HNDIT2042
Data Communication
and Computer Networks

Week 1 - Introduction

Module Details

Course Code : **HNDIT2042**

Course Title : **Data communication and Computer Networks**

Semester : **2**

Course Status :**Compulsory GPA**

Number of Credits : **03**

Module Details

Time Allocation (per Week) :

Lectures : 2 hours

Tutorials /practical : 2 hours

Course Aim

- The course provides both practical and general knowledge of communication.
- It deals with principles and methods for constructing digital communication systems with an emphasis on data link and network protocols and provides an introduction to TCP / IP protocols.

Learning Outcome

After successful completion of this course the student should be able to:

LO1: Describe the evolution of the Internet.

LO2: Understand the protