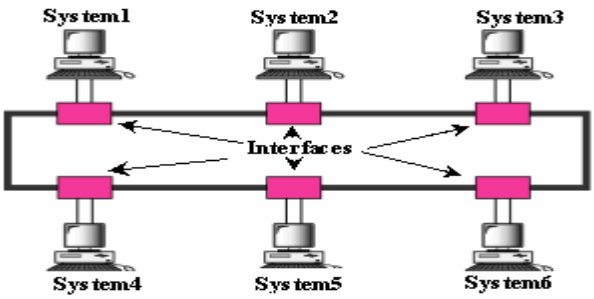


Fig. 4.2 Ring topology illustration.

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.

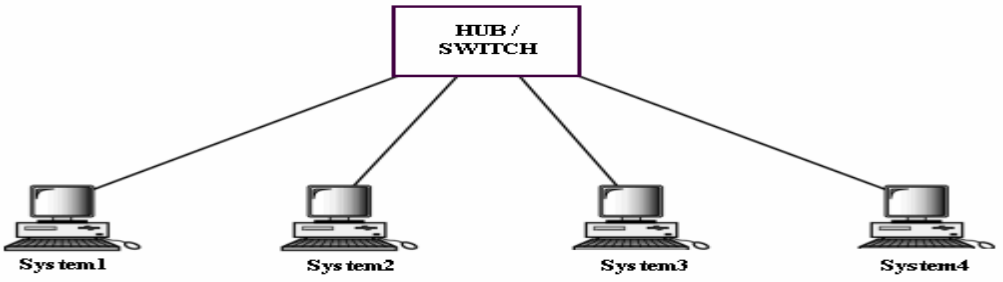


Fig 4.3. Physical topology of Star topology.

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.

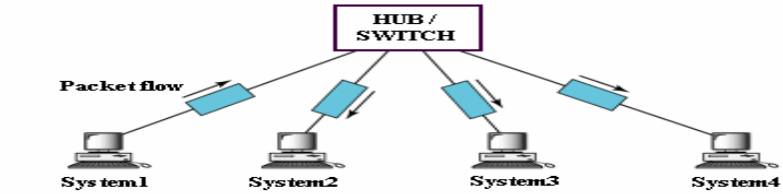


Fig 4.4 Logical topology of Star topology.

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.

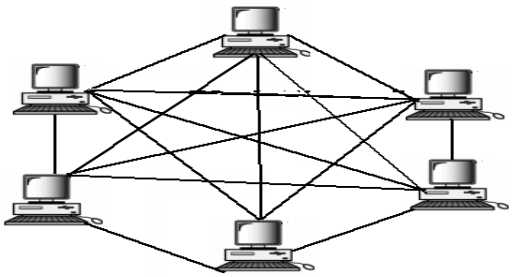


Fig 4.5 Physical topology of Mesh topology.

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?

A network is a set of equipment (often referred as Data Terminal Equipment / DTE, or simply terminals or nodes ..) connected by a communication channel, which can be either guided/unguided media. DTE equipment can be a computer, printer or any device capable of sending and/or receiving data generated by other nodes on the network.

a. 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**.**

5. Types of networks

5.1 Point to point

Figure 5.1 shows a communication system used to interconnect two computers. The computers output electrical signals directly through the serial port. The data can be

passed directly through the communication medium to the other computer if the distance is small (less than 100 meters).

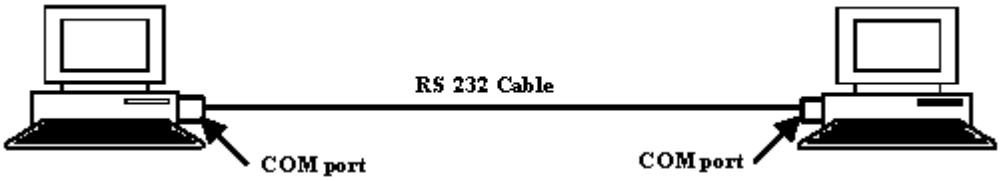


Fig. 5.1 PC to PC communication using com ports

Figure 5.1 shows a communication system in which two PCs communicate with each other over a existing say local telephone exchange (PABX) network. In this system, we introduced device called DTE data terminal equipment. The example here for DTE is modem (modulator demodulator) connected at both ends. The PCs send digital signals, which the modem converts into analog signals and transmits through the medium (copper wires). At the receiving end, the modem converts the incoming analog signal into digital form and passes it on to the PC.

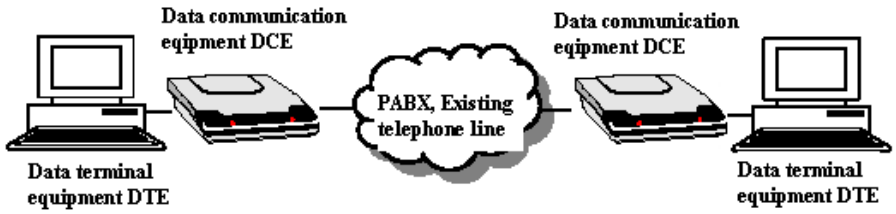


Fig.5.2 PC to PC communication over existing telephone network

5.3 Local Area Network (LAN)

A LAN is a local area network that is a small collection of computers in a small geographic area of less than couple of kilometers and is very fast in data transfer. Depending on technology implementation a LAN can be as simple as two PCs and a printer got connected in a small office or it can extend through out an organization and include multimedia (text, voice, video) data transfers.

The LANs may be configured in many ways. The peer-to-peer configuration is the simplest form. In this configuration computers are connected together to share their recourses among themselves. In such configurations it is very difficult impose security features.

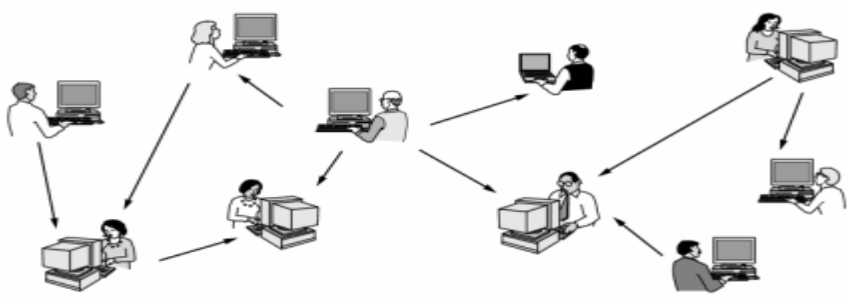


Fig 5.3 In a peer-to-peer configuration there is no security

On the other hand LANs can also be architectured in a client server model with full control over security and protection. Today Ethernet is a dominant LAN technology.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills(يستوفي) the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your which in turn serves it back to the client in your personal computer, which displays the information for you.

The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. So does the Internet's main program, TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing.

In the usual client/server model, one server, sometimes called a daemon, is activated and awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, your Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet.

Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet.

Other program relationship models included master/slave, with one program being in charge of all other programs, and peer-to-peer, with either of two programs able to initiate a transaction.

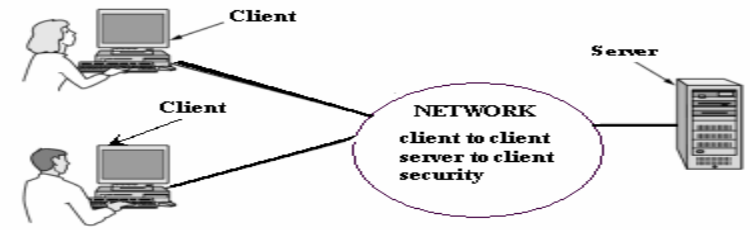


Fig 5.4 Client server model

A typical LAN in a corporate office links a group of related computers, workstations. One of the best computers may be given a large capacity disk drive and made as server and remaining computers as clients.

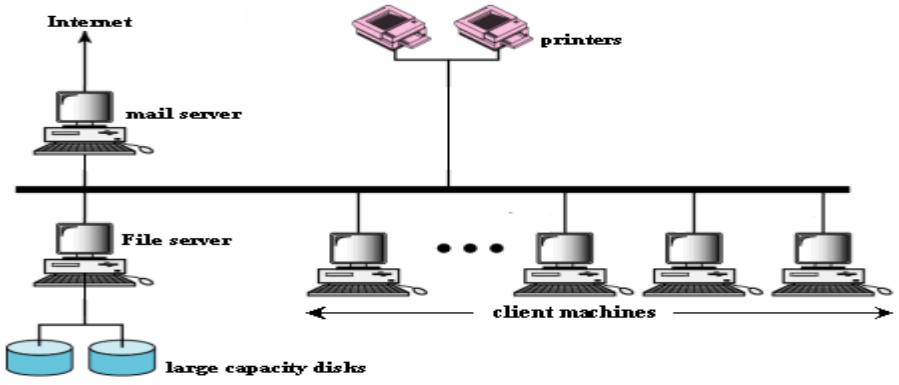


Fig. 5.5 A LAN setup

5.4 Metropolitan Area Network (MAN)

The metropolitan area network is designed to cover an entire city. It can be a single network such as cable TV or a number of LANs connected together within a city to form a MAN. Privately laid cables or public leased lines may be used to form such network. For instance a business organization may choose MAN to inter connect all its branch offices within the city.

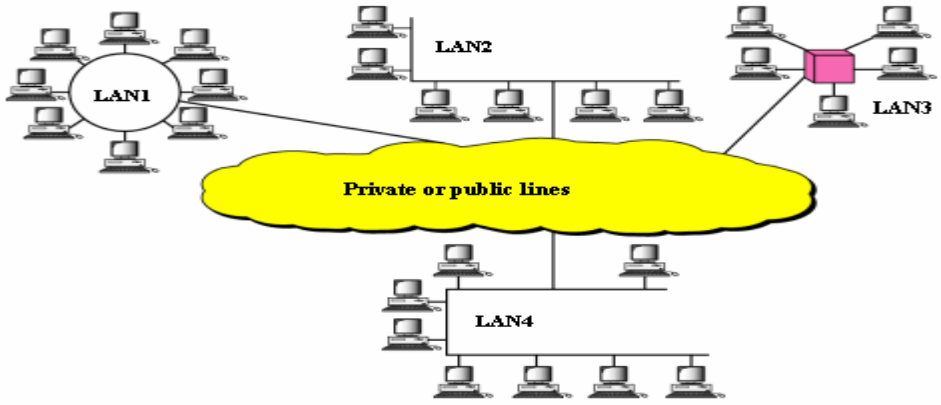


Fig 5.6 Typical Metropolitan area network

5.6 Wide Area Network (WAN)

A WAN is a data communications network that covers a relatively broad geographic area, often a country or continent. It contains a collection of machines intended for running user programs. These machines are called hosts.

The hosts are connected by subnet. The purpose of subnet is to carry messages from hosts to hosts. The subnet includes transmission facilities, switching elements and routers provided by common agencies, such as telephone companies. Now days, routers with satellite links are also becoming part of the WAN subnet. All these machines provide long distance transmission of data, voice, image and video information.

Unlike LAN which depend on their own hardware for transmission, WANs may utilize public, leased, or private communication devices when it come across and therefore span an unlimited number of kilometers. A network device called a router connects LANs to a WAN.

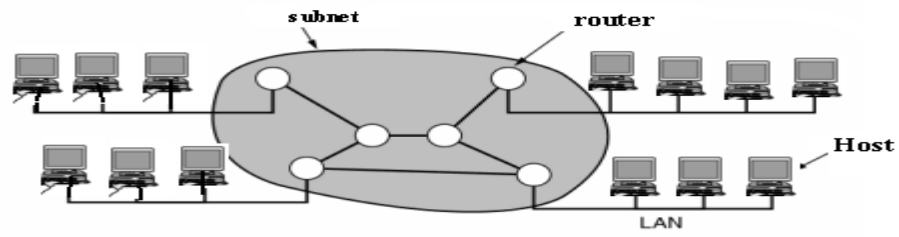


Fig 5.7 Typical WAN setup with hosts, routers and subnet.

The Internet is the largest WAN in existence.

5.6 Value added Network (VAN)

Value-added networks (VAN) are communications networks supplied and managed by third-party companies that facilitate electronic data interchange, Web services and transaction delivery by providing extra networking services.

A value-added network (VAN) is a private network provider (sometimes called a turnkey communications line) that is hired by a company to facilitate electronic data interchanges (EDI) or provides other network services. Before the arrival of the World Wide Web, some companies hired value-added networks to move data from their company to other companies. With the arrival of the World Wide Web, many companies found it more cost-efficient to move their data over the Internet instead of paying the minimum monthly fees and per-character charges found in typical VAN contracts. In response, contemporary value-added network providers now focus on offering EDI translation, encryption, secure email, management reporting, and other extra services for their customers.

Value-added networks got their first real foothold in the business world in the area of electronic data interchange (EDI). VANs were deployed to help trading and supply chain partners automate many businesses-to business communications and thereby reduce the number of paper transfers needed, cut costs and speed up a wide range of tasks and processes, from inventory and order management to payment.

Transaction Delivery Networks (TDN): The newest evolution of VANs, which first appeared in 2000, are the transaction delivery networks (TDN) that provide services for secure end-to-end management of electronic transactions. Also called transaction processing networks or Internet utility platforms, TDNs can guarantee delivery of messages in addition to providing high security and availability, network performance monitoring and centralized directory management.

TDNs typically use a store-and-forward messaging architecture that's designed to adapt readily to a wide range of disparate systems and support any kind of

transaction. Most TDNs offer secure encryption using a public-key infrastructure and certificate authorization for trading partners.

Internetworks: Internetwork or simply the internet are those when two or more networks are get connected. Individual networks are combined through the use of routers. Lowercase internet should not be confused with the worldwide Internet.

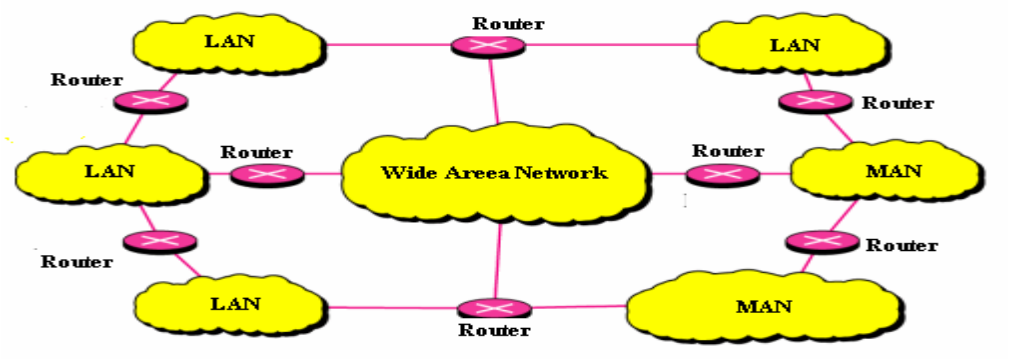
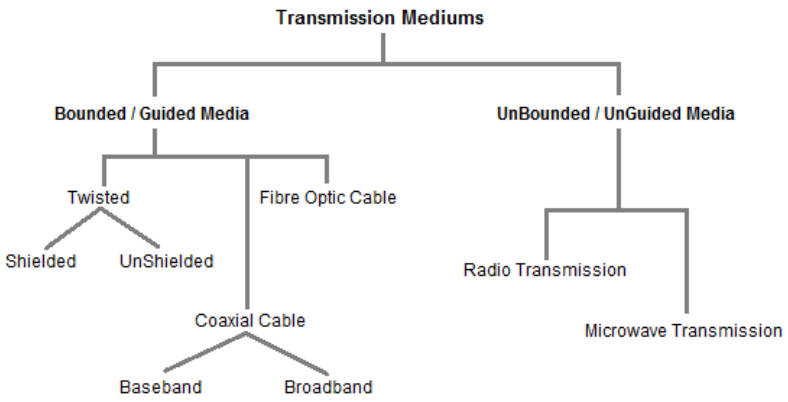


Fig 5.8 Typical internetwork connecting LANs and MANs

6.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).Electromagnetic energy (includes electrical and magnetic fields) includes power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media, we will study the OSI Model later.



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 µs/km.
- Repeater spacing is 2km.

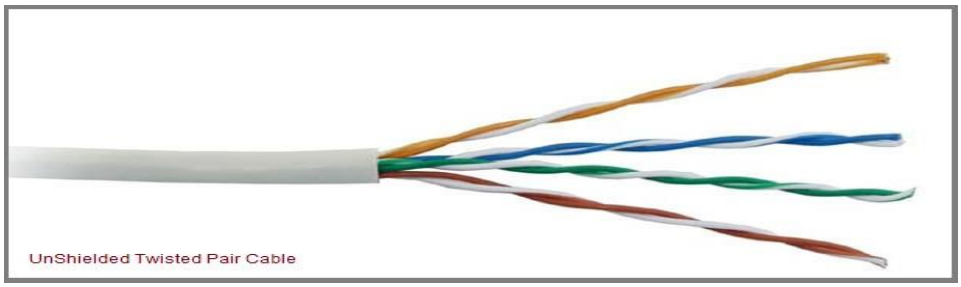
Twisted Pair is of two types :

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
- 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.

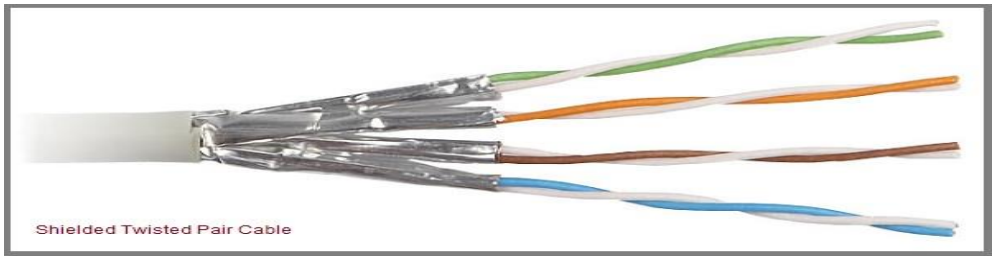
Disadvantages :

- 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.



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

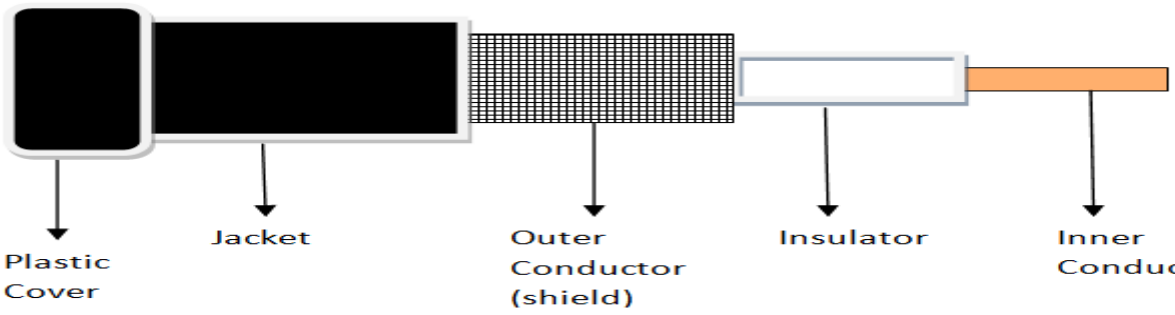
B.Coaxial Cable

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.



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 :

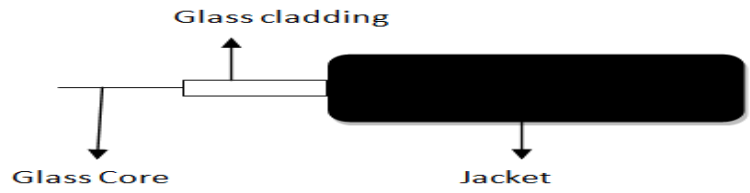
- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

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.

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 Propogation

Radio Transmission utilizes different types of propogation :

- **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

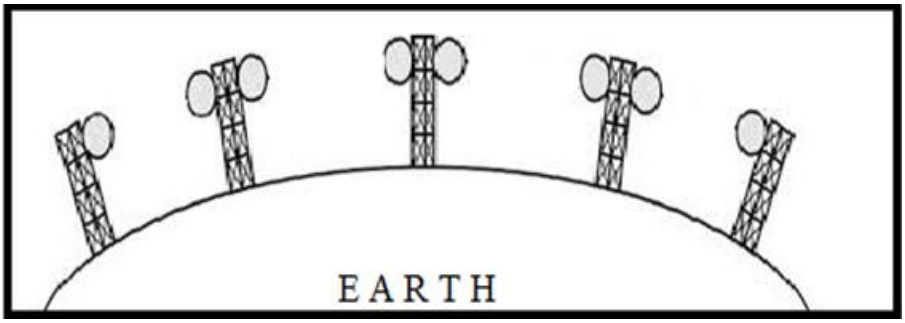
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly.

C.Terrestrial Microwave

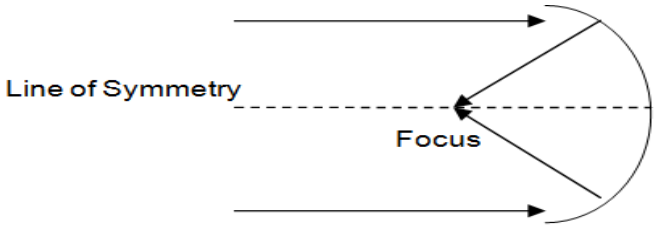
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



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.



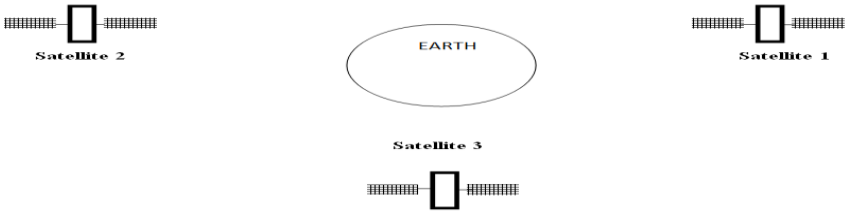
2. Horn Antenna

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 :

- 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

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?

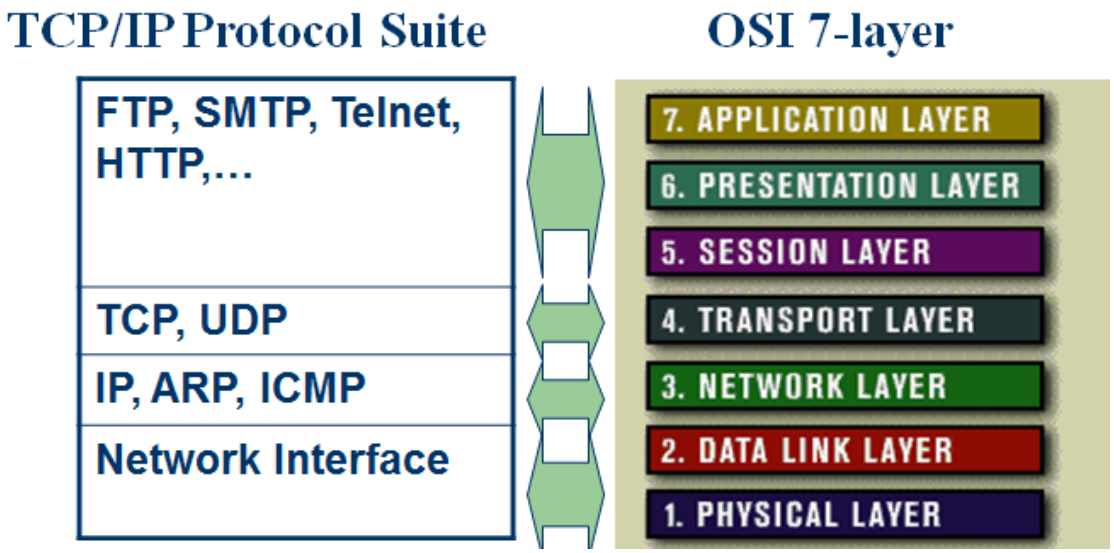
- **A protocol is a collection of rules and procedures for two computers to exchange information**
- **Protocol also defines the format of data that is being exchanged**

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

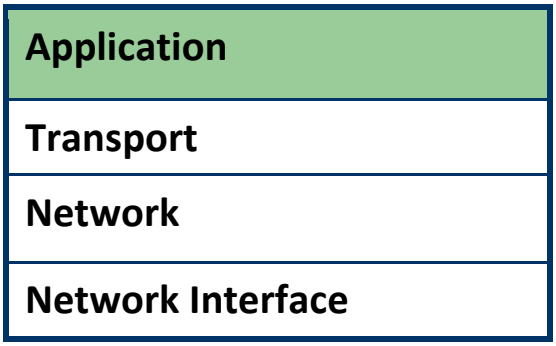
- **Because TCP/IP was developed earlier than the OSI 7-layer mode, it does not have 7 layers but only 4 layers**

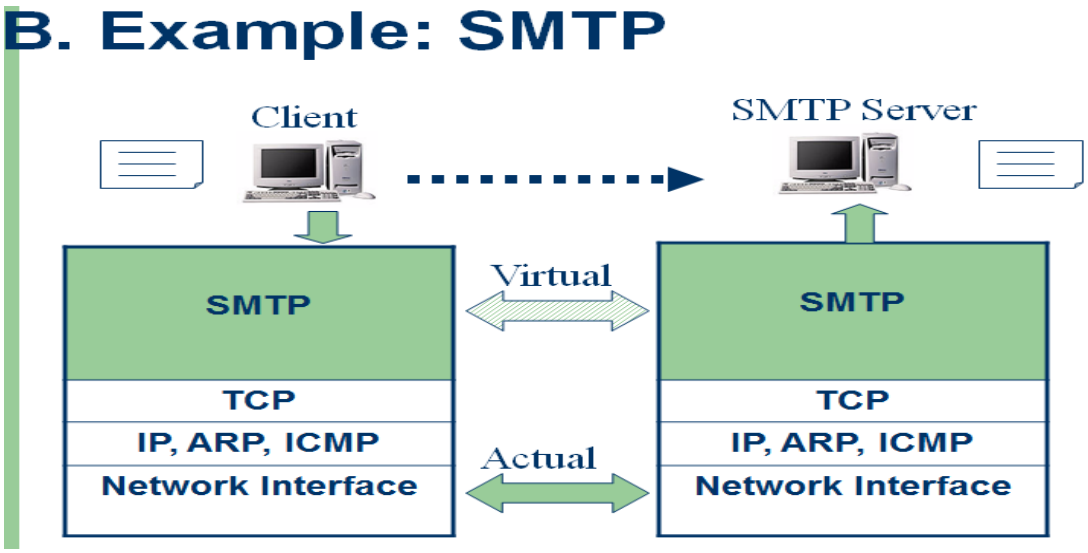


- **Application layer protocols define the rules when implementing specific network applications**
- **Rely on the underlying layers to provide accurate and efficient data delivery**
- **Typical protocols:**
  - **FTP – File Transfer Protocol**
    - **For file transfer**
  - **Telnet – Remote terminal 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**
- **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



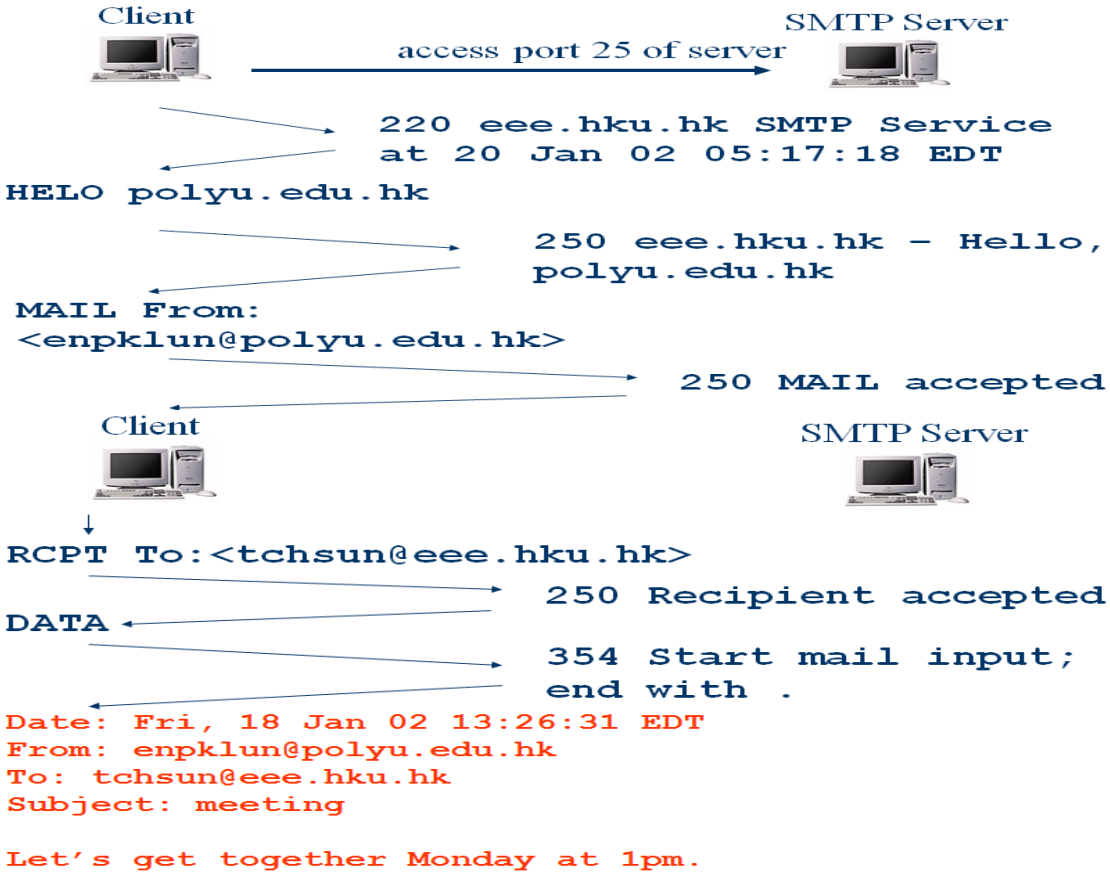


- **The underlying layers have guaranteed accurate data delivery**
- **We need to make a lot agreements with the server in application layer before sending mail**
- **Agree on how data is represented**
  - **Binary or ASCII**
- **Ensure the right recipient**
  - **There may be 1000 users served by the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

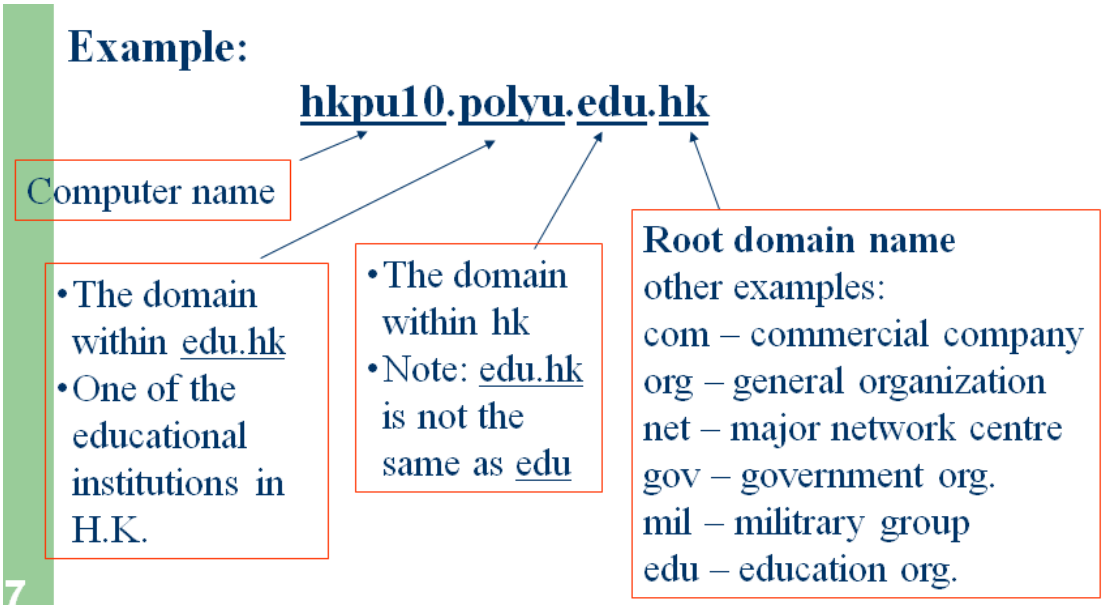


- **The agreement made in the SMTP protocol**
  - **All messages use normal text**
    - **All ASCII characters**
  - **The responses all begin with numbers**
    - **To indicate the status when receiving the command**
  - **Some words are reserved words**
    - **HELO, MAIL, RCPT…**
  - **Mail ends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

C. Domain Name:

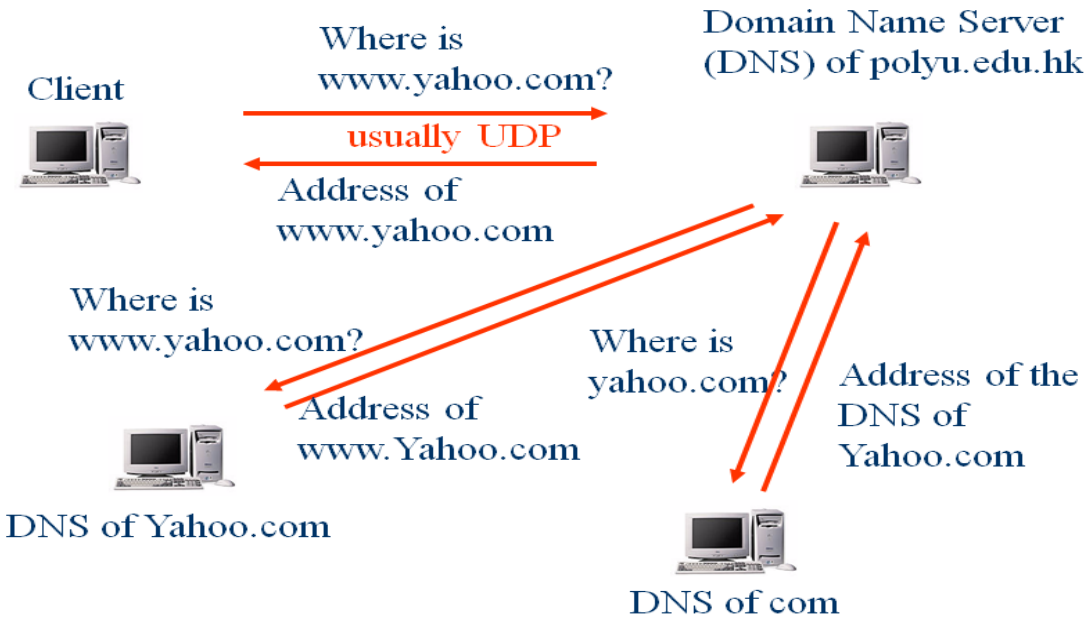
- **Every computer has a network address**
  - **e.g. 158.132.161.99**
- **To access a computer, we need to specify its network address**
- **Human beings are weak in memorizing numbers**
- **We prefer computer name or domain name**
  - **e.g. hkpu10.polyu.edu.hk**

- **Need a machine on the Internet to convert name to number**



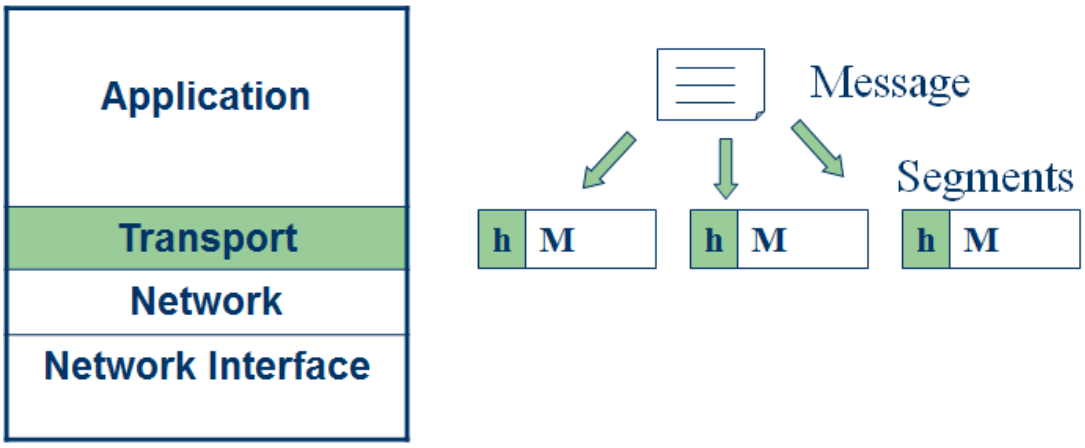
- **An organization needs to register its domain name**
  - **e.g. PolyU has registered its name to the domain of edu.hk**
- **Once a domain name is assigned, the organization is free to assign other names belong to its domain**
  - **e.g. we can have**

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



- **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

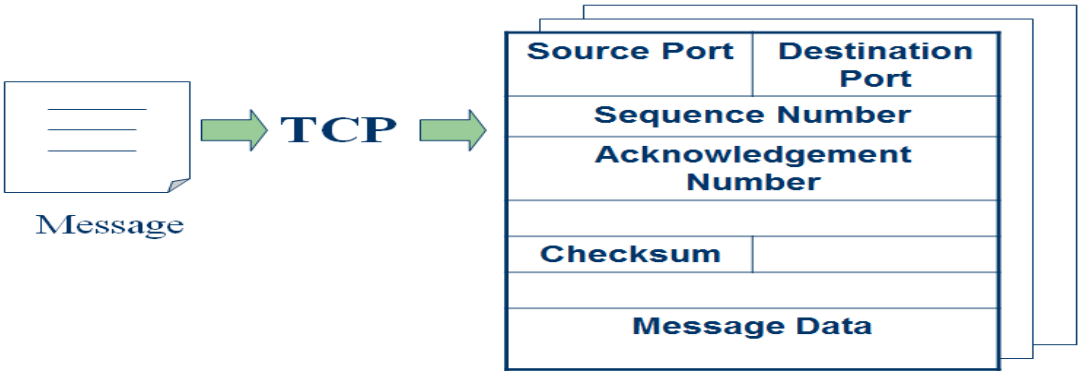


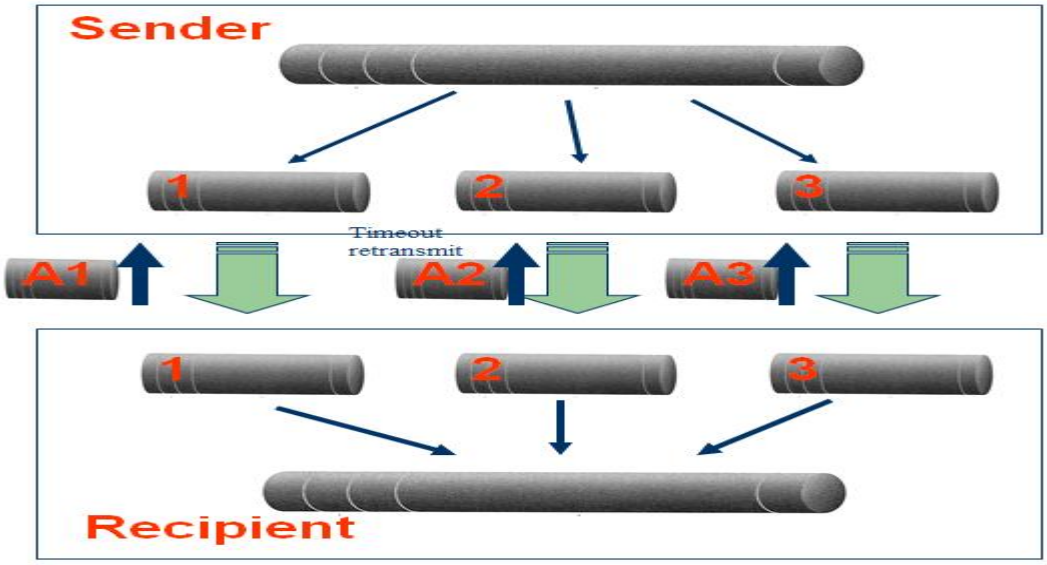
D. TCP and UDP

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

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**

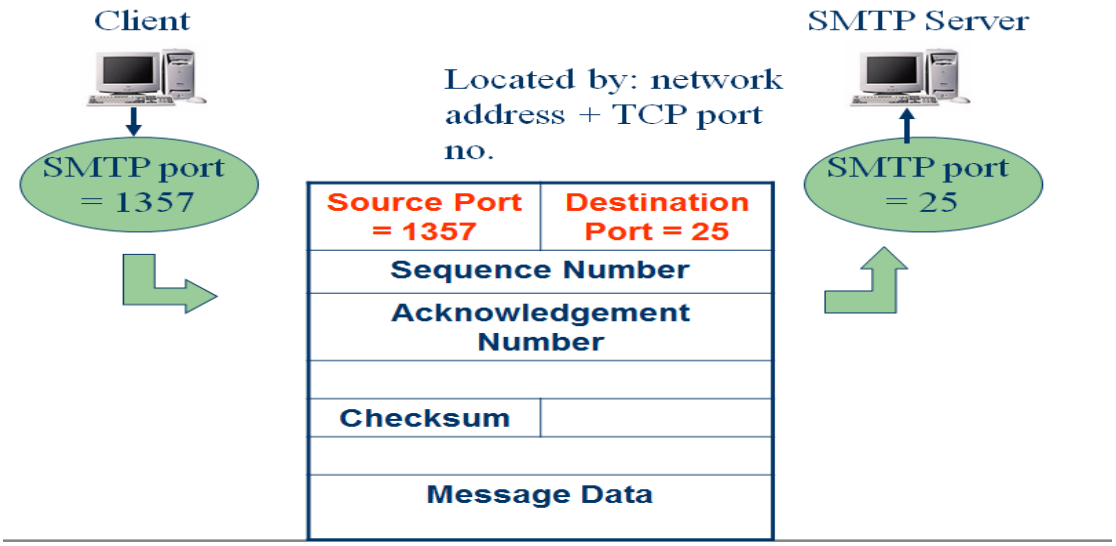
Port Multiplexing

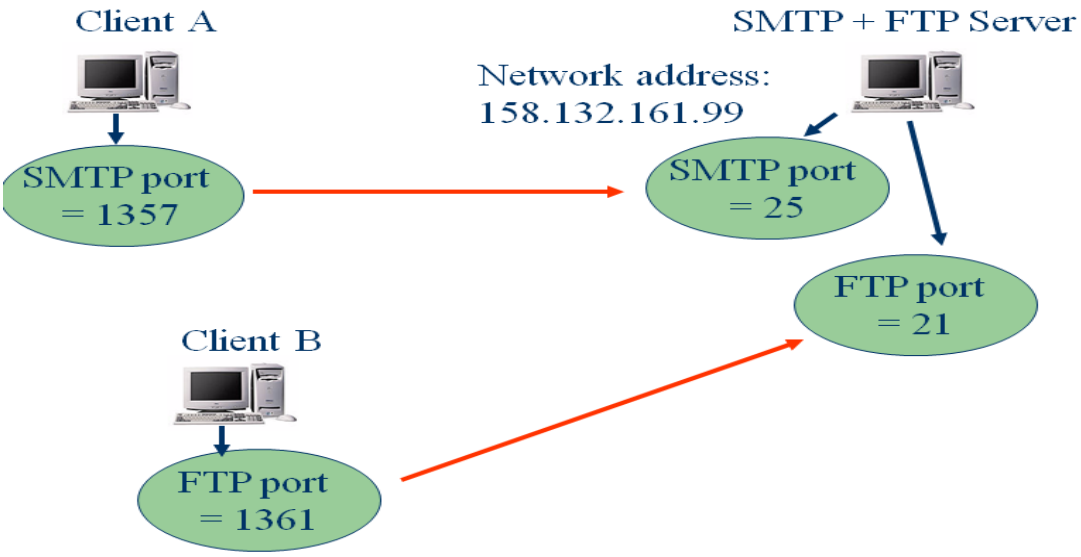
- **A computer may perform a number of network applications at the same time**
  - **FTP + SMTP + HTTP, etc.**
- **Each computer has only one network address, how can it serve so many applications at the same time?**

⇒ by port multiplexing

Well-known Port Numbers

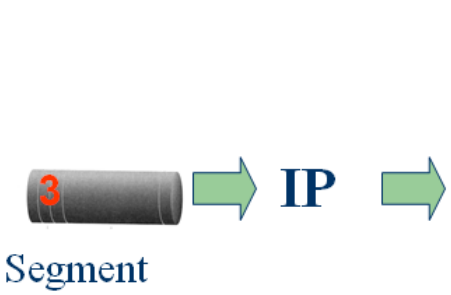
- **Some port numbers are reserved for some purposes**
  - **Port 21: FTP – file transfer**
  - **Port 25: SMTP – mail transfer**
  - **Port 23: TELNET – remote login**
  - **Port 80: HTTP – Web access**
- **These port numbers are well known to all computers in the network**
- **E.g. whenever a client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

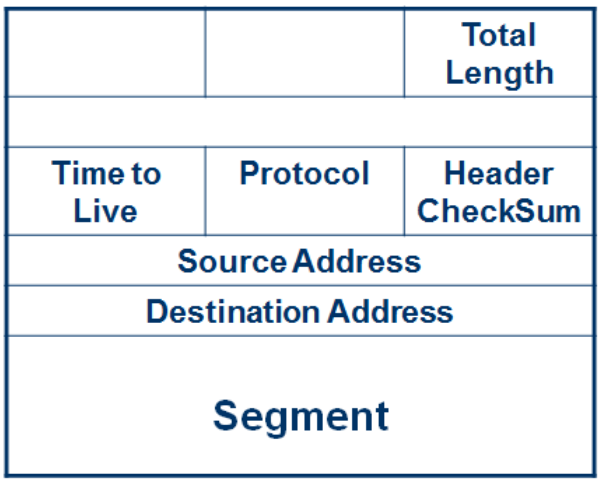




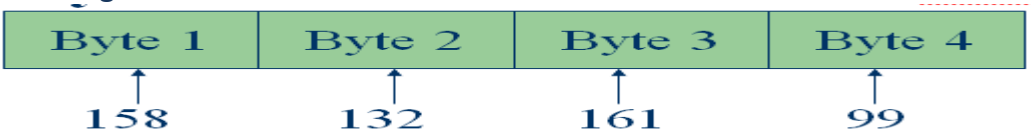
E. Network Addresses and Subnets

- **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.**



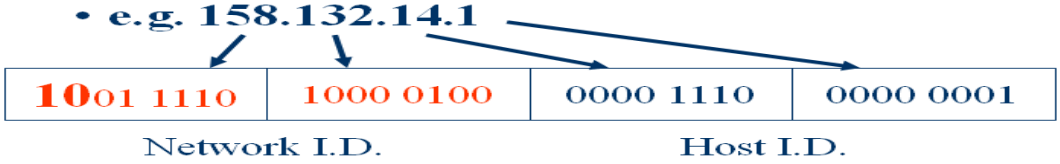
- **IP addresses are hierarchical**
  - **network I.D. and host I.D.**
- **Each Network I.D. on the Internet needs to be registered to the Internet Assigned Number Authority**

Class A – for very large network

- **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

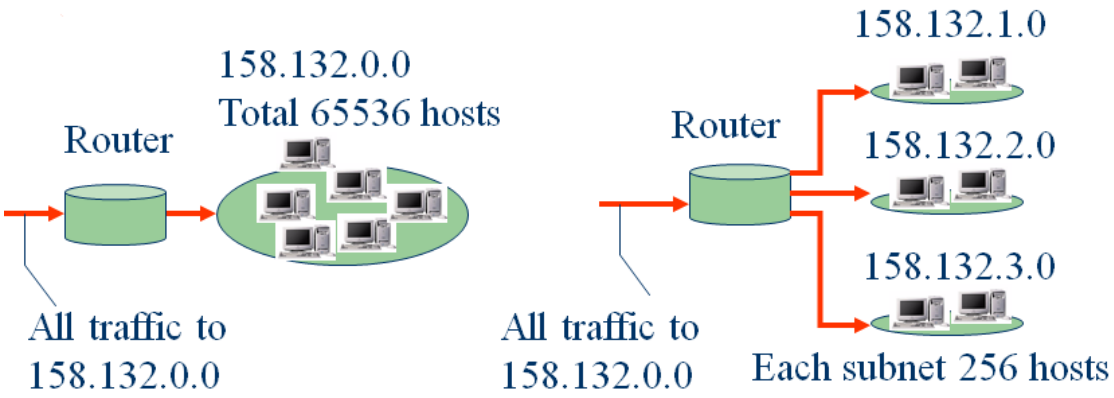
- Packets are addressed to a multicast group
- Not often supported on Internet

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
- 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

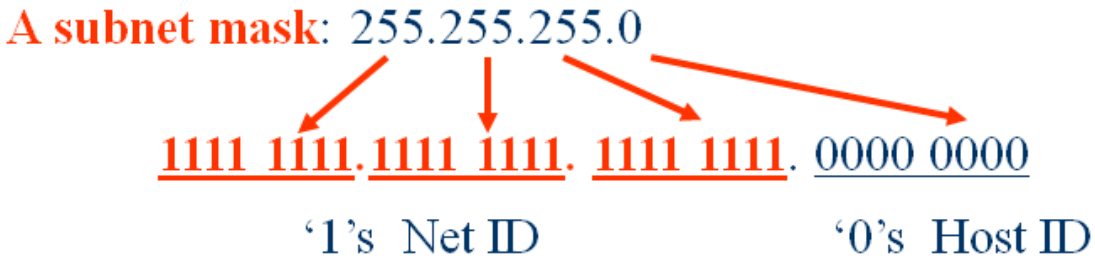
Subnets

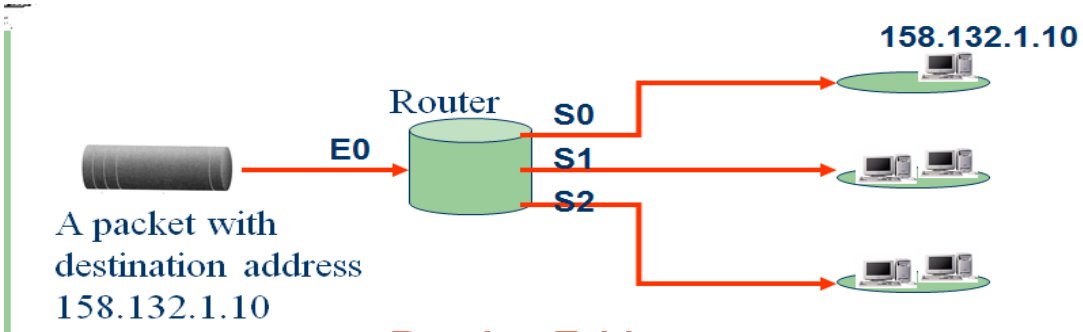
- Difficult to manage
- Usually subdivide into a few small subnets
- Subnetting can also help to reduce broadcasting traffic



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**





Routing Table

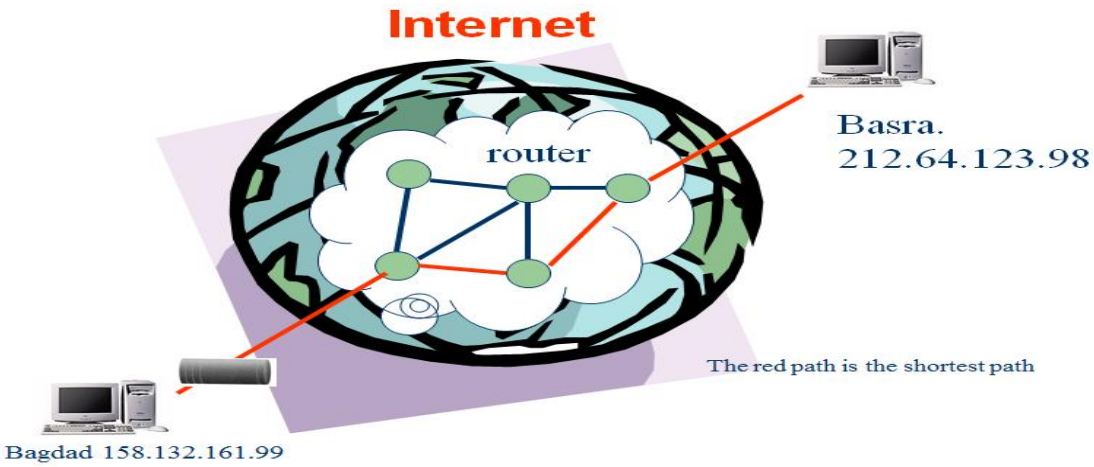
	S0	S1	S2
Subnet	158.132.1.0	158.132.2.0	158.132.3.0
Mask	255.255.255.0	255.255.255.0	255.255.255.0

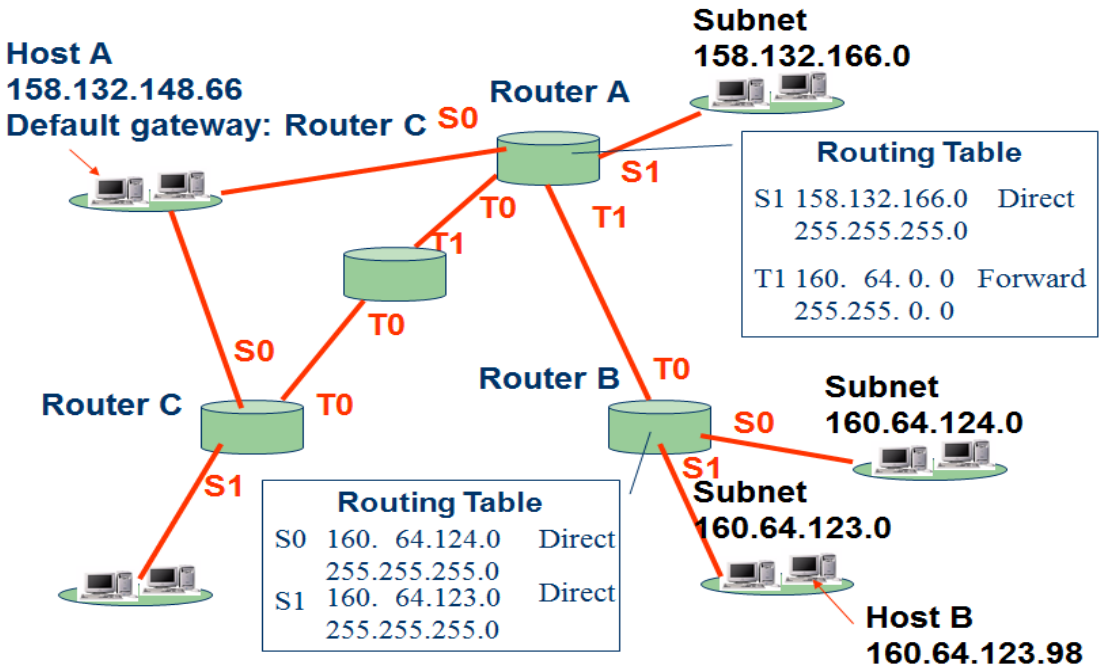
158.132. 1. 10 1001 1110.1000 0100.0000 0001.0000 1010
AND 255.255.255. 0 AND 1111 1111.1111 1111.1111 1111.0000 0000
158.132. 1. 0 1001 1110.1000 0100.0000 0001.0000 0000

Advantage: easy to compute

F. Routing

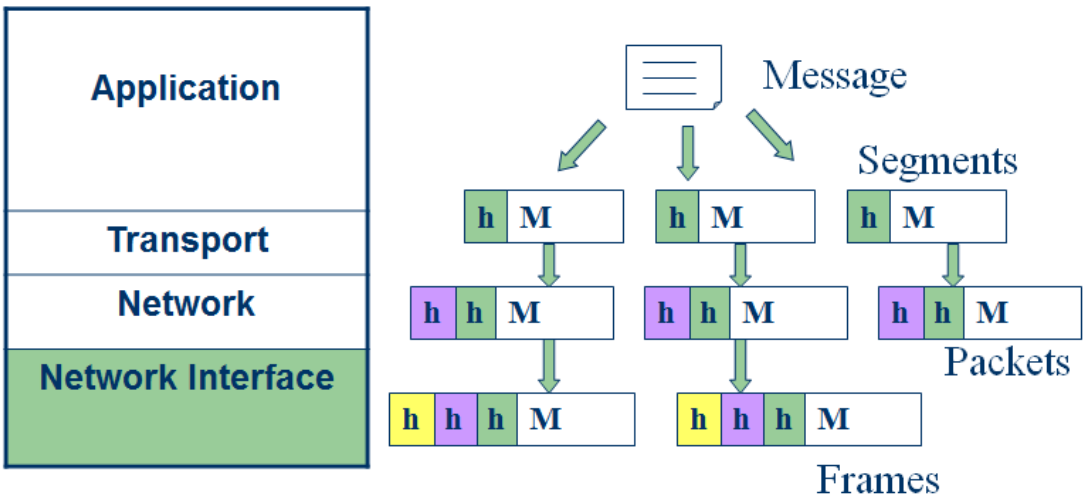
- How a packet finds its way to a computer in a network?
  - By using Routers
- Routing is the selection of a path to guide a packet from the source to the destination
- Criteria in selecting a path may be:
  - Shortest path
  - Quickest path
  - Cheapest path
- Each router has a table that records the 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





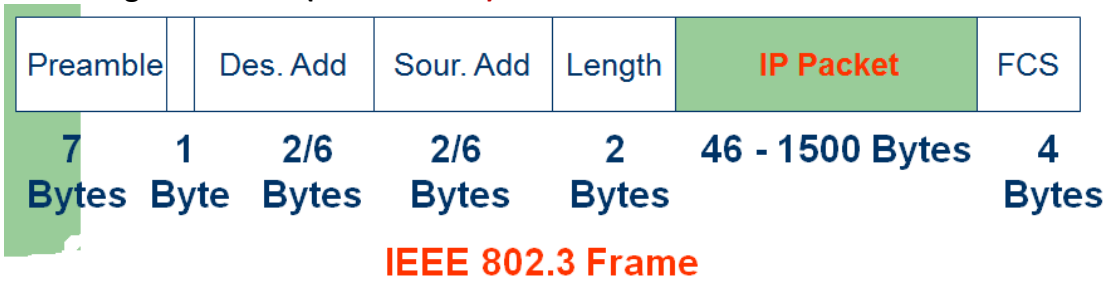
1. **Host A wants to send a packet to Host B with address 160.64.123.98**
2. **Host A checks that 160.64.123.98 is not in the same network**
3. **Send packet to default gateway (Router C)**
4. **Default gateway finds that it cannot provide the best route for the packet, inform Host A to send the packet 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

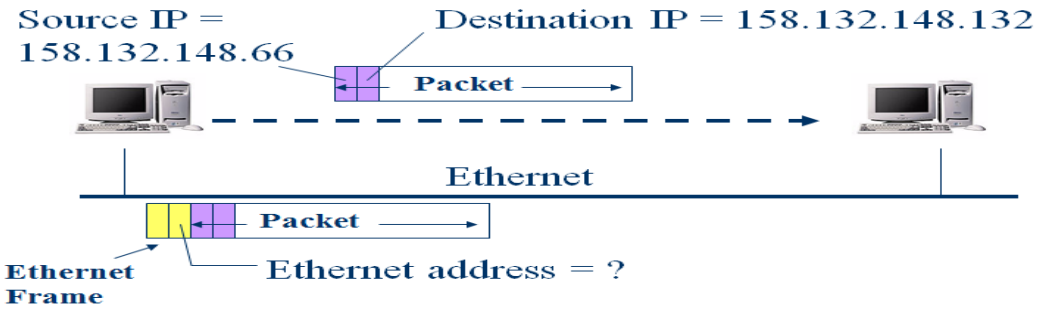


G. Ethernet Encapsulation and ARP

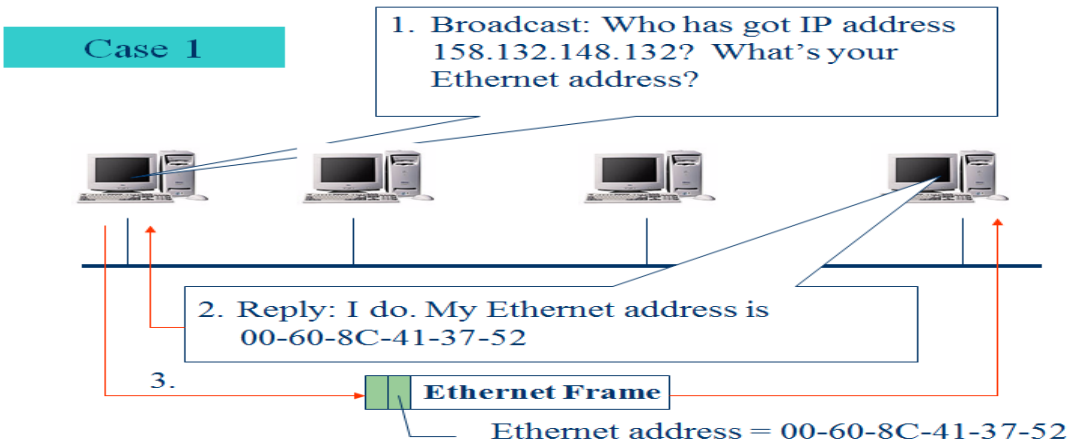
- **An IP packet should be encapsulated into a frame for transmission by data link layer**
- **e.g. if Ethernet (or IEEE 802.3) is used:**



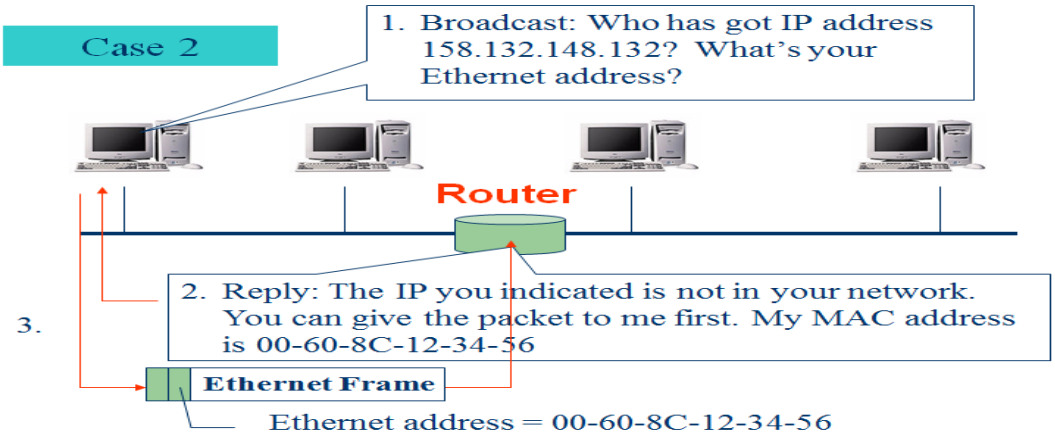
- **Only the hardware address (MAC address) is unique to a host**
- **Need to convert a network address to MAC address**



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

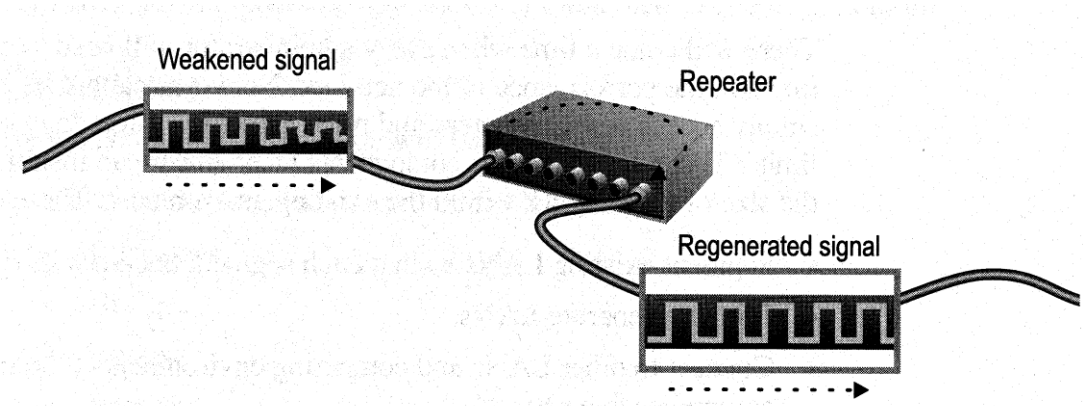
- segment (divide) large LAN to form smaller LANs
- connect LANs

Required components

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

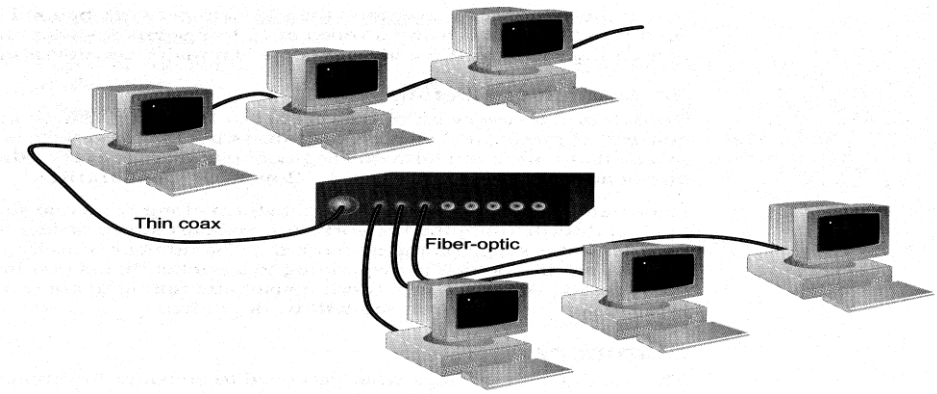
a. Repeaters and Hubs

- **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**

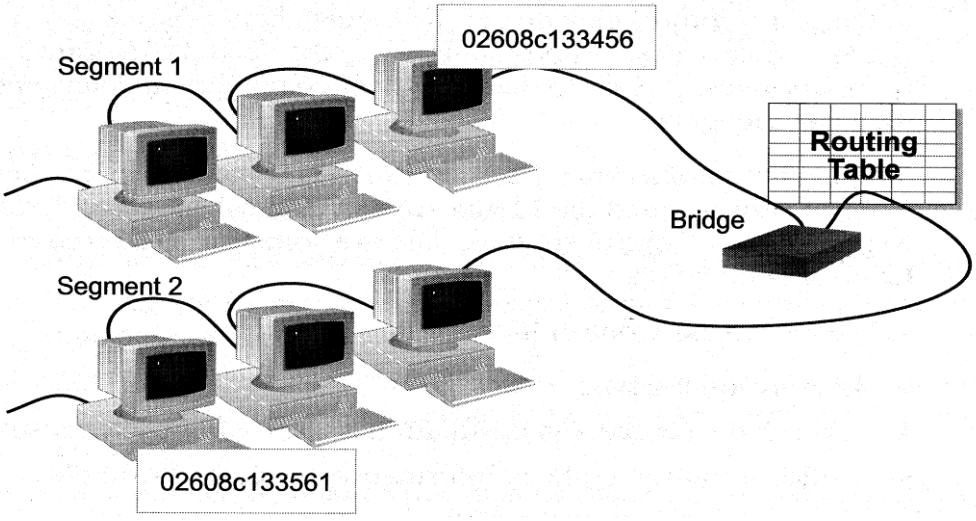


b. Bridges

- **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**

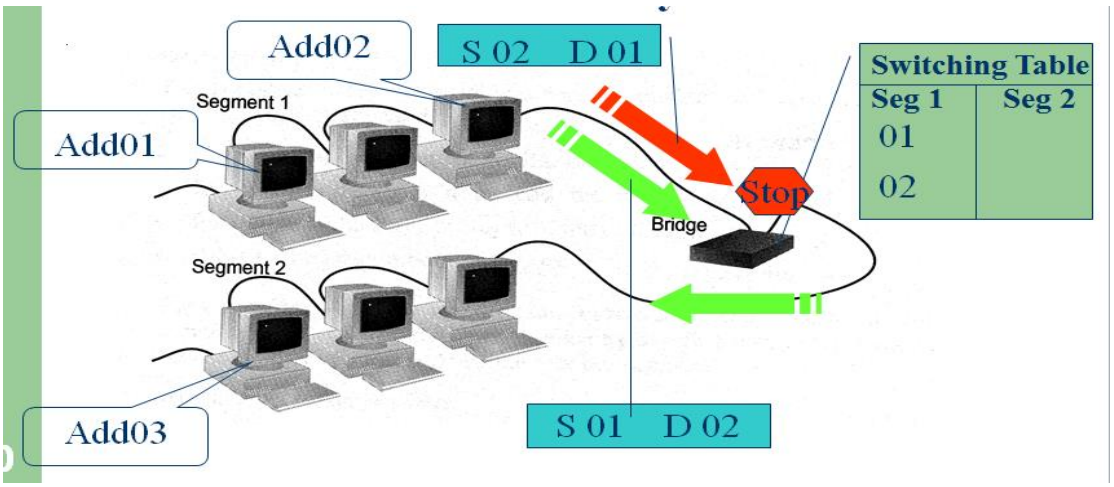
How Bridges Work

- **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**



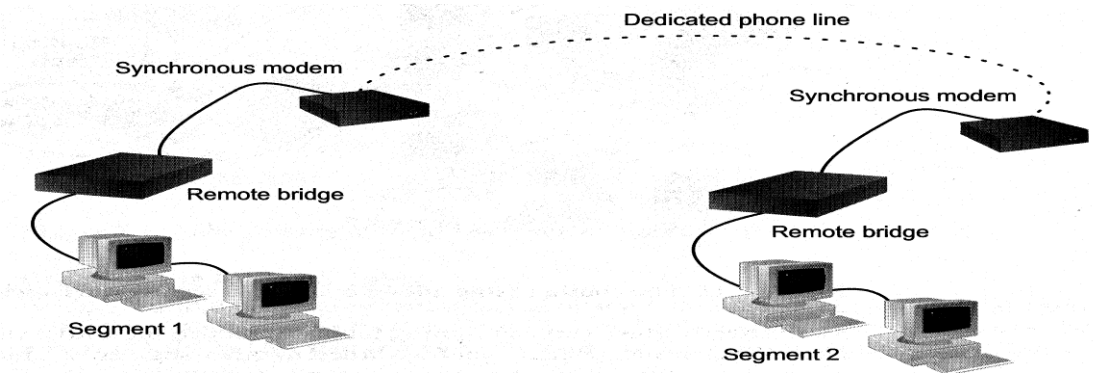
Creating a Switching Table

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



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**

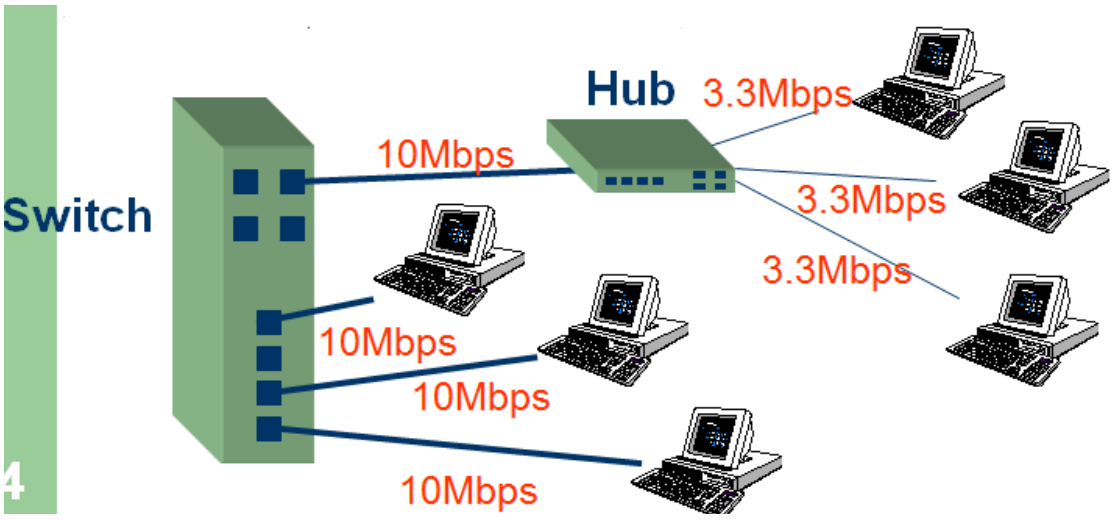


Differences between Bridges and Repeaters

	Repeaters	Bridges
OSI layer	Physical layer	Data link layer
Data regeneration	Regenerate data at the signal level	Regenerate data at the packet level
Reduce network traffic	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
    - 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	2 Bytes	46 - 1500 Bytes	4 Bytes

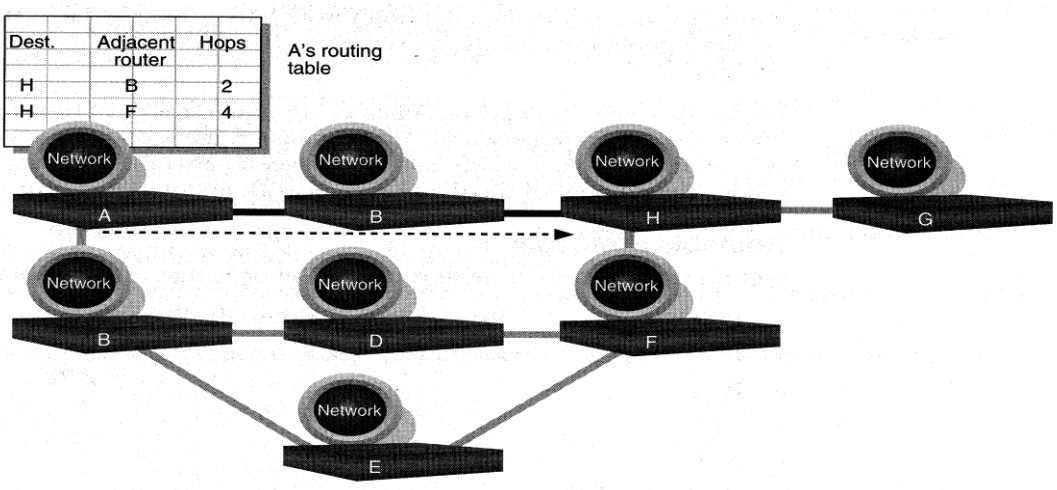
- **Read the first 14 bytes of each packet, then transmit**
- **Much faster**
- **Cannot detect corrupt packets**
- **Can propagate the corrupt packets to the network**
- **Best suited to small workgroups**

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**
- **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**

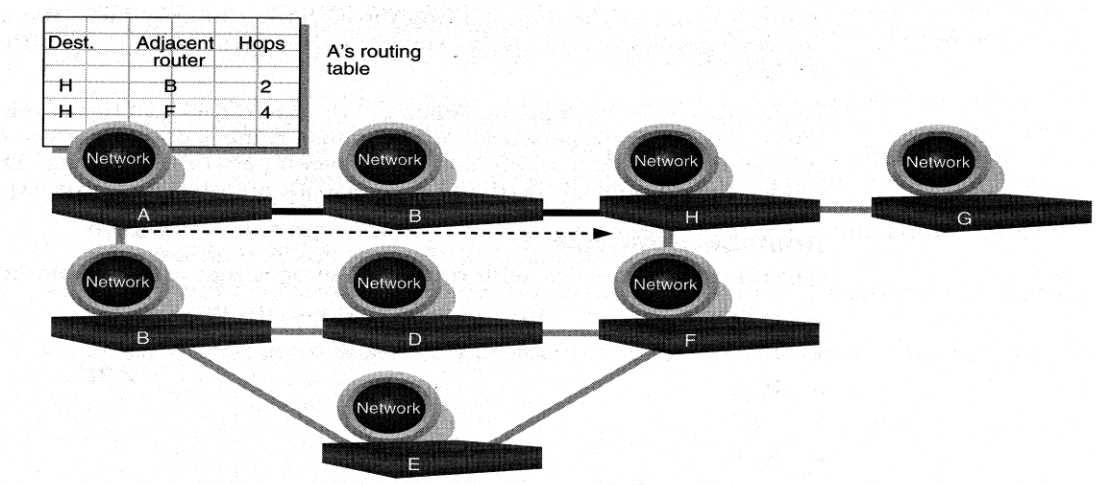


How Routers Work

- 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 ≠ 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

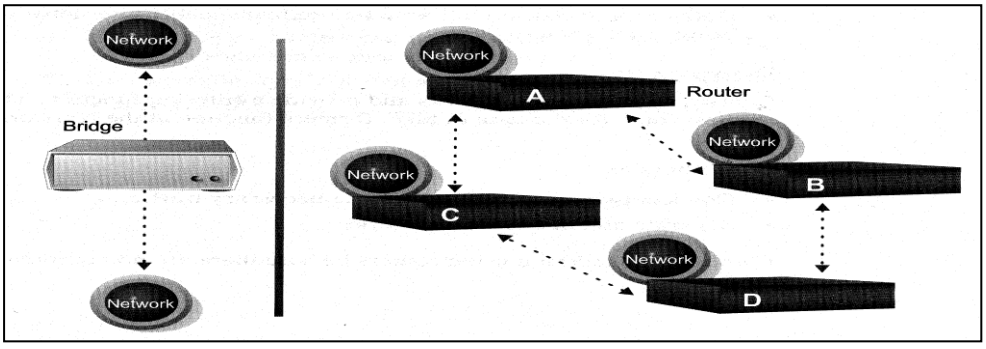
- **OSPF - Open Shortest Path First**
- **Make up the limitations of RIP - can coexist with RIP**
- **In general case, best path refers to the shortest path**
- **In case of traffic congestion, can go a longer path**
- **Each router maintains a database of other router's links**
- **If link failure notice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

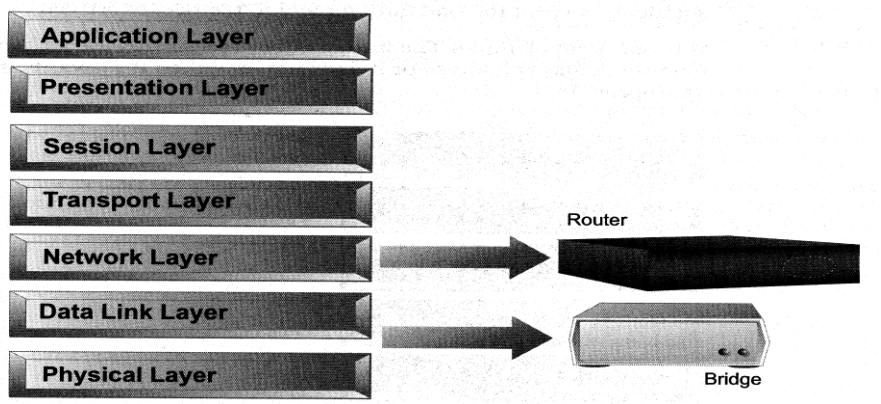
Static and Dynamic Routers

Static Routers	*Dynamic Routers*
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

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**

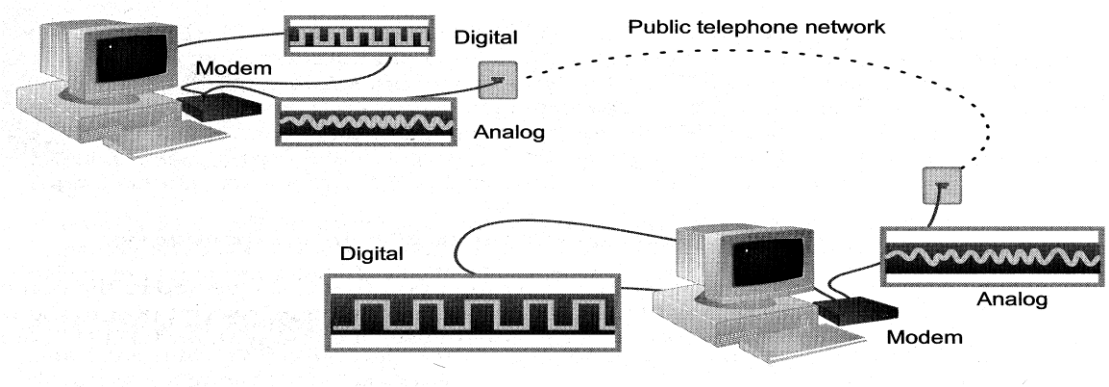
Summary

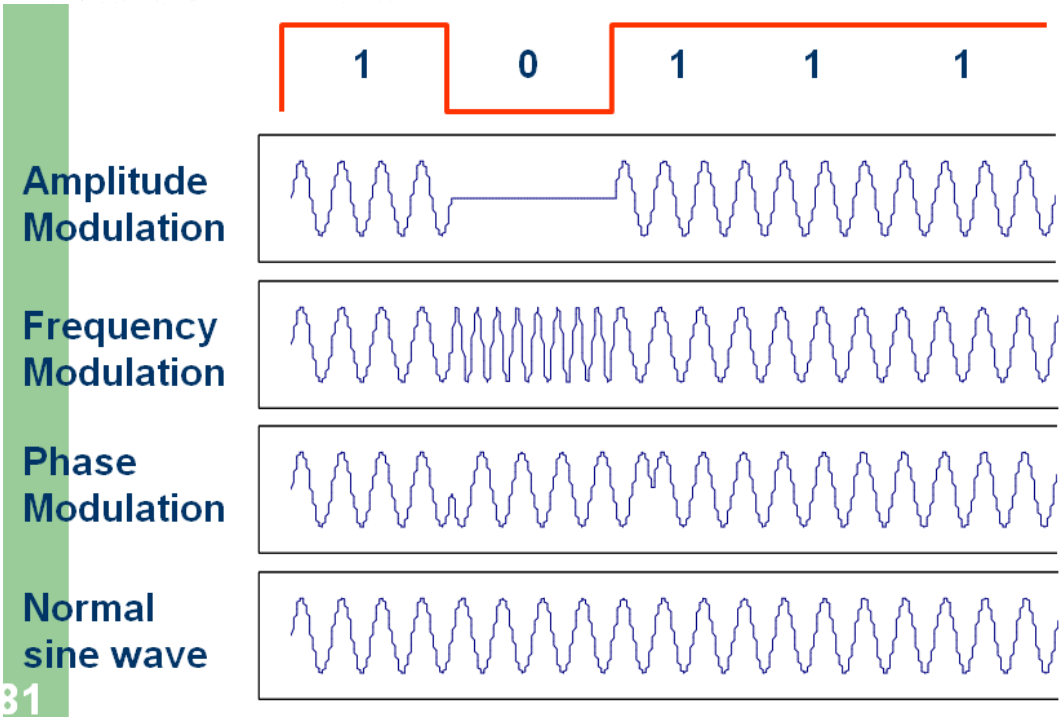
- **Repeaters are the least expensive way to expand a network, but they are limited to connecting two segments**
- **Bridges function similar to repeaters, but can understand the node addresses**
- **Switches can be considered as multiport bridges, can divide a network into some logical channels**
-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

B. Remote Access Devices

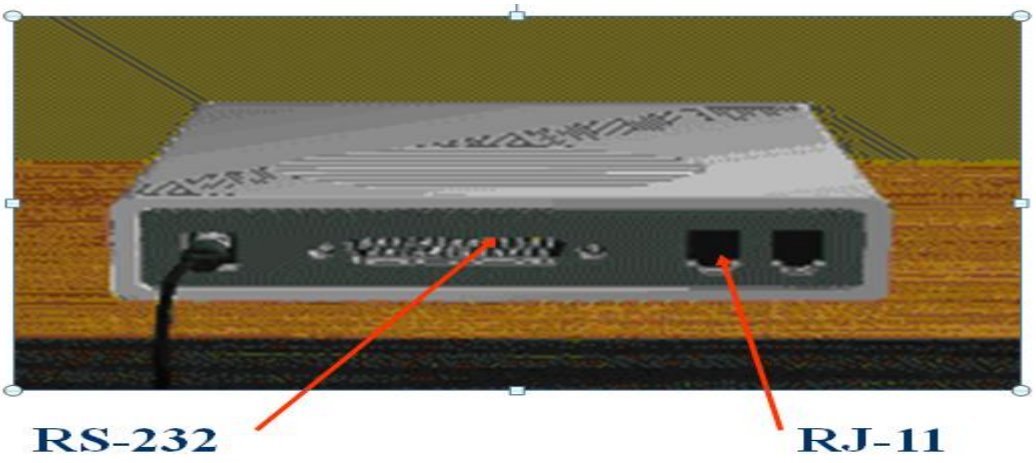
1. Modems

- **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)**



Modem Standards

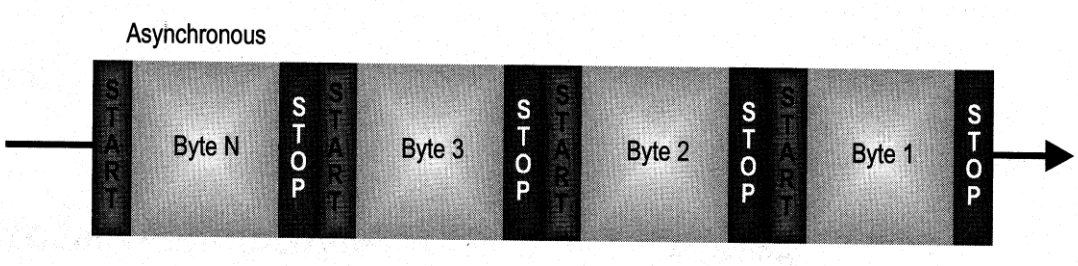
Standard	bps	Introduced	Remarks
V.22bis	2,400	1984	
V.32	9,600	1984	
V.32bis	14,400	1991	
V.32terbo	19,200	1993	Communicate only with another V.32terbo
V.FastClass	28,800	1993	(V.FC)
V.34	28,800	1994	Improved V.FC
V.42bis	115,200	1995	With compression
V.90	56,000	1998	Resolved competition between X2 and Flex56k

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**

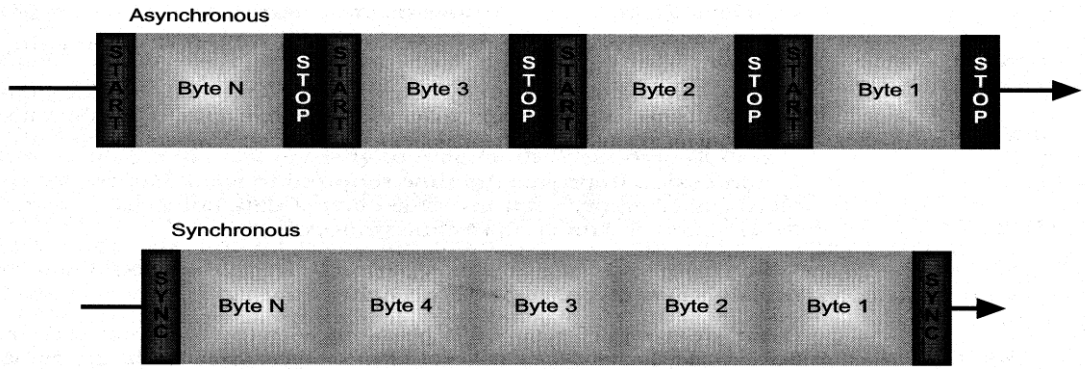
Types of Modem - Asynchronous Modems

- **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**

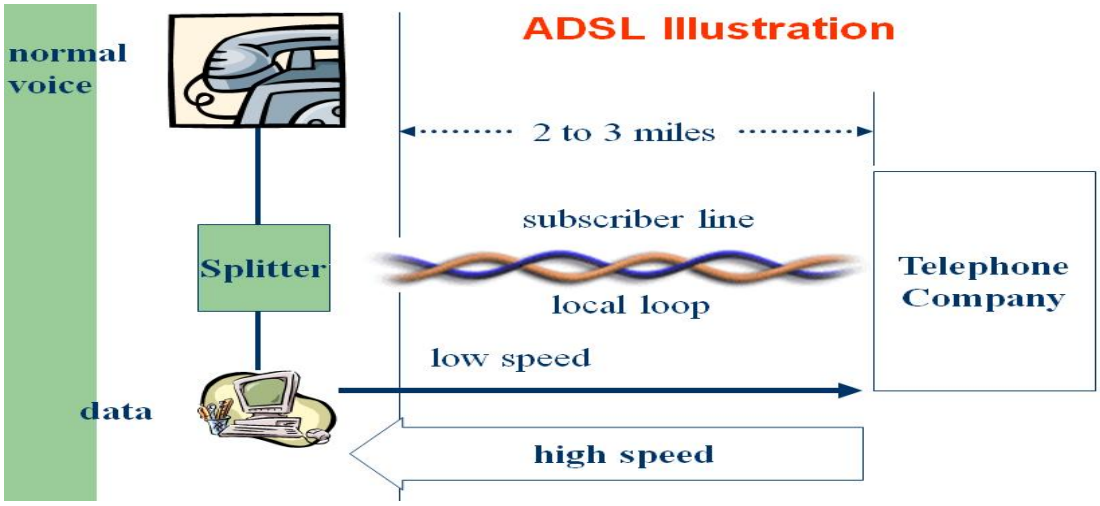


Comparison

- **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?

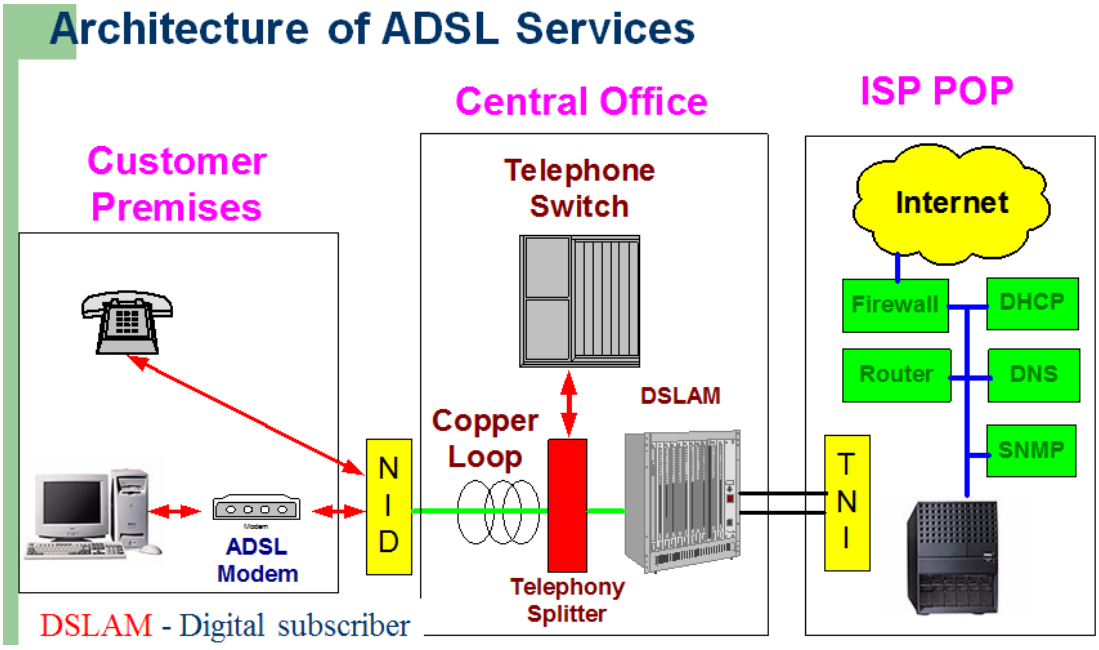
- **In general Internet applications, downstream often requires a higher data rate than upstream**
  - **Downstream - file download, video playback**
  - **Upstream - click a link, send a form**
- **Reducing the resource for upstream can provide more resource for downstream**

Why Subscriber Line?

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

Data Rate	Wire Gauge	Distance	Wire Size	Distance
1.5 or 2 Mbps	24 AWG	18,000 ft	0.5 mm	5.5 km
1.5 or 2 Mbps	26 AWG	15,000 ft	0.4 mm	4.6 km
6.1 Mbps	24 AWG	12,000 ft	0.5 mm	3.7 km
6.1 Mbps	26 AWG	9,000 ft	0.4 mm	2.7 km

- **More than 80% of the current installed subscriber lines can fulfill this requirement**
- **Hence no extra cabling is required**


Architecture of ADSL Services
Central Office
ISP POP
Customer Premises
Telephone Switch
Internet
Firewall
DHCP
Router
DNS
SNMP
DSLAM
Copper Loop
N I D
ADSL Modem
Telephony Splitter
T N I
DSLAM - Digital subscriber

Using Public IP Addresses

Every IP address on the public Internet is unique. To allow networks to obtain unique addresses for the Internet.
The Internet Assigned Numbers Authority (IANA) divides up the nonreserved portion of the IP address space and delegates responsibility for address allocation to a number of regional registries throughout the world. These registries include

1. Asia-Pacific Network Information Center (APNIC),
2. American Registry for Internet Numbers (ARIN),
3. Réseaux IP Européens (RIPE NCC). The regional registries allocate blocks of addresses to a small number of large Internet Service Providers (ISPs) that then assign smaller blocks to customers and smaller ISPs.

Typically, your ISP assigns you one public IP address for each of your computers that is directly connected to the ISP. This IP address can be assigned dynamically to each computer when the computer connects, or it can be reserved statically for your dedicated line or dial-up account.

Using Private IP Addresses

The IANA has reserved a certain number of IP addresses that are never used on the global Internet. These private IP addresses are used for hosts that require IP connectivity but that do not need to be seen on the public network.
For example, a user connecting computers in a home TCP/IP network does not need to assign a public IP address to each host. The user instead can take advantage of the address ranges shown in Table (1) to provide addresses for hosts on the network.

Table (1) Private Address Ranges

Starting Address	Ending Address
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Hosts addressed with a private IP address can connect to the Internet through the use of a proxy server or a computer running Windows Server 2003 configured as a Network Address Translation (NAT) server.

Understanding the Structure of IP Addresses

People usually recognize IP addresses by their distinctive sequence of four numbers separated by dots, such as 192.168.100.22. However, this version of an IP address is really just a transcription—called *dotted-decimal notation* (Octet)

The logic behind IP addressing is revealed when you look at this native binary version of IP addresses. To be able to configure, manage, and troubleshoot IP addressing, therefore, you must be able to understand and work with the binary form of IP addresses, as well as translate between binary and decimal notations.

Converting Between Binary and Decimal Notation

For example, the IP address 192.168.0.225 is expressed in binary notation in the following manner:

11000000 10101000 00000000 11100001 (4 bytes 0r 32 bits length)

For any 32-bit IP address, octets and bit places are numbered from left to right. Consequently, the first octet refers to the leftmost octet, and bit places 1 through 8 refer to the eight leftmost bit places, beginning on the far left. The second octet refers to the next eight bits (bit places 9–16), followed by the third octet (bit places 17–24), and the fourth octet (bit places 25–32). Periods are used to separate the four octets in dotted decimal notation, and spaces are used to separate them in binary notation.
Table (2) shows the scientific and decimal notations associated with each bit place within a binary octet.

Table (2) Potential Values in a Binary Octet

Octet	First Bit	Second Bit	Third Bit	Fourth Bit	Fifth Bit	Sixth Bit	Seventh Bit	Eighth Bit
Scientific notation	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal notation	128	64	32	16	8	4	2	1
Example	1	0	1	0	1	1	0	0

Binary-to-Decimal Conversion :

Example The following binary string shows a possible first octet in an IP address:
10101100

In this eight-digit binary number the first, third, fifth, and sixth bit places contain 1. All other bit places are filled with 0. To understand the decimal value of this binary octet, you can easily draw a conversion table, such as the one shown here, in which to enter the potential bit values of the octet:

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

Using this table as a reference, you can perform simple addition of each bit place's decimal equivalent value to find the decimal sum for this octet string, as follows:

first bit (128) + third bit (32) + fifth bit (8) + sixth bit (4) = octet total (172)

Because the sum is 172, the first octet of the example IP address is expressed as 172 in decimal form.

Next, suppose that the following four octets represent the complete IP address:

10101100 00010001 00000111 00011011
172 . 17 .7 .27

After using this method on the other octets, you can determine that the complete dotted- decimal equivalent of the IP address is 172.17.7.27.

Network ID and Host ID

The routers that direct packets of data between TCP/IP networks do not usually need to know the exact host for which an IP packet is destined (متجهة). Instead, routers need to read from an IP packet only *the destination network address* of which the particular destination host is a member. The routers then use information stored in *their routing tables* to determine how to move the packet toward the network of the destination host. Only after the packet is delivered to the *destination's network segment* is the precise location of the destination host determined.
To assist (ولمساعدة) in this routing process, an IP address is divided into two components:

1. The first part of an IP address, the *network ID*, identifies a particular network within a larger TCP/IP internetwork (such as the Internet).
2. The last part of an IP address, the *host ID*, identifies a TCP/IP host (a workstation, server, router, or other TCP/IP device) specific to the network defined by the network ID.

Figure (1) shows a sample view of an IP address (131.107.16.200) as it is divided into network ID and host ID sections. In this example, the network ID portion (131.107) is

indicated by the first two numbers of the IP address. The host ID portion (16.200) is indicated by the last two numbers of the IP address.

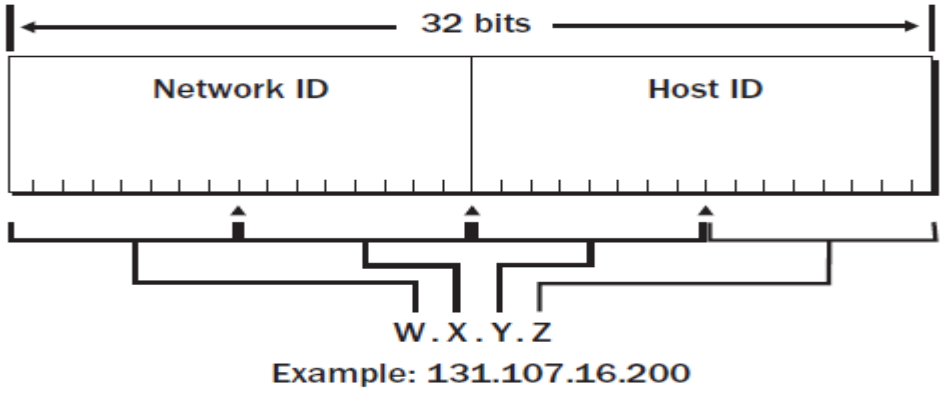


FIgure (1) Network and host IDs

You should follow several general guidelines when assigning network IDs and host IDs:

1. The network ID and host ID bits cannot be all 1s. If all bits are set to 1, the address is interpreted as a broadcast rather than a host ID.
2. The network ID and host ID bits cannot be all 0s. If all bits are set to 0, the address is interpreted to mean "this network only."
3. The host ID must be unique to the local network ID.

IP Address Classes

The *class* of an address, which is determined by the value of the first octet, designates which of its 32 bits represent the default network ID. The address class also defines, for each network ID, how many hosts that network can support. The Internet community has defined five address classes. Only Class A, B, and C addresses are used for assignment to TCP/IP nodes.

Table (3) uses *w.x.y.z* to designate the four octet values in any given IP address. The table is used to show the following:

1. How the value of the first octet (*w*) of any given IP address effectively indicates the class of address
2. How the octets in an address are divided into network ID and host ID
3. The number of possible networks and hosts per network available for each class

Table(3) IP Address Classes

Class	Value of w	Value of First Bits	Network ID	Host ID	Number of Networks within Class	Number of Hosts per Network (Default)
A	1–126	0	w	$x.y.z$	126	16,777,214
B	128–191	10	$w.x$	$y.z$	16,384	65,534
C	192–223	110	$w.x.y$	z	2,097,152	254
D	224–239	1110	Reserved for multi-cast addressing	N/A	N/A	N/A
E	240–254	1111	Reserved for experimental use	N/A	N/A	N/A

Figure (2) illustrates the differences among Class A, B, and C addresses.

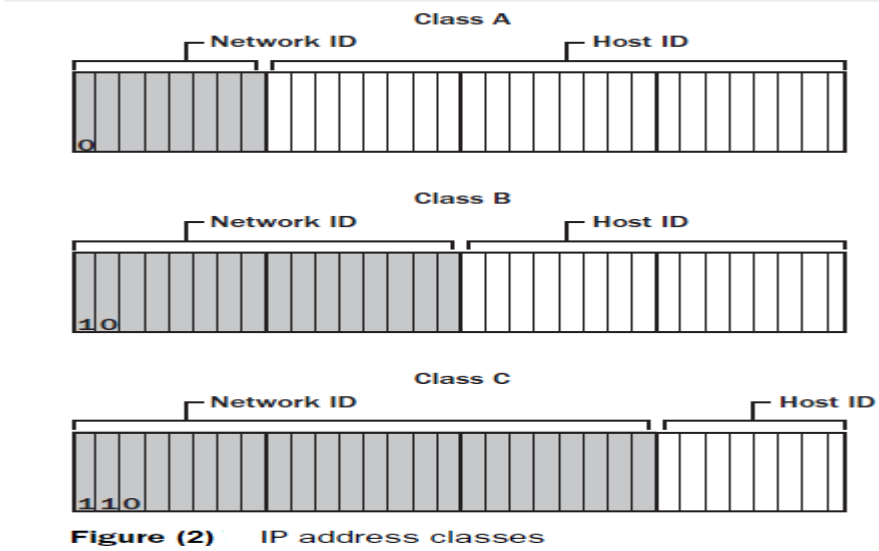


Figure (2) IP address classes

Subnet Masks

Another setting whose proper configuration is required for TCP/IP to function is the *subnet mask*. This value is used by a host to determine whether the destination of a packet is on the local network or on a remote network. Each subnet mask is a 32-bit address that uses a string of 1-bits to block, or *mask*, the network ID of a packet's destination address and to distinguish this network ID from the host ID. Every host on a

TCP/IP network requires a subnet mask—either a default subnet mask, which is used when a network has not been subnetted (and therefore consists of a single subnet), or a custom subnet mask, which is typically used when a network is divided into *multiple subnets*.

For Example, the following 32-bit number represents the default subnet mask used by hosts configured with a Class B address (such as 172.20.16.200):

11111111 11111111 00000000 00000000 (255.255.0.0)

For Example:

If a TCP/IP host with the address 172.20.16.200 sends a packet to the address 172.21.17.201, the host first performs a bitwise AND operation between the local address and the locally configured subnet mask. Because ANDing two numbers results in a figure with 0s in all bit places except those where both original binary numbers have 1-bits, the result of ANDing 172.20.16.200 and 255.255.0.0 is 172.20.0.0. The host then performs a bitwise AND operation between the destination address and this same subnet mask, which results in the binary equivalent of 172.21.0.0. TCP/IP then compares the values resulting from these two bitwise AND operations. If the two values are identical, the TCP/IP host concludes(يستخلص،يستنتج،يقرر) that the destination is on the local subnet. If the two values differ, the host determines that the destination is remote.

Network Prefix Length Representation of Subnet Masks

Because the network ID bits must always be chosen in a contiguous fashion(صيغة اواسلوب التجاور) from the high-order (leftmost) bits, a shorthand way (طريقة الاختزال) of expressing a subnet mask is to denote the number of bits that define the network ID as a *network prefix*. The subnet mask can then be expressed using network prefix notation: *IP address /network prefix*. For example, the IP address 131.107.16.200 and subnet mask 255.255.0.0 can be designated more simply by the notation 131.107.16.200/16. The 16 after the slash represents the number of 1-bits used in this particular subnet mask. Similarly, /24 designates a subnet mask of 255.255.255.0 for a Class C address such as 206.73.118.23/24.

Note Network prefix notation is also known as classless interdomain routing (CIDR; pronounced "cider") notation.

Table 4 displays default subnet masks for the Internet address classes.

Table (4) Subnet Masks

Address Class	Default Subnet Mask in Binary	Network Prefix with Decimal Equivalent
Class A	11111111 00000000 00000000 00000000	/8 = 255.0.0.0
Class B	11111111 11111111 00000000 00000000	/16 = 255.255.0.0
Class C	11111111 11111111 11111111 00000000	/24 = 255.255.255.0

Understanding Default Gateways

If a TCP/IP host needs to communicate with a host on another network, it usually does so through a router. Routers contain multiple interfaces connected to separate networks, and *routing* is the process of receiving IP packets at one interface and

sending these packets out another interface toward a final destination. For a given host on a TCP/IP network, the *default gateway* is the IP address of a router, within broadcast range, that is configured to forward IP traffic to other networks.

When a computer attempts to communicate with another host on an IP network, the computer uses the subnet mask to determine whether the destination host is local or remote. If the destination is a host on the local network segment, the computer simply sends the packet on the local network by means of a broadcast. If, however, the destination is a remote host, the computer forwards the packet to the default gateway defined in its TCP/IP properties. The router specified at the default gateway address is then responsible for forwarding the packet to the correct network.

Exercise 1: Convert Between Dotted-Decimal and Network Prefix Subnet Masks In this practice, you convert nondefault subnet masks from dotted-decimal to network prefix, and from network prefix to dotted-decimal. Note that these values represent nondefault subnet masks, which are explained above of this lecture.

Use Table 4 to help you convert between the two ways of expressing a subnet mask.
1. 255.255.255.192
2. 255.255.252.0
3. /27
4. /21
1. What does the local host use to determine the destination network ID of a particular packet?

a. The IP header
b. The subnet mask
c. The address class

2. A host determines that the destination network ID of a packet is the same as its own network ID. What does the host do with the packet?

a. It broadcasts an ARP request to determine the Media Access Control (MAC) address of the destination host and transmits the packet on the local network.
b. It sends the packet to the server, which broadcasts the packet on the local network.
c. It sends the packet to the default gateway for delivery.

3. Which of the following is the dotted-decimal notation equivalent of the binary address 11001100 00001010 11001000 00000100? To answer the question, first perform notation conversion manually, and then verify your answer.

a. 204.18.200.3
b. 204.34.202.4
c. 204.10.200.4
d. 202.10.200.4

4. Which of the following is the binary equivalent of the dotted-decimal address 207.209.68.100? To answer the question, first perform notation conversion manually, and then verify your answer with Calculator.

a. 11001111 11010001 01000100 01100100
b. 11000111 11010001 01000100 01100100
c. 11001111 11010001 01000100 01101100
d. 11001111 11010001 11001101 01100100

5. Determine the dotted-decimal equivalent of the following address. Use CIDR notation to designate the default subnet mask. perform this notation conversion manually, and..

10010010 01101011 00100111 10001001

Lecture Summary

1. Public IP addresses are the globally unique addresses that are connected to the Internet. Private IP addresses are confined to (تقتصر على) specific ranges and can be used by any private network.
2. An alternate configuration enables an automatically configured computer to use a manually specified IP address configuration instead of APIPA in the absence of a DHCP server.
3. In TCP/IP, the default gateway is the router that connects the host's subnet to other networks.
4. The subnet mask of the local host is used to compare the network ID of the local host to the network ID of every IP packet it sends on the network. If the network ID of the host matches the destination network ID of the IP packet, the packet is transmitted on the local network. If the destination network ID of the packet is different from that of the host, the packet is sent to the local default gateway.
5. The address class of an IP address determines its default subnet mask.

Subnetting and Supernetting IP Networks

By manipulating subnet masks, you can customize address space to suit your network needs. Using subnetting, you can subdivide networks into distinct and separate groups. Using supernetting and CIDR, you can combine separate networks into a single address space.

عن طريق التلاعب باقنعة الشبكة الفرعية، يمكنك تخصيص مساحة العنوان لتتناسب مع احتياجات شبكتك.حيث يمكنك تقسيم الشبكات إلى مجموعات لها ميزتها وخصاصها وتكون متميزة ومنفصلة

Notes

Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and routing Internet Protocol packets. The Internet Engineering Task Force introduced CIDR in 1993 to replace the previous addressing architecture of classful network design in the Internet. Its goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses.[1][2]

IP addresses are described as consisting of two groups of bits in the address: the most significant bits are the *network address*, which identifies a whole network or subnet, and the least significant set forms the *host identifier*, which specifies a particular interface of a host on that network. This division is used as the basis of traffic routing between IP networks and for address allocation policies. Classful network design for IPv4 sized the network address as one or more 8-bit groups, resulting in the blocks of Class A, B, or C addresses. Classless Inter-Domain Routing allocates address space to Internet service providers and end users on any address bitboundary, instead of on 8-bit segments. In IPv6, however, the interface identifier has a fixed size of 64 bits by convention, and smaller subnets are never allocated to end users.

Subnetting and Supernetting IP Networks

By manipulating subnet masks, you can customize address space to suit your network needs. Using subnetting, you can subdivide networks into distinct and separate groups. Using supernetting and CIDR, you can combine separate networks into a single address space.

After this Lecture, you will be able to:

1. Manipulate subnet masks to configure subnets for a variety of network restrictions and needs
2. Given any network address and subnet mask, determine the number of subnets and hosts available
3. Determine the range of IP addresses for each subnet implied by a given network address and subnet mask
4. Manipulate subnet masks to configure a supernetted address space
5. Configure variable-length subnet masks to meet network requirements for subnets of varying sizes

Understanding Subnetting

Subnet masks are used by hosts to determine which portion of an IP address is considered the network ID of that address. Class A, B, and C addresses use default subnet masks that cover the first 8, 16, and 24 bits, respectively, of a 32-bit address.

The logical network that is defined by a subnet mask is known as a *subnet*.

Default subnet mask values are acceptable for networks that do not need to be subdivided. For example, on a network with 100 computers connected only through Gigabit Ethernet cards, cables, and switches, all hosts can communicate with each other by using the local network. Routers are not needed within the network to shield excessive broadcasts or to connect hosts on separate physical segments. For such simple requirements, a single Class C network ID is sufficient. Figure 2-6 illustrates a single-subnet network such as this.

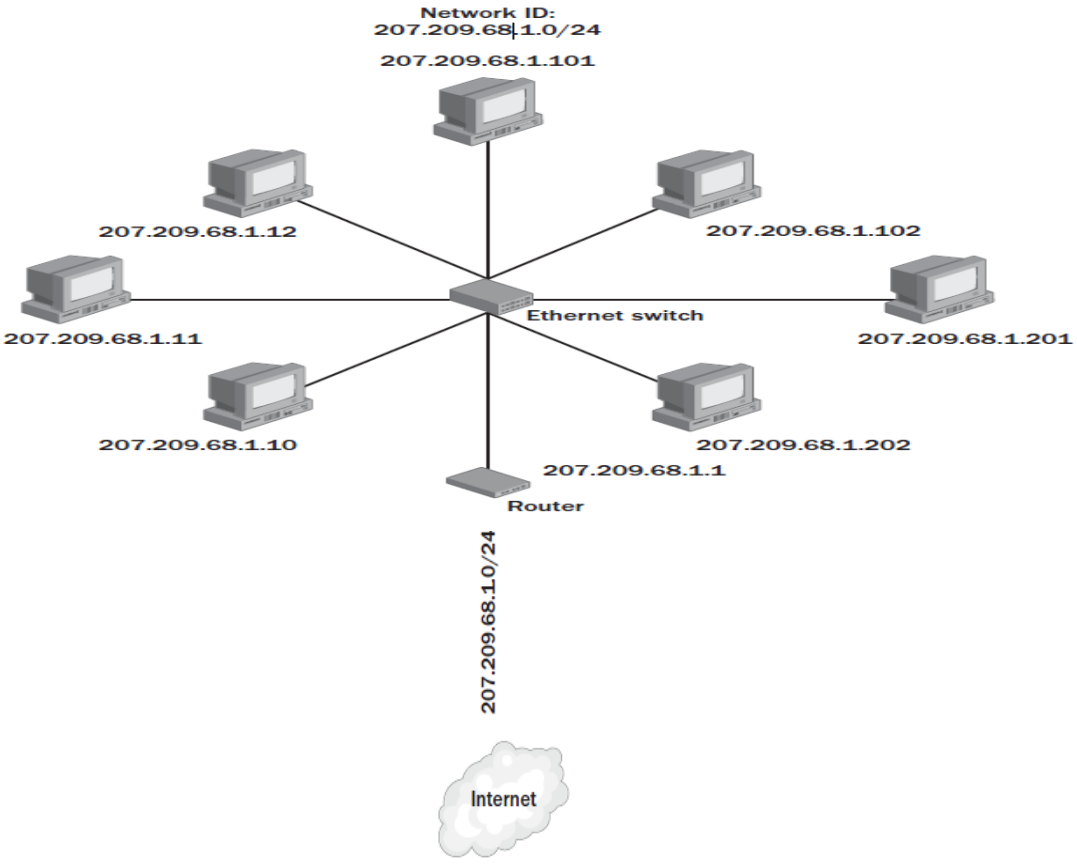


Figure (5) Single-subnet network

What Is Subnetting?

Subnetting refers to the practice of logically subdividing a network address space by extending (تمديد،توسيع) the string of 1-bits used in the subnet mask of a network. This extension enables you to create multiple subnets within the original network address space.

For example, when the default subnet mask of 255.255.0.0 is used for hosts within the Class B network of 131.107.0.0, the IP addresses 131.107.1.11 and 131.107.2.11 are found on the same subnet, and these hosts communicate with each other by means of a broadcast. However, when the subnet mask is extended to 255.255.255.0, the addresses 131.107.1.11 and 131.107.2.11 are found on different subnets. To communicate with each other, hosts with addresses 131.107.1.11/24 and 131.107.2.11/24 send IP packets to the default gateway, which is then responsible for routing the datagram toward the destination subnet. Hosts external to the network continue to use the default subnet mask to communicate with hosts within the network. Figure (7) and Figure (8) illustrate the two versions of this network.

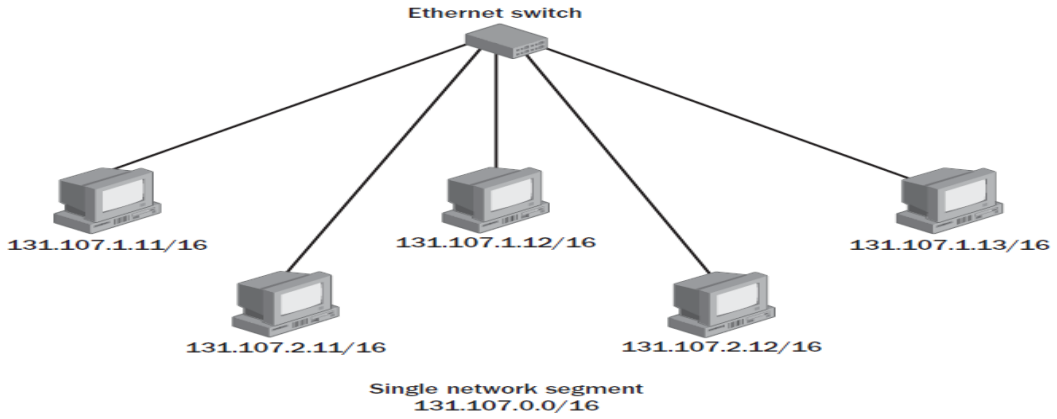


Figure (7) Class B address space not subnetted

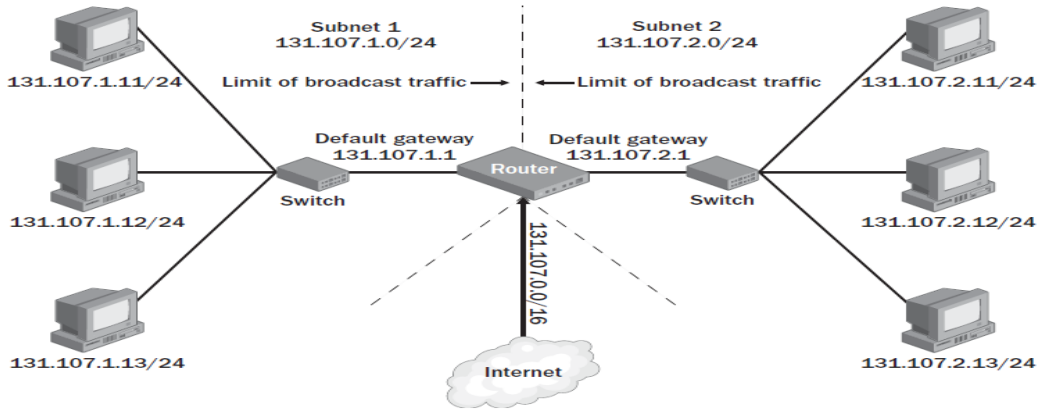


Figure (8) Subnetted Class B address space

Whereas the original Class B network address space in Figure (7) consisted of a single subnet of up to 65,534 hosts, the new subnet mask configured in Figure (8) allows you to subdivide this original space into 256 subnets with as many as 254 hosts each.

Accommodating Physical Topology (استيعاب(ملائمة) التبولوجيا المادية)

Suppose you are designing a campus network with 200 hosts spread over four buildings—Voter Hall, Twilight Hall, Monroe Hall, and Sunderland Hall. You want each of these four buildings to include 50 hosts. If your ISP has allocated to you the Class C network 208.147.66.0, you can use the addresses 208.147.66.1–208.147.66.254 for your 200 hosts. However, because these hosts are distributed among four physically separate locations, these hosts are not all able to communicate with each other by means of a local network broadcast. By extending the subnet mask and borrowing 2 bits from the host ID portion of your address space, you can divide the network into four logical subnets. You can then use a router to connect the four physical networks. Figure (9) illustrates this scenario.

من خلال توسيع قناع الشبكة الفرعية (subnet mask) والاقتراض ٢ بت من جزء معرف المضيف (the host ID portion) من مساحة العنوان وبذلك يمكنك تقسيم الشبكة إلى أربع شبكات فرعية منطقية. يمكنك بعد ذلك استخدام جهاز التوجيه (router) لربط شبكات أربع المادية كما موضح في الشكل (٩).

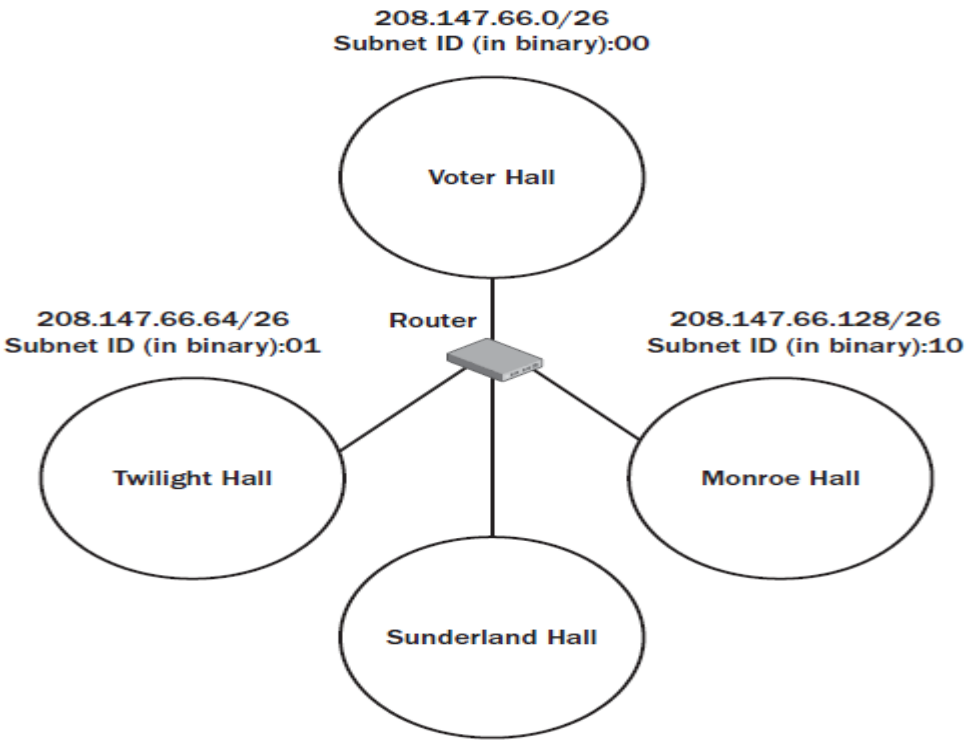


Figure (9) Subnetting in a divided physical topology

Determining Host Capacity for Networks

For any specific network address, you can determine the quantity of host addresses available within that network by raising 2 to the power of the number of bits in the host ID, and then subtracting 2. For instance, the network address 192.168.0.0/24 reserves 8 bits for the host ID. Therefore, you can determine the number of hosts by calculating $2^8 - 2$, which equals 254.

Determining Subnet Capacity

When the string of 1-bits in the subnet mask is extended beyond its default to create multiple subnets within any address space, the host ID is shortened (تقصر), and a new address space for the subnet IDs is created, as shown in Figure (10) and Figure (11).

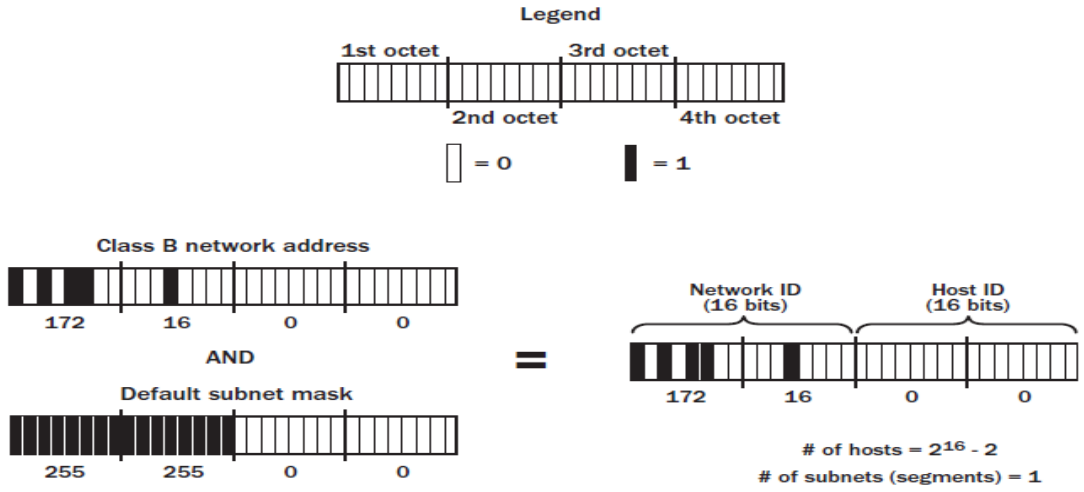


Figure (10) Default Class B address space

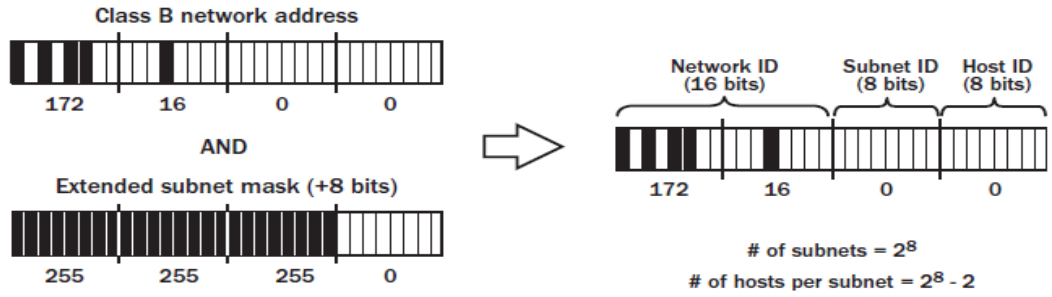


Figure (11) Address space with subnet ID

To determine the number of subnets available within an address space, simply calculate the value of 2^y, where y equals the number of bits in the subnet ID. For example, when the networks address space 172.16.0.0/16 is subnetted to /24, 8 bits

are reserved for the subnet ID. Therefore, the number of available subnets is 2^8, or 256

Hosts per Subnet

Calculating the number of host IDs per subnet is the same as calculating the number of host IDs per network. When your network address space has been subnetted, the value $2^x - 2$ (where *x* equals the number of bits in the host ID) yields the number of hosts per subnet. For example, because the address space 172.16.0.0/24 reserves 8 bits for the host ID, the number of available hosts per subnet is equal to $2^8 - 2$, or 254. To calculate the number of hosts available for your entire subnetted network, simply multiply this figure by the number of available subnets. In this example, the address space 172.16.0.0/24 yields 254 × 256, or 65,024 total hosts.

Note

When you are configuring a network address space and subnet mask to suit your network needs, be sure to assign a number of bits to the host ID that will accommodate both the number of hosts you now use per subnet and plan to use per subnet in the future.

Tip (نصيحة)

Using Calculator, you can quickly determine the number of bits you need to assign to the host ID. Simply add 1 to the number of hosts you need to accommodate per subnet, enter this number in decimal format, convert to binary, and count the bit places. For example, if you need to accommodate 33 hosts per subnet, enter 34 in Calculator, and then select Bin. The result is 100010, which means that to accommodate your network needs, you must reserve 6 bits for the host ID.

Subnet Examples

In the preceding example, the original address space 172.16.0.0/16 was subnetted by extending the string of 1-bits within the subnet mask a full octet to 255.255.255.0. In practice, the string of 1-bits within subnet masks can be extended any number of bits, not just full octets.

For example, Figure (12) shows the address space for 10.0.0.0/12. Because this address is a Class A address, the default number of 1-bits in the subnet mask is 8; the mask has been extended 4 bits. Thus, 4 bits remain for the subnet ID and 20 bits remain for the host ID. On such a network, the range of addresses on the first subnet (ID 000) is 10.0.0.1–10.15.255.254.

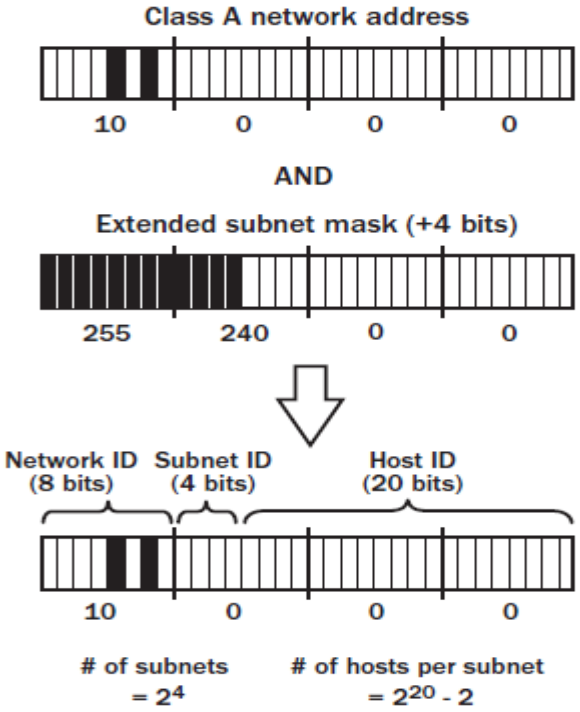


Figure (12) Subnetted Class A address space

In Figure (13), a Class B address of 172.20.0.0 has been given a custom subnet mask of 255.255.248.0, which extends the default subnet mask by 5 bits. On such a network, the range of addresses on the first subnet (ID 00000) is 172.20.0.1–172.20.7.254.

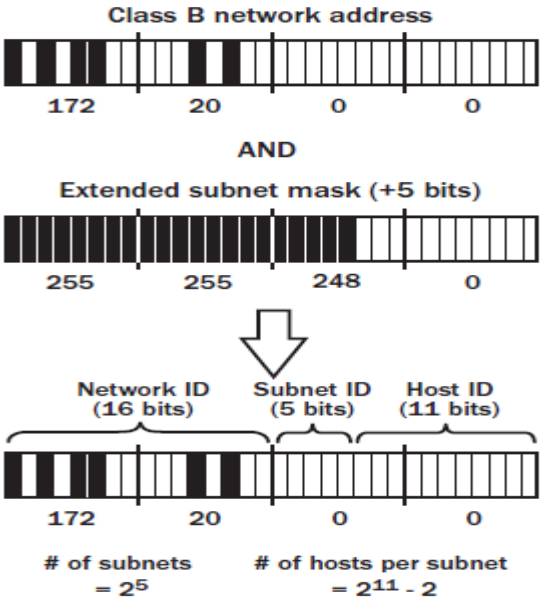


Figure (13) Subnetted Class B address space

Figure (14) shows a Class C address of 192.168.0.0/26. In this example, 2 bits have been reserved for the subnet ID and 6 have been reserved for the host ID. On such a

network, the range of addresses on the first subnet (ID 00) is 192.168.0.1–192.168.0.62.

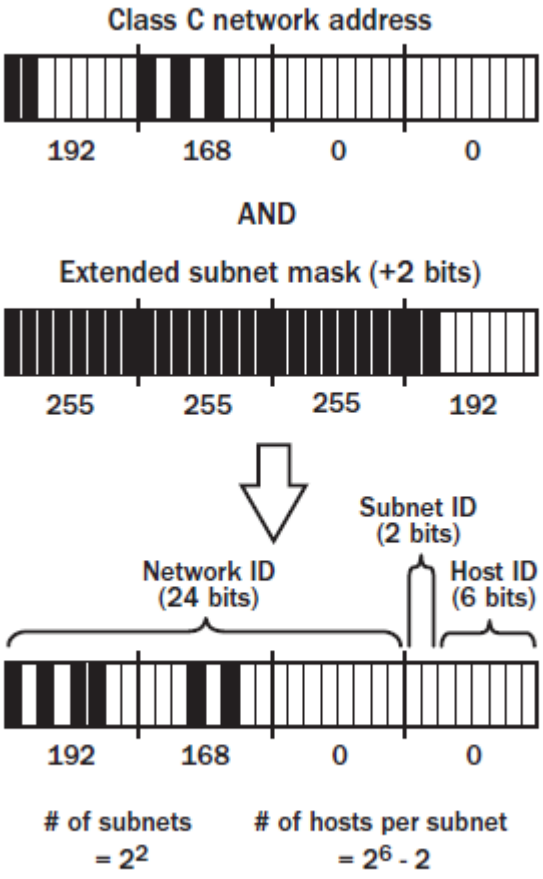


Figure (14) Subnetted Class C address space

Estimating Subnet Address Ranges

By using the dotted-decimal form of the subnet mask, you can estimate the ranges of IP addresses in each subnet simply by subtracting from 256 the value of the relevant octet (ذات الصلة،المعنية) in the subnet mask. For example, for a Class C network such as 207.209.68.0 with a subnet mask of 255.255.255.192, subtracting 192 from 256 results in the value 64. As a result, the network's subnet address ranges are grouped in 64: 207.209.68.0– 207.209.68.63, 207.209.68.64–207.209.68.127, etc. For a Class B network such as 131.107.0.0 with a subnet mask of 255.255.240.0, subtracting 240 from 256 yields 16.

Therefore, the subnet address ranges reveal groupings of 16 in the third and relevant octet (ذات الصلة،المعنية), whereas the fourth octet ranges from 0–255: 131.107.0.0–131.107.15.255, 131.107.16.0–131.107.31.255, and so on.

Remember that hosts cannot be assigned an all-1s or all-0s host ID, so the first and last address of every subnet range cannot be assigned to hosts.

Summarizing Routes through Supernetting

To prevent the depletion (نفاد) of higher-class network IDs, the Internet authorities devised a scheme called ***supernetting,*** which allows many networks (routes) to be grouped together (or summarized) in a single larger network. **Supernetting** offers the advantage of more efficient allocation of network address space. For example, suppose an organization needs to accommodate 2000 hosts. This number is too large for a single Class C network ID, which can accommodate only 254 hosts.

Although a Class B network can accommodate as many as 65,534 hosts, only 16,383 Class B network IDs exist, and the number of unused Class B networks is rapidly decreasing. It therefore does not make sense for an ISP to assign a valuable Class B network (if the ISP even has one to assign) to an organization that plans to use only 3 percent of that space. By using **supernetting**, an ISP can assign an organization a block of Class C addresses that can be treated as a single network somewhere between a Class C and a Class B address. In this example, a block of 8 Class C network IDs could meet the organization's needs by accommodating 2032 hosts.

How Supernetting Works

Supernetting differs from subnetting in that supernetting borrows bits from the network ID and masks them as the host ID. For example, suppose your ISP has assigned you a block of 8 network addresses ranging from 207.46.168.0 through 207.46.175.0.

Assigning a /21 subnet mask (instead of the default /24) to routers at your ISP and to all hosts within your organization results in all your networks being seen as a single network because, thanks to the shortened network ID stemming (النابعة) from the /21 subnet mask, the network ID portion of each of these 8 addresses is now seen as identical. Figure (15) illustrates this scenario.

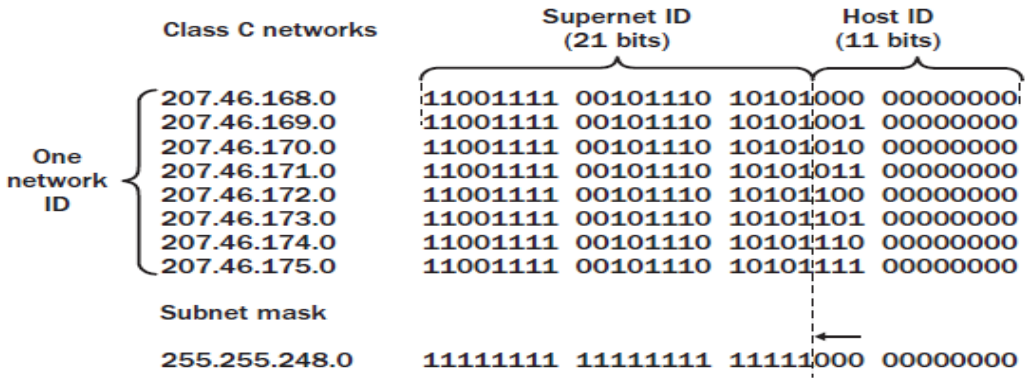


Figure (15) Supernetted block of Class C addresses

What is the difference between classless and classful ip address? Explain and give an example, to differentiate them.

الجواب : كما نعلم أن الـ IP Classes تملك خمس مستويات(تصنيفات) وهي A,B,C,D,E وهو مايعترف فيه الـ Classful ومايتجاهله الـ Classless وهو الفرق الأول بين الاثنان أما الفرق الثاني فهو مع الـ Routing Protocol فالـ Classful لايقوم بأرسال الماسك مع التحديثات إلى روترات آخرى ويكتفي بأرسال الـ IP فقط للتعريف بالشبكات التى يرتبط معها بينما يقوم الـ Classless بأرسال الماسك وحقيقة هذه النقطة لاتحتاج إلى توضيح فهي مستنتجة من وحي النقطة الأولى لأن الـ Classful لايحتاج إلى أرسال الماسك كون العملية لديه معترف عليها بقواعد ثابتة تدعى الـ IP Classes فكل أيبي يصله يستطيع أن يحدد الماسك الخاص به مجرد النظر إليه لأن لكل Class من الأيبيات لها rang معين ولها ماسك ثابت وبالتالي هو لايحتاج إلى ارسال الماسك أما الـ Classlessفهو يحتاج إلى أرسال الماسك لأنه ببساطة تخلى عن لعبة الـ Classes of IP وبدأ يلعب على قواعده من خلال الـ VLSM(Variable-Length Subnet Masks) أما القاعدة الثالثة والتى تحتاج إلى تركيز بسيط تقول لو في حال كان لدينا Default Route في الـ Routing Table مع بعض المعطيات الآخرى لشبكات ترتبط مع الروتر وصدف وصول باكيت إلى هذا الروتر ووجهتها لاتنتمي إلى أحد هذه الشبكات فمصيره هو الـ Drop وبغض النظر عن وجود Default Route أما مع الـ Classless فالأمر مختلف فالباكيت لن تسقط بل سوف تتابع طريقها أعتمادا على الـ Default Route الموجود وهذا الجدول لتوضيح النقاط جميعها بشكل مختصر وسريع.

Classful	Classless
يعتمد على قاعدة الـ IP Classes في توزيع الأيبيات	يتجاهل هذه القاعدة ويتم توزيع الأيبيات بشكل حر وأعتمادا على تقنية الـ VLSM
لايرسل الـ Subnet Mask مع التحديثات الخاصة به على الشبكة لان الماسك ثابت ومعروف عند كل الروترات	يرسل الـ Subnet Mask مع كل الأيبيات المرسلة إلى روترات آخرى لأنه متغير وبحسب الطلب.
يتم عمل Drop للباكيت لو في حال لم يتم تطابقها مع أحد معطيات الـ Routing Table	يتم أرسال الباكيت إلى الـ Default Route لو في حال لم يتم تطابقها مع أحد الشبكات الموجودة في الجدول

What is the difference between classless and classful ip address?

Classful Ip address:

Classful Ip address is take only the pre-defined bits in Network ID (8,16,24) in addressing. Example. Class A pre-defined bits - 8 10.2.1.10 /8, Class B Pre-defined bits - 16 172.16.1.20 / 16, Class C Pre-defined Bits -24 192.168.1.30 /24 This type of address is called Classful Ip address.

Classless Ip

Classless Ip address is assign any number of bits in network ID is called Classless IP

address. Example 10.2.1.10 /12. Bits barrow from Host Id added in to Network id. This called Classless Ip address.

Classfull IP Address:

the Default mask of Classes are called Classful ,Example:
Class A= 255.0.0.0 , Classs B: 255.255.0.0 Class C= 255.255.255.0

Classless IP 19ddress:

Defined by System Administrator. It means used From IP Sub netting

Example: Class A: IP 10.0.0.0 /9 => sub net = 255.128.0.0
Class B: Ip 172.0.0.0 /18 => Sub net => 255.255.192.0
Class C: IP 192.0.0.0/ 27 =>sub net => 255.255.255.224
The difference between classful IP addressing and classless IP addressing is in selecting the number of bits used for the network ID portion of an IP address. In classful IP addressing, the network ID portion can take only the predefined number of bits 8, 16, or 24. In classless addressing, any number of bits can be assigned to the network ID.

Classless have a subnet mask. Classful are simple A-E networks and the mask implied(ضمنية).

==========

3. 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

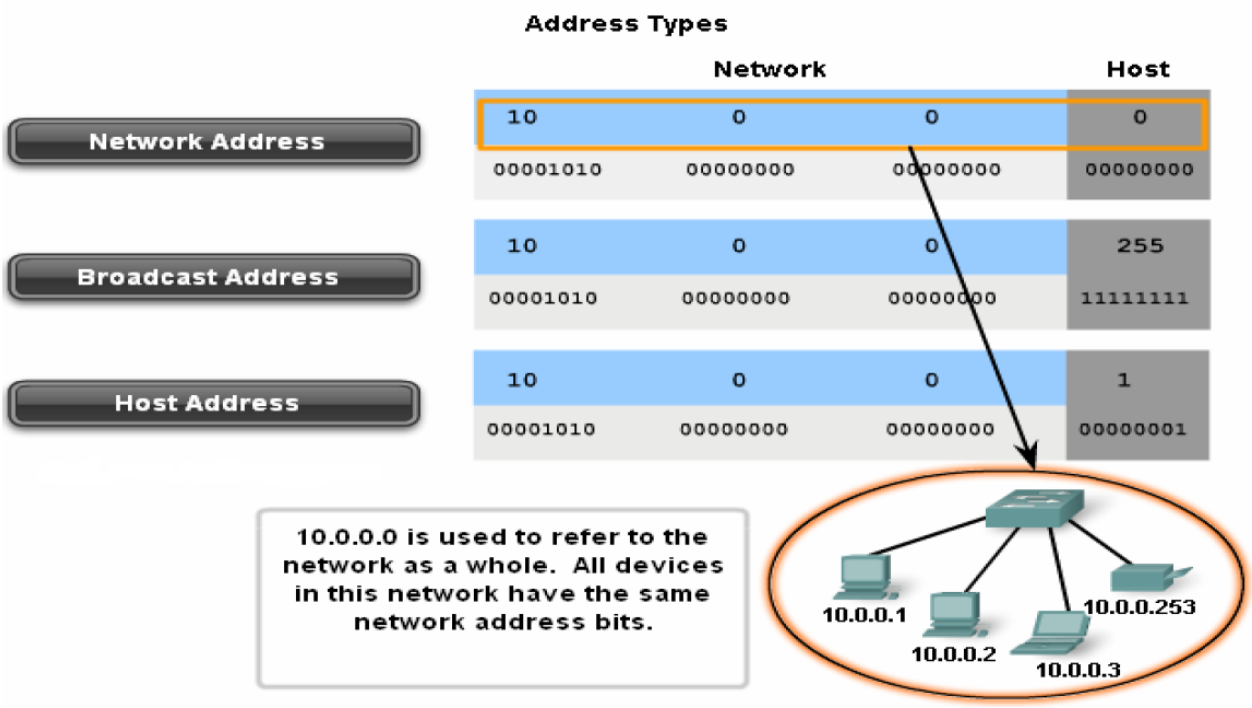
Broadcast address - A special address used to send data to all hosts in the network

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 **10.0.0.0** 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 **10.0.0.0** network will have the same network bits.

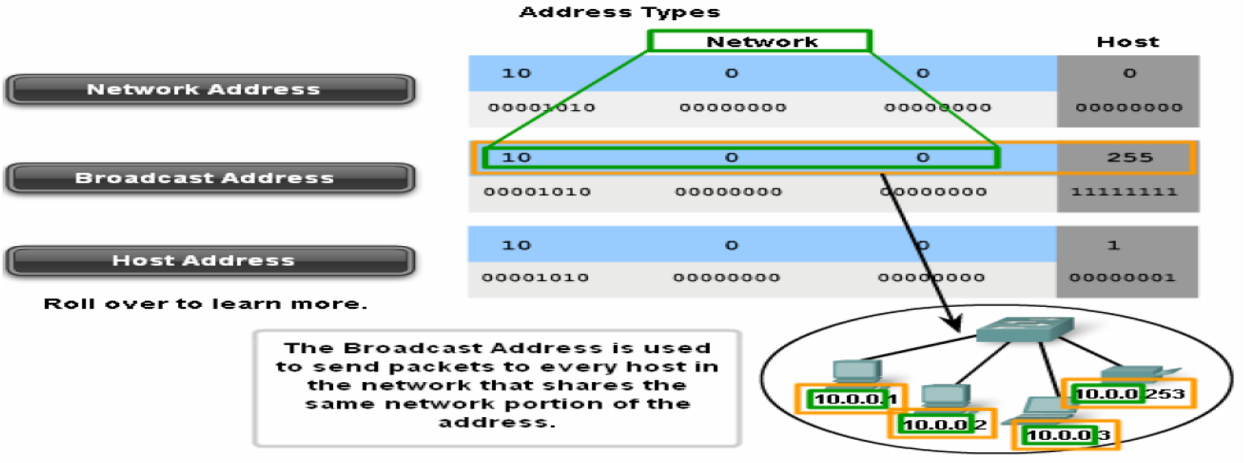
Within the IPv4 address range of a network, the lowest address is reserved for the network address. This address has a 0 for each host bit in the host portion of the address.



3.1.2 Broadcast Address

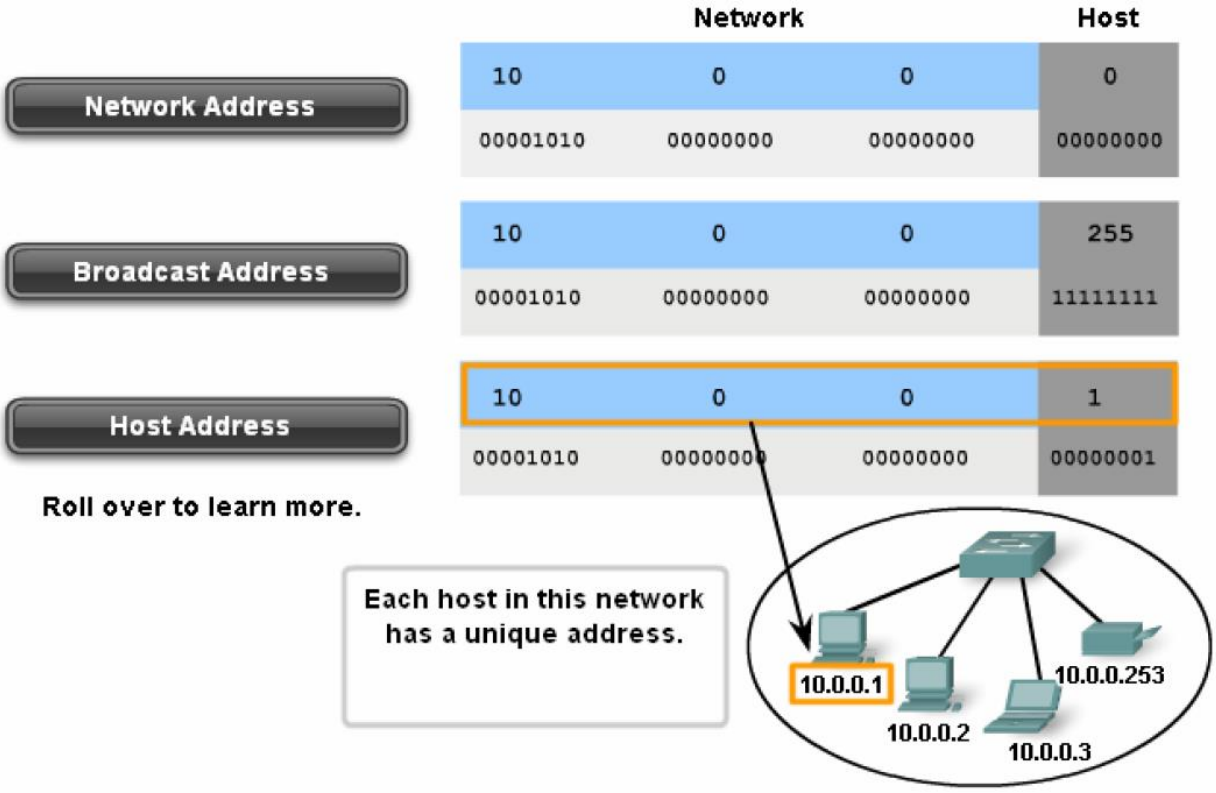
The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

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.



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.

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.

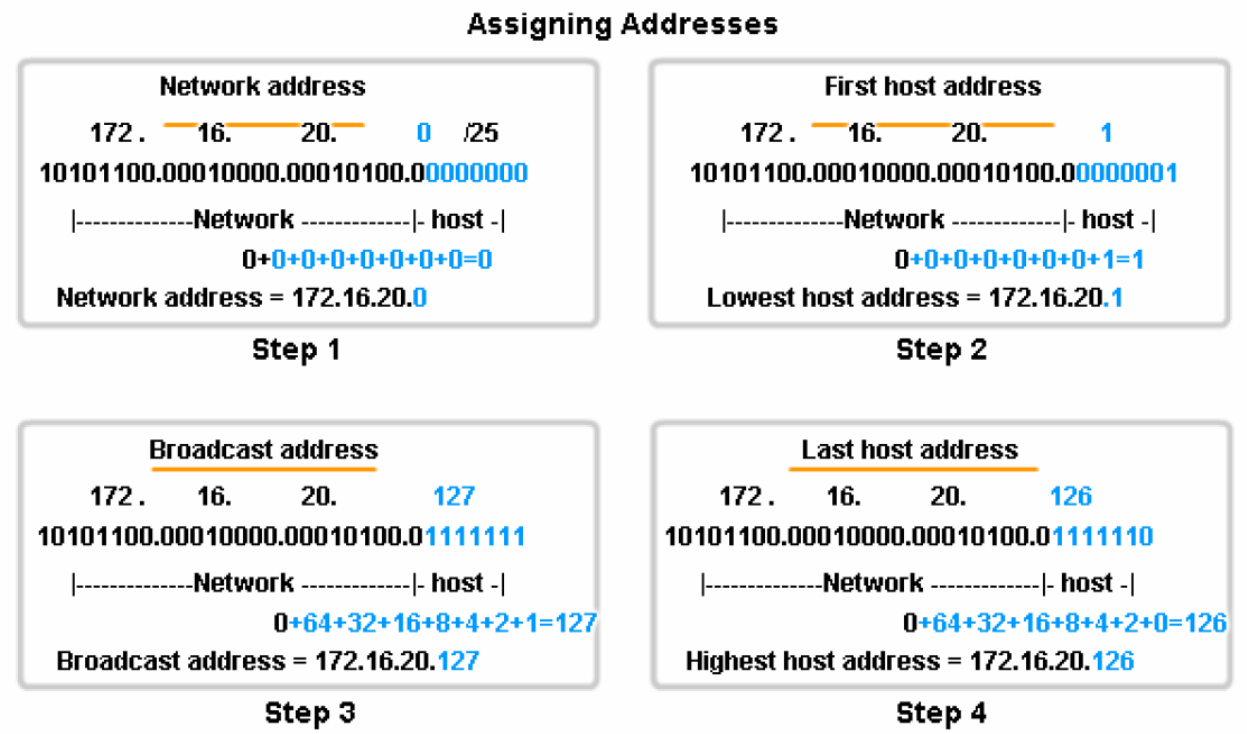
In the second box, we see the calculation of the lowest host address. This is always one greater than the network address. In this case, the last of the seven host bits becomes a '1'. With the lowest bit of host address set to a 1, the lowest host address is 172.16.20.1.

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.



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

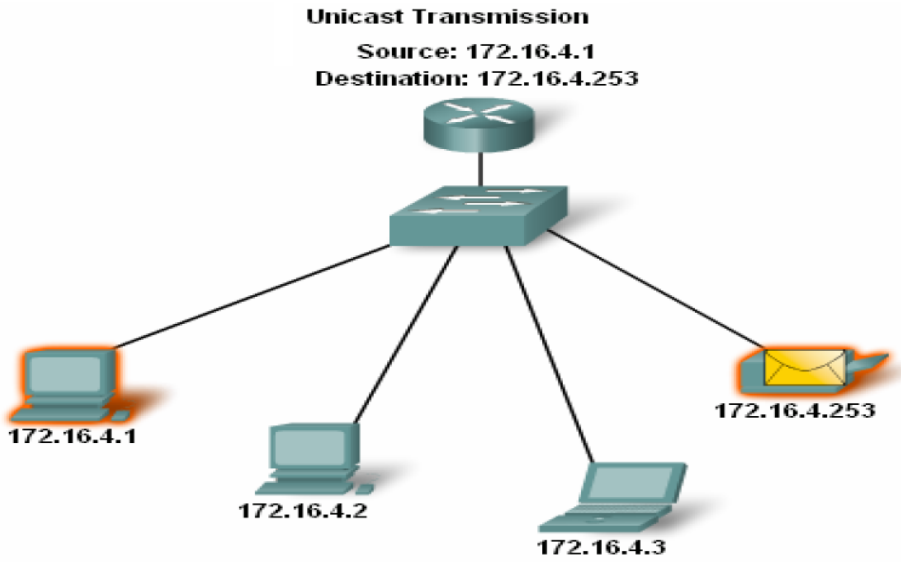
Broadcast - the process of sending a packet from one host to all hosts in the network

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 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

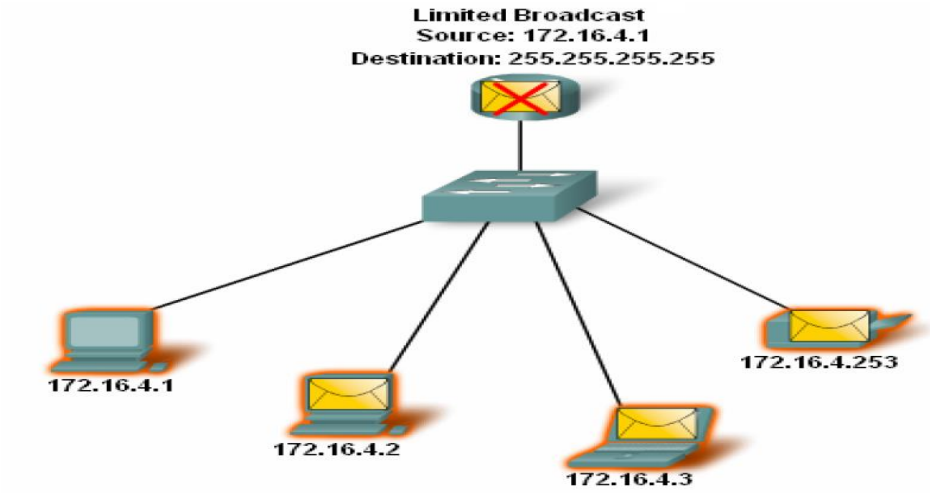
A directed broadcast is sent to all hosts on a specific network. This type of broadcast is useful for sending a broadcast to all hosts on a non-local network. For example, for a host outside of the network to communicate with the hosts within the **172.16.4.0 /24** network, the destination address of the packet would be 172.16.4.255. This is shown in the figure. Although routers do not forward directed broadcasts by default, they may be configured to do so.

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**. Routers do not forward this broadcast. Packets addressed to the limited broadcast address will only appear on the local network. For this reason, an IPv4 network is also referred to as a broadcast domain. Routers form the boundary for a broadcast domain.

As an example, a host within the **172.16.4.0 /24** network would broadcast to all the hosts in its network using a packet with a destination address of **255.255.255.255**.

Play the animation to see an example of broadcast transmission.



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. To reach multiple destination hosts using unicast communication, a source host would need to send an individual packet addressed to each host. With multicast, the source host can send a single packet that can reach thousands of destination hosts.

Some examples of multicast transmission are:

- Video and audio broadcasts
- Routing information exchange by routing protocols

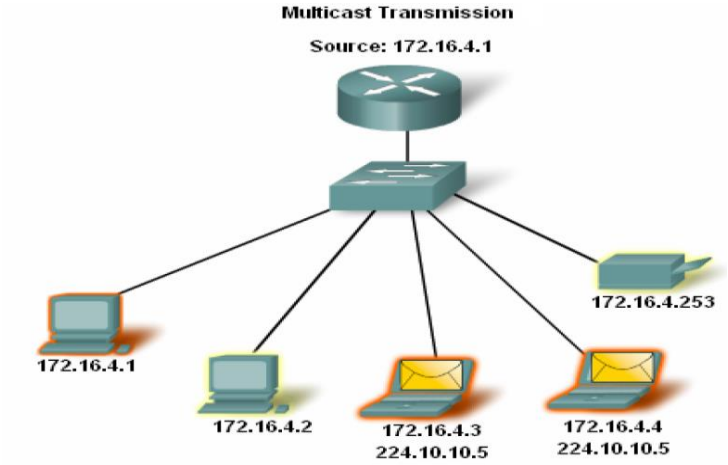
- Distribution of software
- News feeds

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.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address as well as packets addressed to its uniquely allocated unicast address. As we will see, IPv4 has set aside a special block of addresses from 224.0.0.0 to 239.255.255.255 for multicast groups addressing.

The animation demonstrates clients accepting multicast packets.



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.

The IPv4 multicast addresses **224.0.0.0** to **224.0.0.255** are reserved link local addresses. These addresses are to be used for multicast groups on a local network. Packets to these destinations are always transmitted with a time-to-live (TTL) value of 1. Therefore, a router connected to the local network should never forward them. A typical use of reserved link-local addresses is in routing protocols using multicast transmission to exchange routing information.

The globally scoped addresses are **224.0.1.0** to **238.255.255.255**. They may be used to multicast data across the Internet. For example, 224.0.1.1 has been reserved for Network Time Protocol (NTP) to synchronize the time-of-day clocks of network 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.

Reserved IPv4 Address Ranges

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	• 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.

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.

Many hosts in different networks may use the same private space addresses. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses. Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

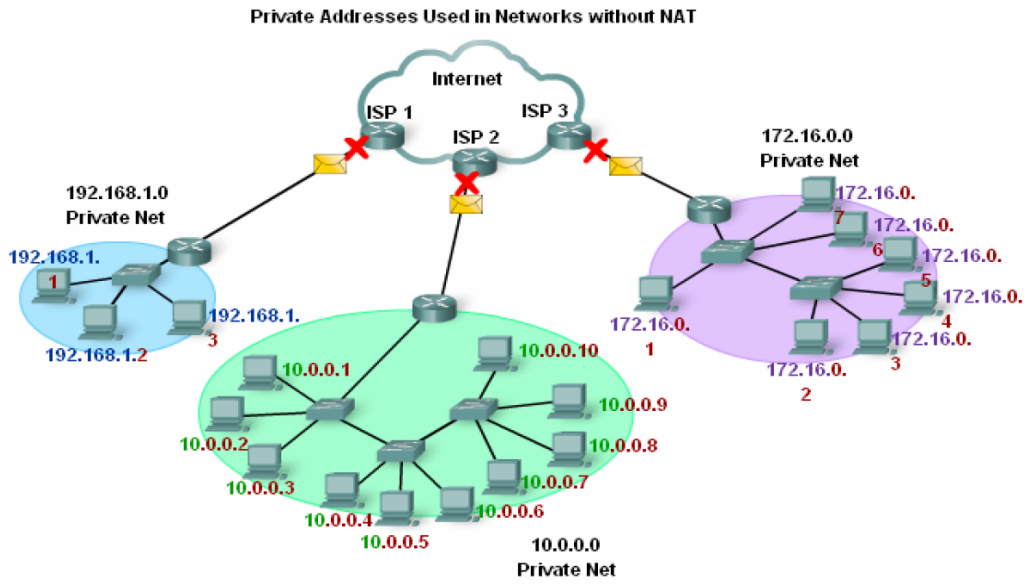
3.5.2 Network Address Translation (NAT)

With services to translate private addresses to public addresses, hosts on a privately addressed network can have access to resources across the Internet. These services, called Network Address Translation (NAT), can be implemented on a device at the edge of the private network.

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.



3.6 Special IPv4 Address

There are certain addresses that cannot be assigned to hosts for various reasons. There are also special addresses that can be assigned to hosts but with restrictions on how those hosts can interact within the network.

3.6.1 Network and Broadcast Addresses

As explained earlier, within each network the **first and last addresses** cannot be assigned to hosts. These are the network address and the broadcast address, respectively.

3.6.2 Default Route

Also presented earlier, we represent the IPv4 default route **as 0.0.0.0**. The default route is used as a "catch all" route when a more specific route is not available. The use of this address also reserves all addresses in the **0.0.0.0 - 0.255.255.255 (0.0.0.0 /8)** address block.

3.6.3 Loopback

One such reserved address is the IPv4 loopback address **127.0.0.1.** The loopback is a special address that hosts use to direct traffic to themselves. The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with one another. By using the loopback address instead of the assigned IPv4 host address, two services on the same host can bypass the lower layers of the TCP/IP stack. You can also ping the loopback address to test the configuration of TCP/IP on the local host.
Although only the single **127.0.0.1** address is used, addresses **127.0.0.0** to **127.255.255.255** are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.

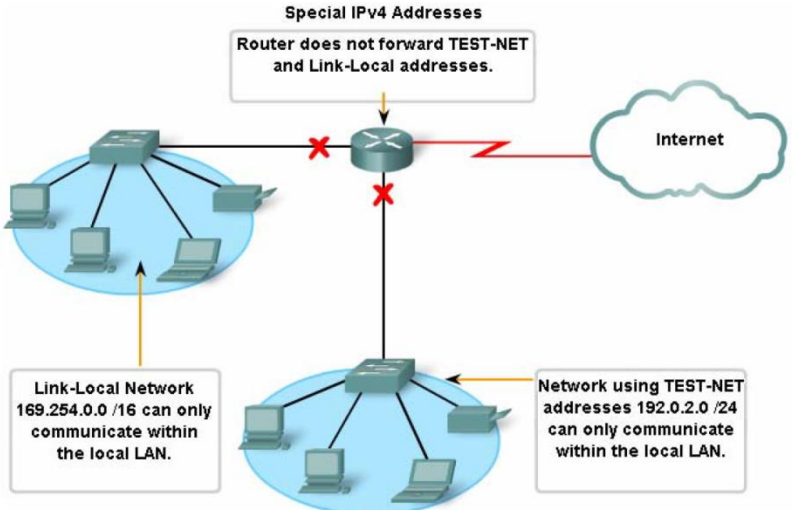
3.6.4 Link-Local Addresses

IPv4 addresses in the address block **169.254.0.0** to **169.254.255.255 (169.254.0.0 /16)** are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a ***Dynamic Host Configuration Protocol (DHCP) server.***

Communication using IPv4 link-local addresses is only suitable for communication with other devices connected to the same network, as shown in the figure. A host must not send a packet with an IPv4 link-local destination address to any router for forwarding and should set the IPv4 TTL for these packets to 1.
Link-local addresses do not provide services outside of the local network. However, many client/server and peer-to-peer applications will work properly with IPv4 link-local addresses.

3.6.5 TEST-NET Addresses

The address block **192.0.2.0** to **192.0.2.255 (192.0.2.0 /24)** is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples. Unlike the experimental addresses, network devices will accept these addresses in their configurations. You may often find these addresses used with the domain names example.com or example.net in RFCs, vendor, and protocol documentation. Addresses within this block should not appear on the Internet.



3.7 Legacy IPv4 Addressing

3.7 .1 Historic Network Classes

Historically, RFC1700 grouped the unicast ranges into specific sizes called class A, class B, and class C addresses. It also defined class D (multicast) and class E (experimental) addresses, as previously presented.

The unicast address classes A, B, and C defined specifically-sized networks as well as specific address blocks for these networks, as shown in the figure.

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

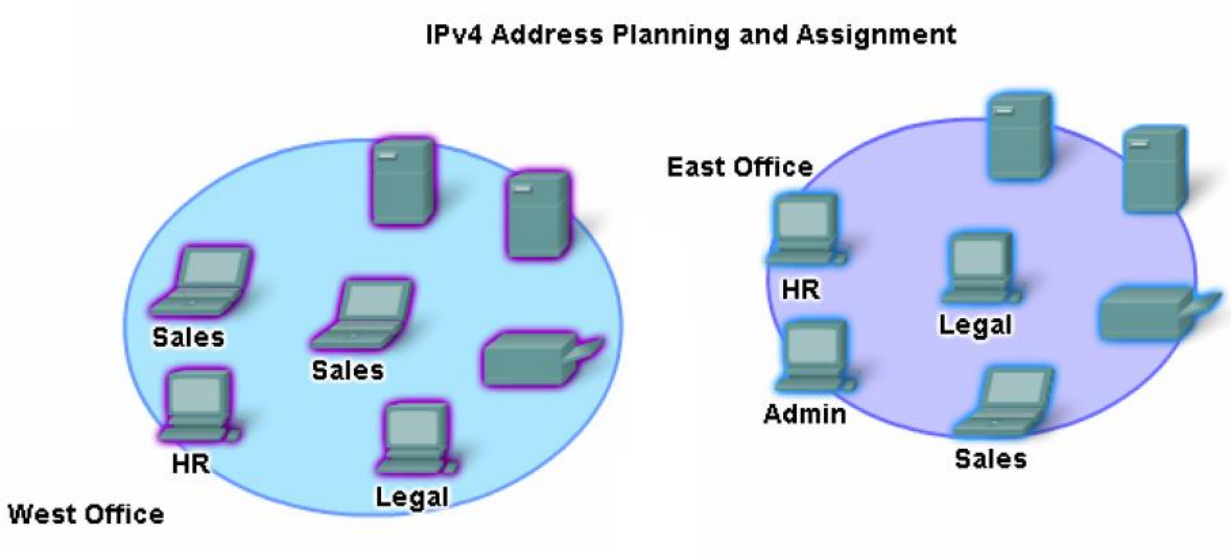
Similarly, we need to monitor the security and performance of the network hosts and the network as a whole. As part of the monitoring process, we examine network traffic looking for addresses that are generating or receiving excessive packets. If we have proper planning and documentation of the network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

3. 10.1 Addresses for User Devices

In most data networks, the largest population of hosts includes the end devices such as PCs, IP phones, printers, and PDAs. Because this population represents the largest number of devices within a network, the largest number of addresses should be allocated to these hosts.

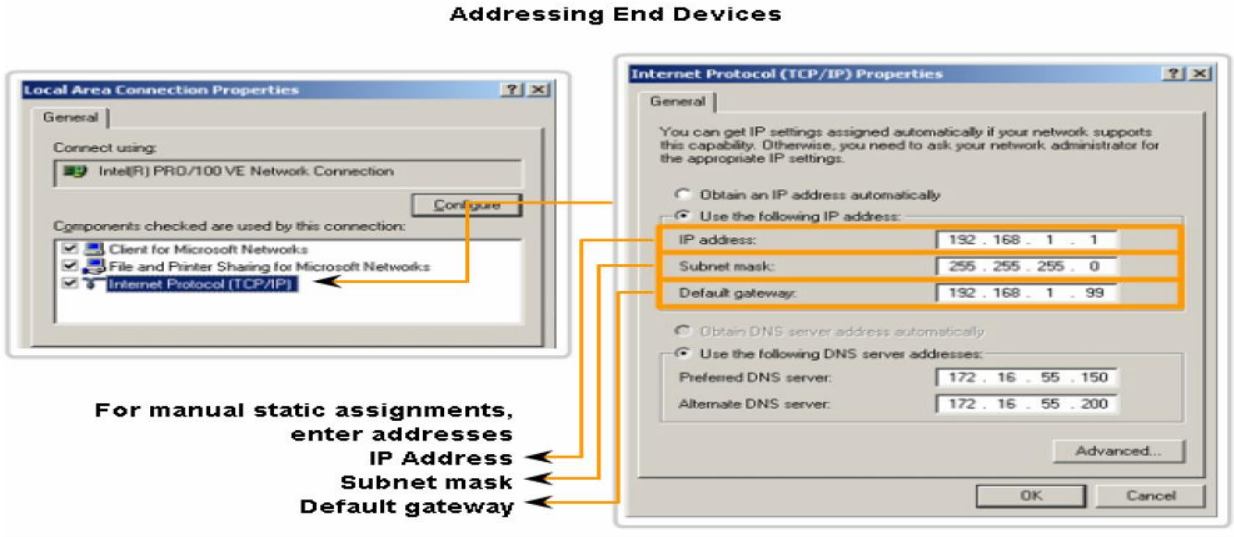
IP addresses can be assigned either statically or dynamically.

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.



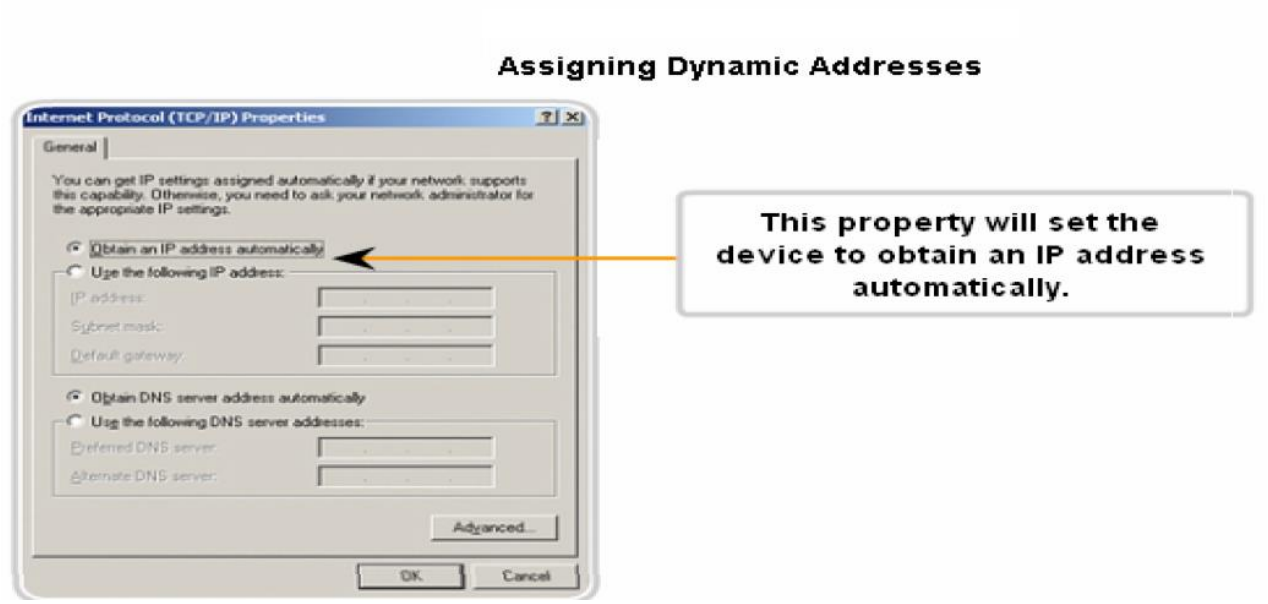
3. 10.3 Dynamic Assignment of Addresses

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



3.11 Assigning Addresses to other Devices

3.11.1 Addresses for Servers and Peripherals

Any network resource such as a server or a printer should have a static IPv4 address, as shown in the figure. The client hosts access these resources using the IPv4 addresses of these devices. Therefore, predictable addresses for each these servers and peripherals are necessary.

Servers and peripherals are a concentration point for network traffic. There are many packets sent to and from the IPv4 addresses of these devices. When monitoring network traffic with a tool like

Wire shark, a network administrator should be able to rapidly identify these devices. Using a consistent numbering system for these devices makes the identification easier.

Addresses for Hosts that are Accessible from Internet

In most internetworks, only a few devices are accessible by hosts outside of the corporation. For the most part, these devices are usually servers of some type. As with all devices in a network that provide network resources, the IPv4 addresses for these devices should be static.

In the case of servers accessible by the Internet, each of these must have a public space address associated with it. Additionally, variations in the address of one of these devices will make this device inaccessible from the Internet. In many cases, these devices are on a network that is numbered using private addresses. This means that the router or firewall at the perimeter of the network must be configured to translate the internal address of the server into a public address. Because of this additional configuration in the perimeter intermediary device, it is even more important that these devices have a predictable address.

3.11.2 Addresses for Intermediary Devices

Intermediary devices are also a concentration point for network traffic. Almost all traffic within or between networks passes through some form of intermediary device. Therefore, these network devices provide an opportune location for network management, monitoring, and security.

Most intermediary devices are assigned Layer 3 addresses. either for the device management or for their operation. Devices such as hubs, switches, and wireless access points do not require IPv4 addresses to operate as intermediary devices. However, if we need to access these devices as hosts to configure, monitor, or troubleshoot network operation, they need to have addresses assigned.

Because we need to know how to communicate with intermediary devices, they should have predictable addresses. Therefore, their addresses are typically assigned manually. Additionally, the addresses of these devices should be in a different range within the network block than user device addresses.

3.11.3 Routers and Firewalls

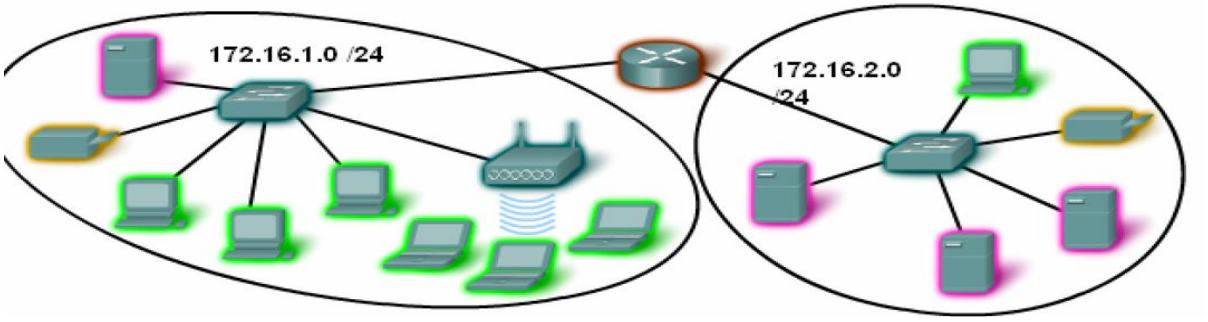
Unlike the other intermediary devices mentioned, routers and firewall devices have an IPv4 address assigned to each interface. Each interface is in a different network and serves as the gateway for the hosts in that network. Typically, the router interface uses either the lowest or highest address in the network. This assignment should be uniform across all networks in the corporation so that network personnel will always know the gateway of the network no matter which network they are working on.

Router and firewall interfaces are the concentration point for traffic entering and leaving the network. Because the hosts in each network use a router or firewall device interface as the gateway out of the network, many packets flow through these interfaces. Therefore, these devices can play a major role in network security by filtering packets based on source and/or destination

IPv4 addresses. Grouping the different types of devices into logical addressing groups makes the assignment and operation of this packet filtering more efficient.

Devices IP Address Ranges

Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



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. These registration companies are called Regional Internet Registries (RIRs), as shown in the figure.

The major registries are:

- AfriNIC (African Network Information Centre) - Africa Region http://www.afrinic.net
- APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region http://www.apnic.net
- ARIN (American Registry for Internet Numbers) - North America Region http://www.arin.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands http://www.lacnic.net
- RIPE NCC (Reseaux IP Europeans) - Europe, the Middle East, and Central Asia http://www.ripe.net

Entities that Oversee IP Address Allocation

Global	IANA				
Regional Internet Registries	AfriNIC Africa Region	APNIC Asia/ Pacific Region	LACNIC Latin America And Caribbean Region	ARIN North America Region	RIPE NCC Europe, Middle East, Central Asia Region

3.12 Assigning Addresses

3.12.1 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:

Improved packet handling

Increased scalability and longevity

QoS mechanisms

Integrated security

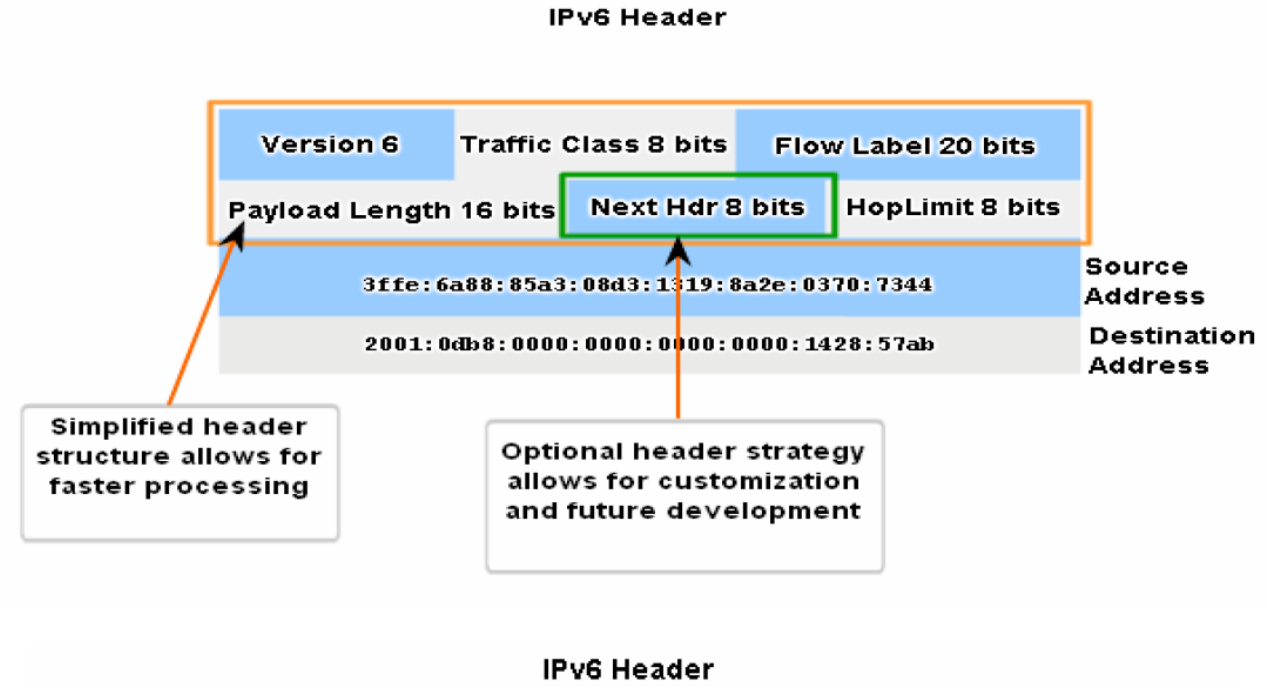
To provide these features, IPv6 offers:

- 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 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.



IPv6 Header

3.13. Is It on My Network?

3.13.1The 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

Subnet mask
255.255.255.224
11111111.11111111.11111111.11100000

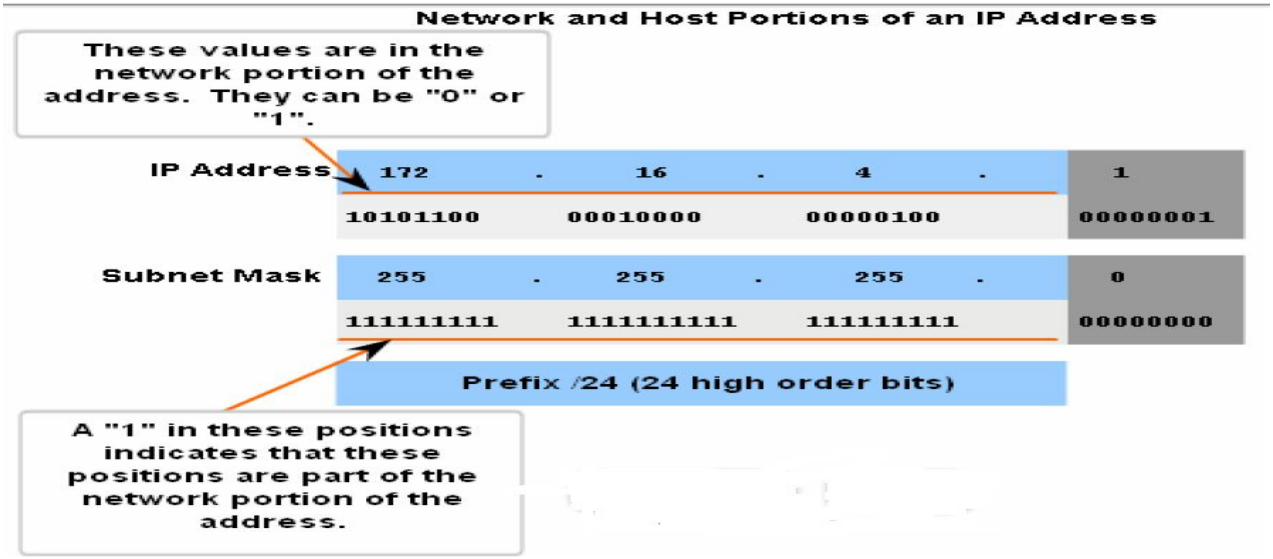
Network address
172.16.20.32
10101100.00010000.00010100.00100000

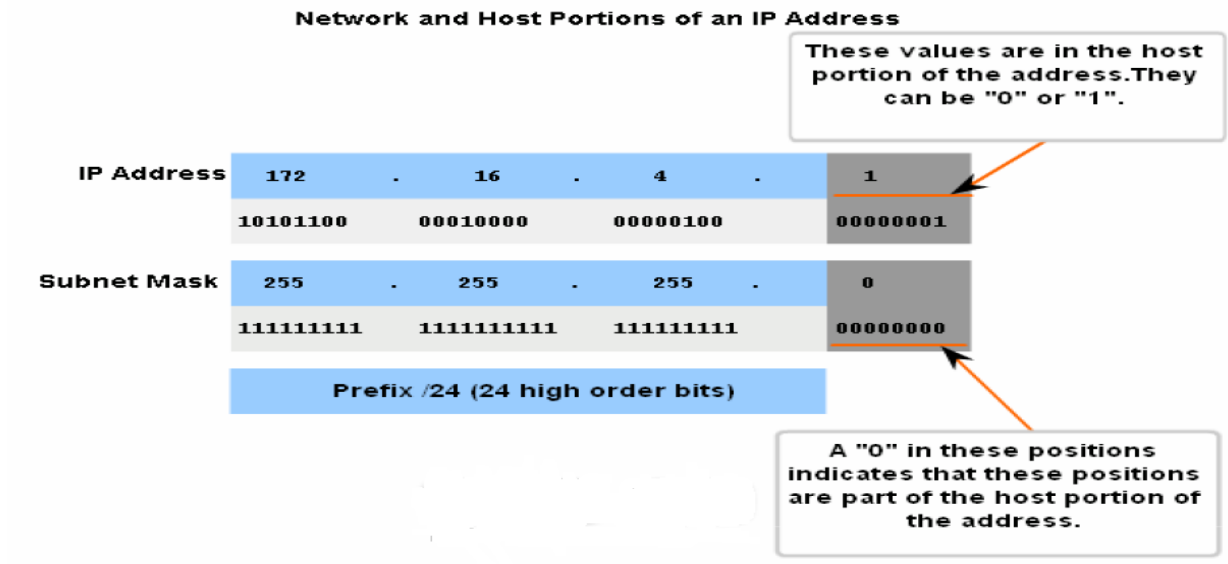
Because the high order bits of the subnet masks are contiguous 1s, there are only a limited number of subnet values within an octet. You will recall that we only need to expand an octet if the network and host division falls within that octet. Therefore, there are a limited number 8 bit patterns used 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 AND 1 = 1
1 AND 0 = 0
0 AND 1 = 0
0 AND 0 = 0

The result from anything ANDed with a 1 yields a result that is the original bit. That is, 0 AND 1 is 0 and 1 AND 1 is 1. Consequently, anything ANDed with a 0 yields a 0.These properties of ANDing are used with the subnet mask to "mask" the host bits of an IPv4 address. Each bit of the address is ANDed with the corresponding bit of the subnet mask.

Because all the bits of the subnet mask that represent host bits are 0s, the host portion of the resulting network address becomes all 0s. Recall that an IPv4 address with all 0s in the host portion represents the network address.

Likewise, all the bits of the subnet mask that indicate network portion are 1s. When each of these 1s is ANDed with the corresponding bit of the address, the resulting bits are identical to the original address bits.

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.

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.

3.13.5 The Importance of AND

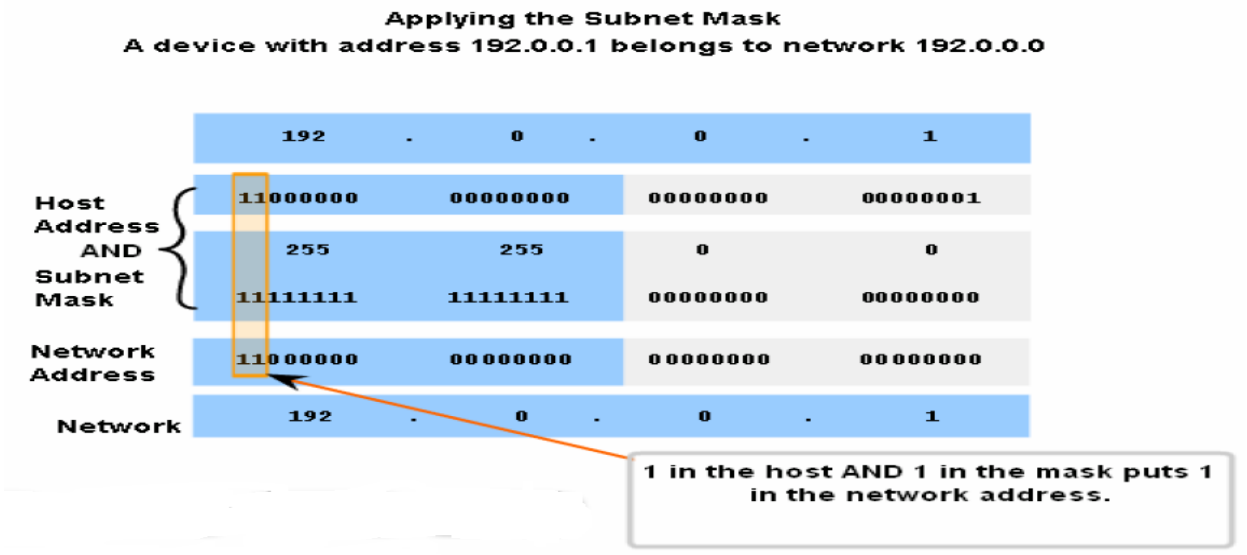
If the routers and end devices calculate these processes without our intervention, why do we need to learn how to AND? The more we understand and are able to predict about the operation of a network, the more equipped we are to design and/or administer one.

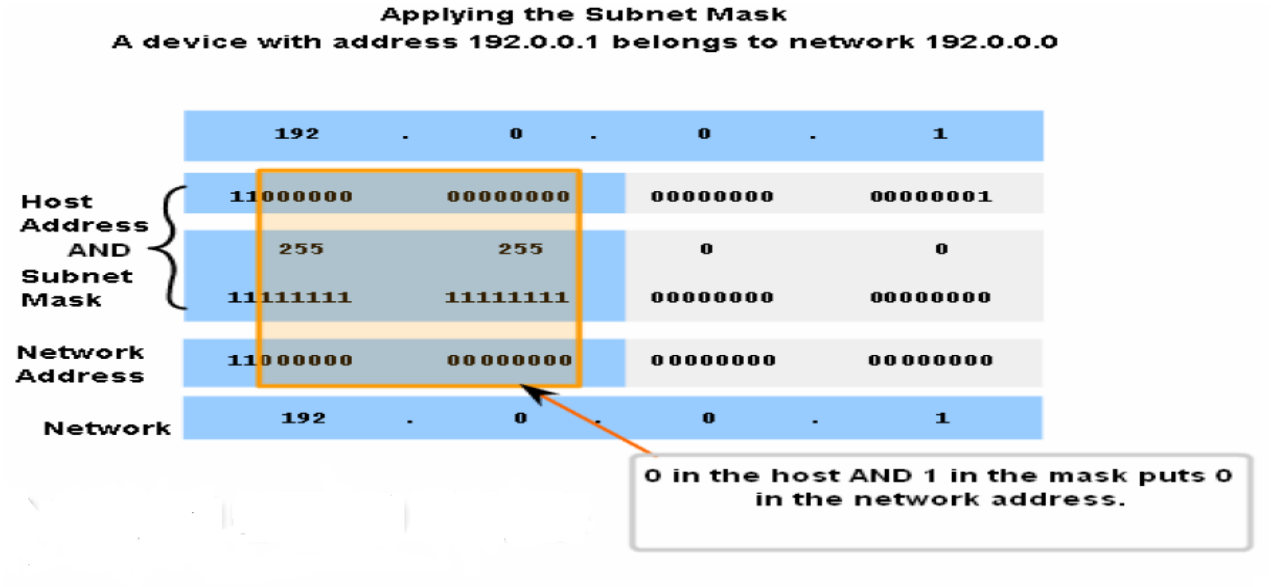
In network verification/troubleshooting, we often need to determine what IPv4 network a host is on or if two hosts are on the same IP network. We need to make this determination from the perspective of the network devices. Due to improper configuration, a host may see itself on a

network that was not the intended one. This can create an operation that seems erratic unless diagnosed by examining the ANDing processes used by the host.

Also, a router may have many different routes that can satisfy the forwarding of packet to a given destination. The selection of the route used for any given packet is a complex operation. For example, the prefix forming these routes is not directly associated with the networks assigned to the host. This means that a route in the routing table may represent many networks. If there were issues with routing packets, you would need to determine how the router would make the routing decision.

Although there are subnet calculators available, it is helpful for a network administrator to know how to manually calculate subnets.





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

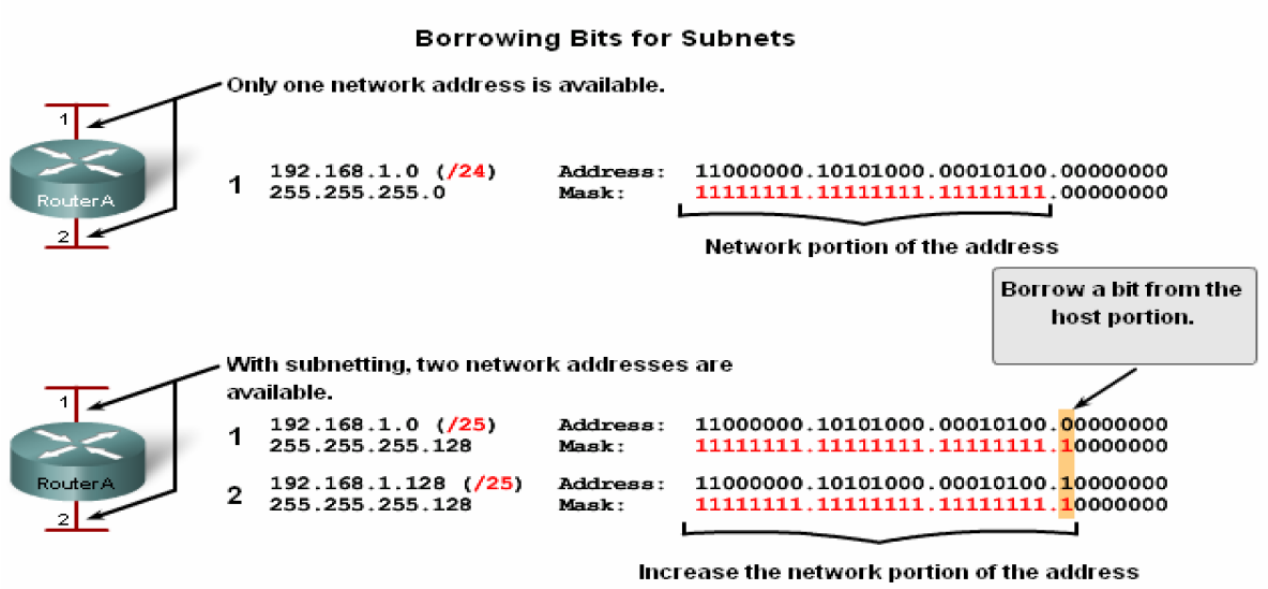
Use this formula to calculate the number of subnets:
2^n where n = the number of bits borrowed
In this example, the calculation looks like this:
2^1 = 2 subnets

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.



Borrowing Bits for Subnets

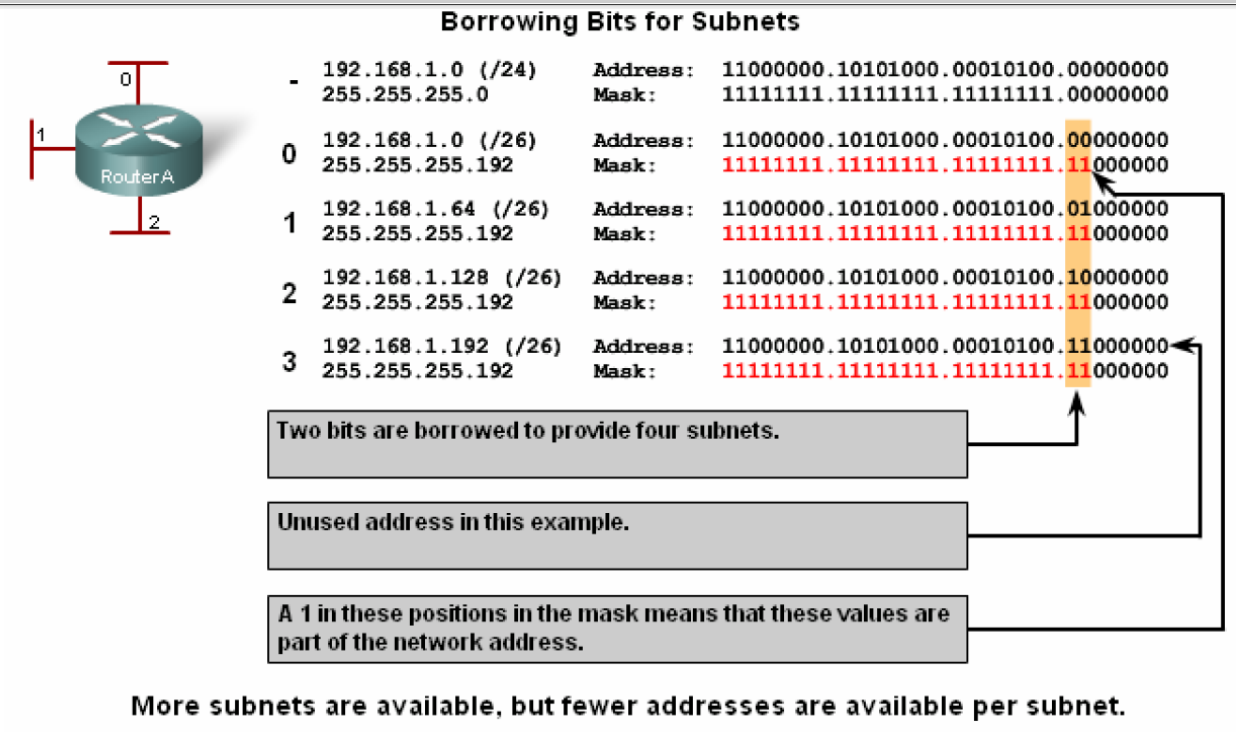
Addressing Scheme: Example of 2 networks

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.
2^6 - 2 = 62 hosts per subnet
See the figure for the addressing scheme for these networks.



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.

0 = 00000000

32 = 00100000

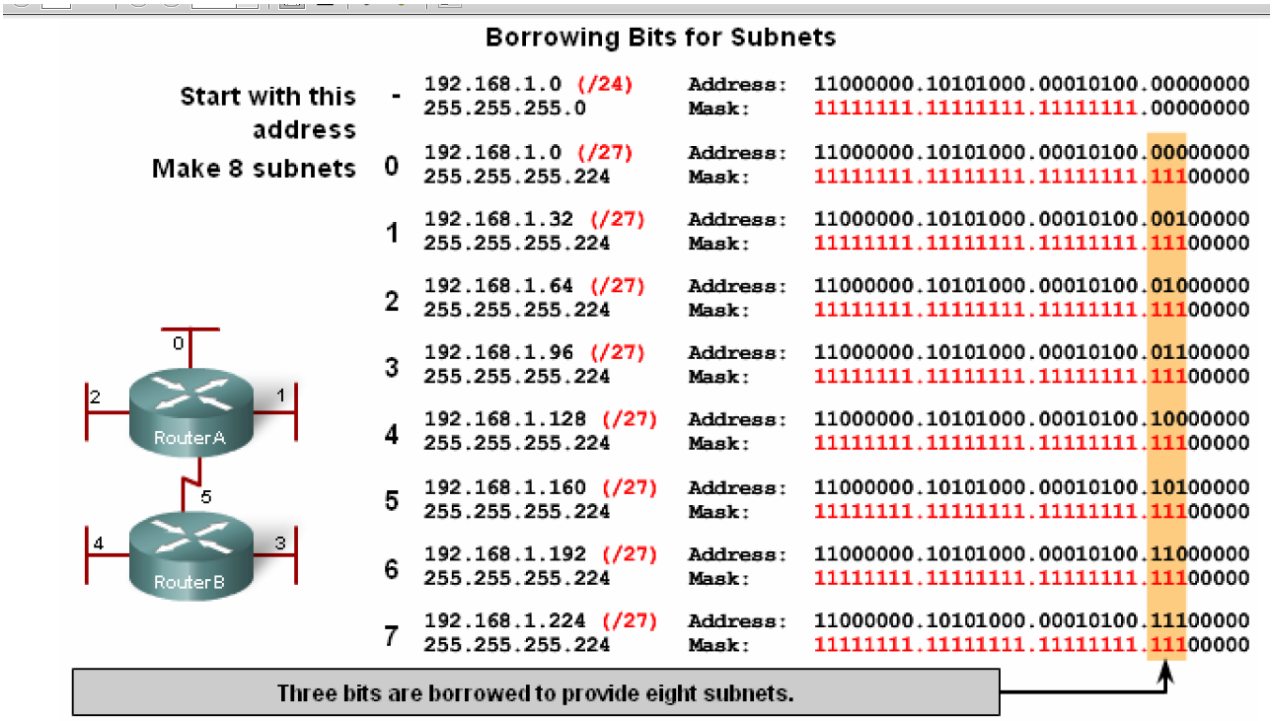
64 = 01000000

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

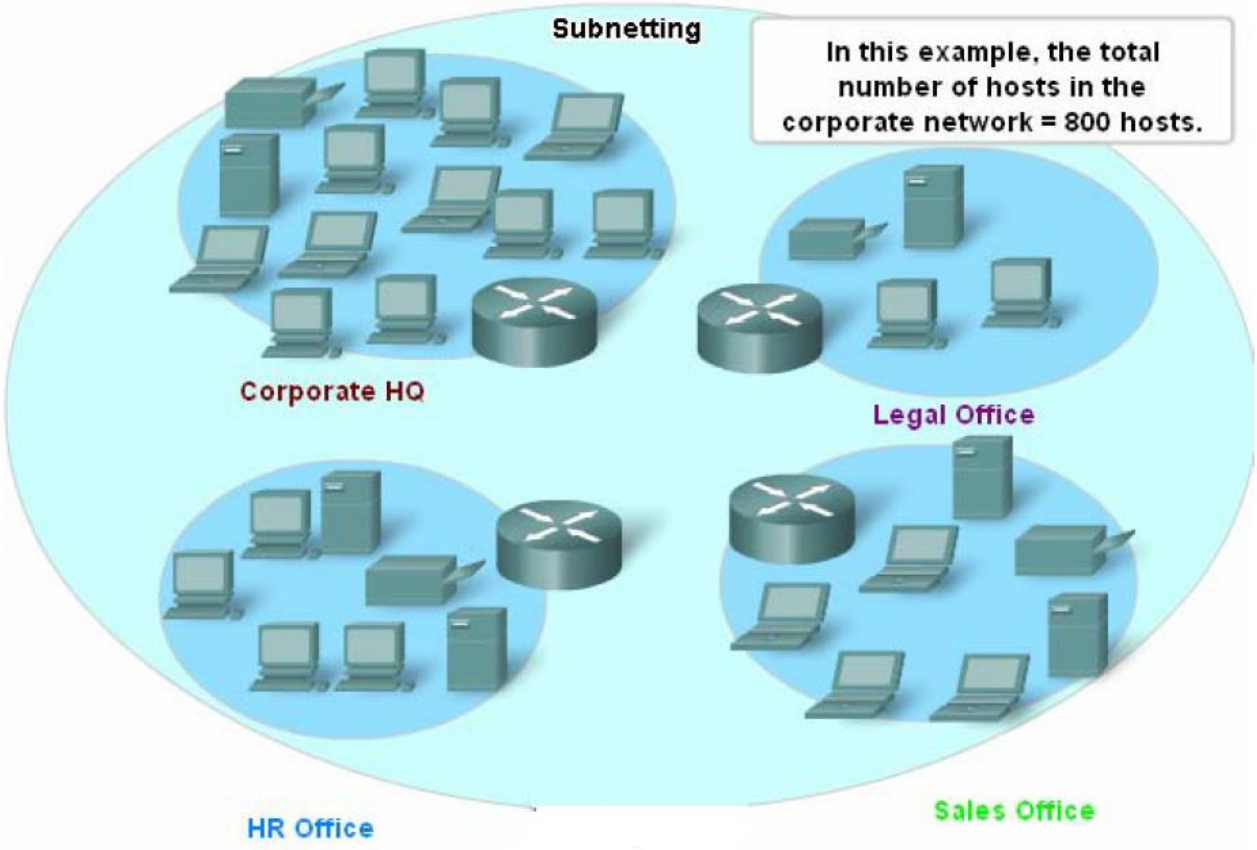
15. Subnetting-Dividing Networks into Right Sizes

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.

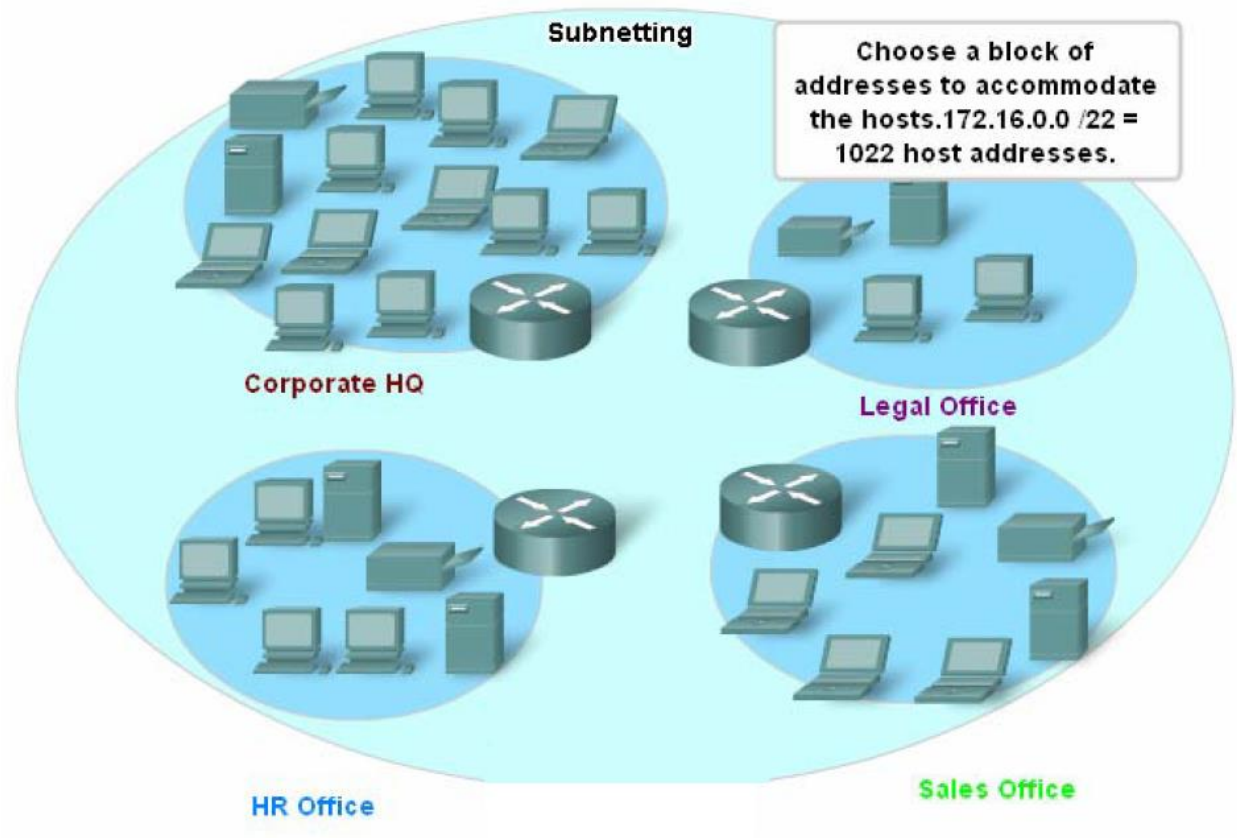


Consider the example of a corporate internetwork that needs to accommodate 800 hosts in its four locations.

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.



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.

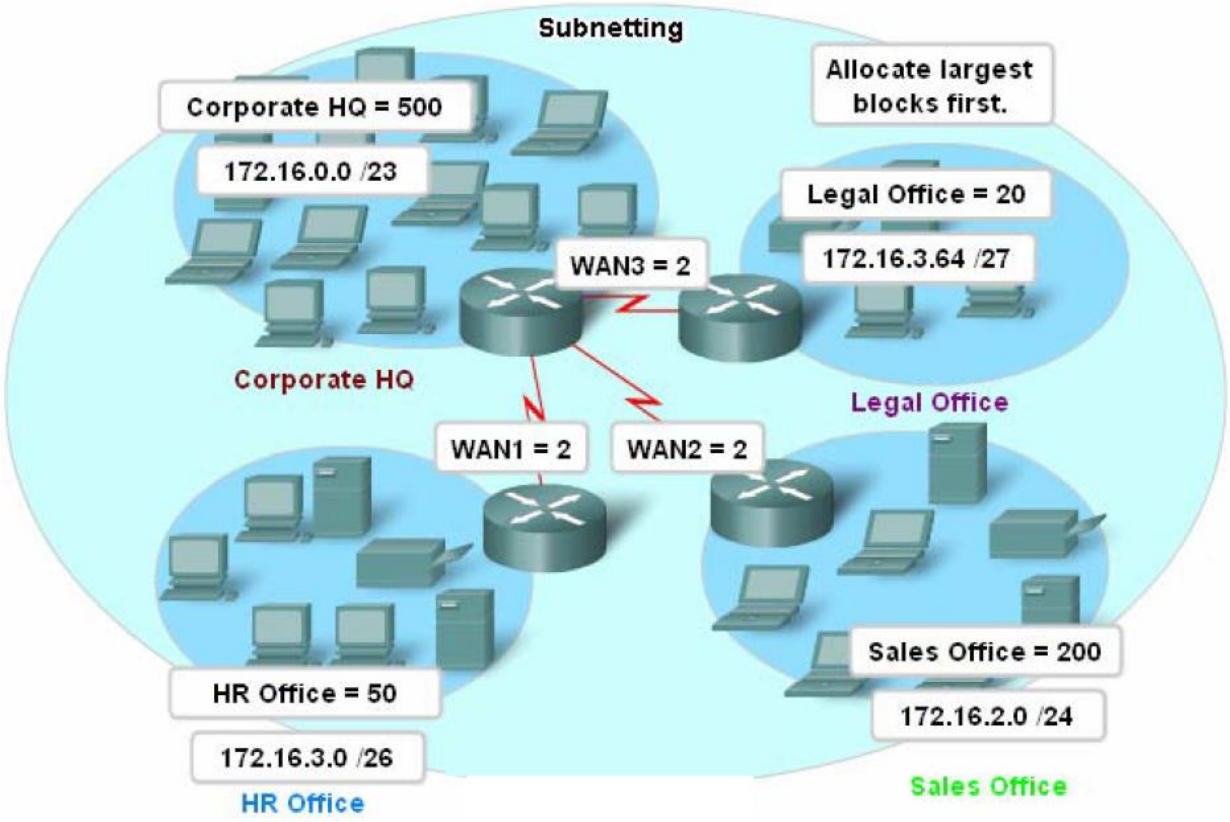
One useful tool in this address planning process is a network diagram. A diagram allows us to see the networks and make a more accurate count.

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.

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:
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.
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

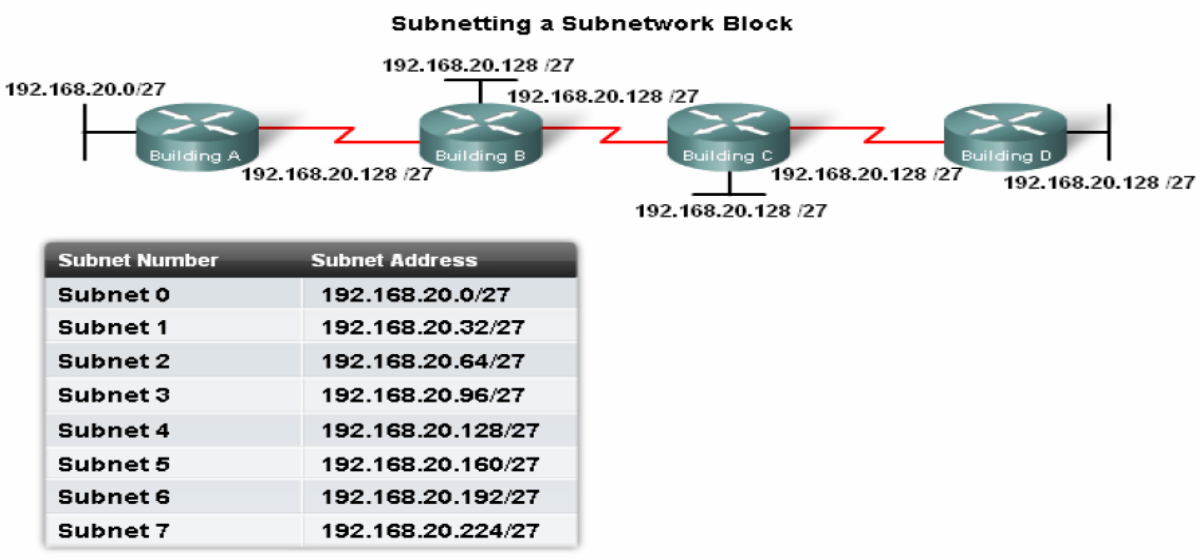
the original subnets free to be allotted to other devices and prevents many addresses from being wasted.

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.

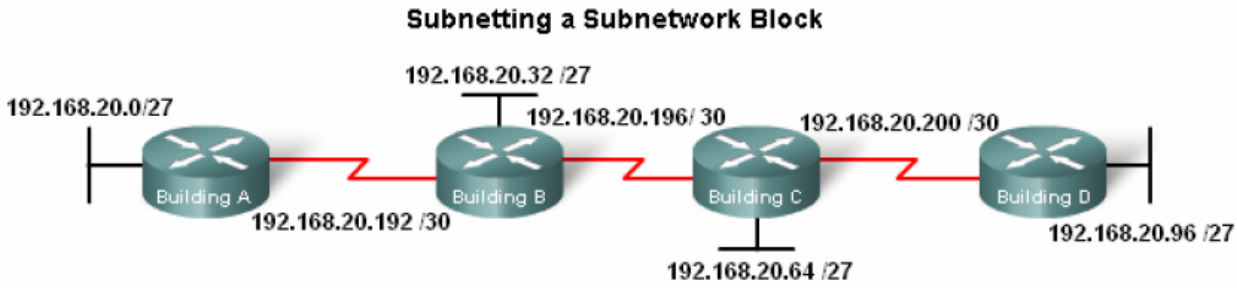
Address: 192.168.20.192 In Binary: 11000000.10101000.00010100.11000000

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.



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	192.168.20.20/30

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.

16.1 Getting More

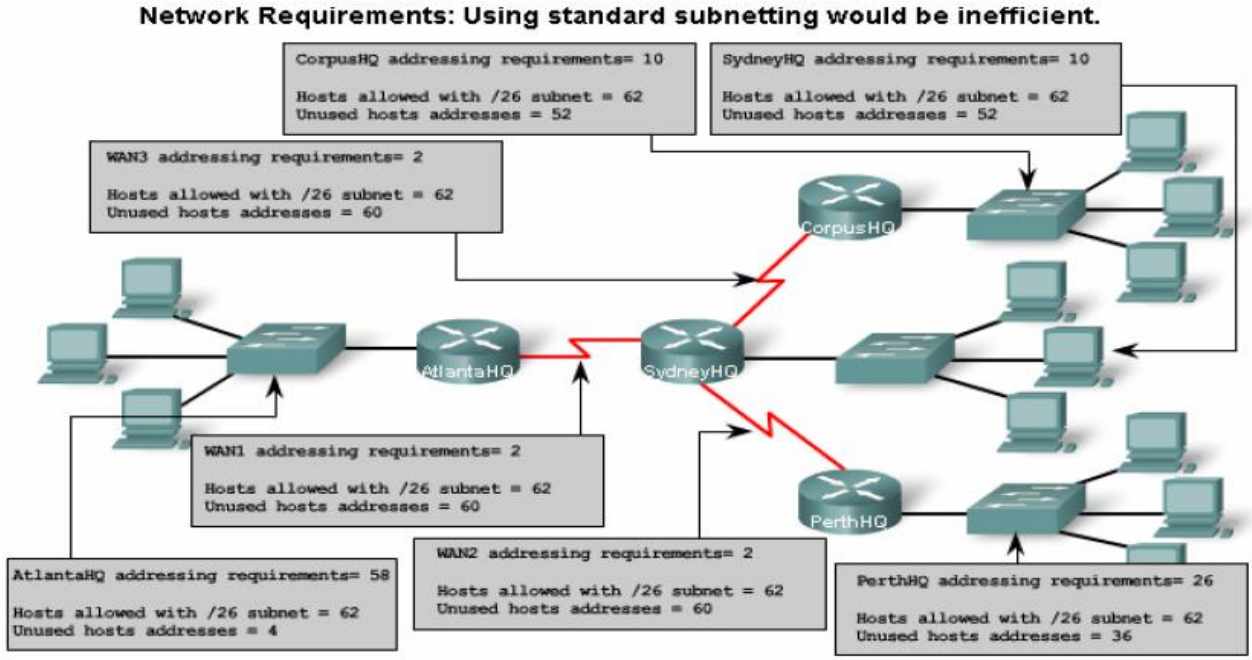
When creating an appropriate addressing scheme, always begin with the largest requirement. In this case, the AtlantaHQ, with 58 users, has the largest requirement. Starting with 192.168.15.0, we will need 6 host bits to accommodate the requirement of 58 hosts, this allows 2 additional bits for the network portion. The prefix for this network would be /26 and a subnet mask of 255.255.255.192.

Let's begin by subnetting the original address block of 192.168.15.0 /24. Using the Usable hosts = 2^n - 2 formula, we calculate that 6 host bits allow 62 hosts in the subnet. The 62 hosts would meet the required 58 hosts of the AtlantaHQ company router.

Address: 192.168.15.0 In Binary: 11000000.10101000.00001111.00000000

Mask: 255.255.255.192 26 Bits in binary: 11111111.11111111.11111111.11000000

The next page shows the process of identifying the next sequence of steps.



Network Requirements: Using standard subnetting would be inefficient.

	Actual Requirements	Total Wasted Addresses
AtlantaHQ	58 host addresses	4 addresses
PerthHQ	26 host addresses	36 addresses
SydneyHQ	10 host addresses	52 addresses
CorpusHQ	10 host addresses	52 addresses
WAN links	2 host addresses (each)	60 addresses

The steps for implementing this subnetting scheme are described here.

Assigning the AtlantaHQ LAN

See Steps 1 and 2 in the figure.

The first step shows a network-planning chart. The second step in the figure shows the entry for the AtlantaHQ. This entry is the results of calculating a subnet from the original 192.168.15.0 /24 block to accommodate the largest LAN, the AtlantaHQ LAN with 58 hosts. Doing this required borrowing an additional 2 host bits, to use a /26 bit mask.

By comparison, the following scheme shows how 192.168.15.0 would be subnetted using fixed block addressing to provide large enough address blocks:

Subnet 0: 192.168.15.0 /26 host address range 1 to 62

Subnet 1: 192.168.15.64 /26 host address range 65 to 126

Subnet 2: 192.168.15.128 /26 host address range 129 to 190

Subnet 3: 192.168.15.192 /26 host address range 193 to 254

The fixed blocks would allow only four subnets and therefore not allow enough address blocks for the majority of the subnets in this internetwork. Instead of continuing to use the next available subnet, we need to ensure we make the size of each subnet consistent with the host requirements. Using an addressing scheme directly correlated to the host requirements requires the use of a different method of sub netting.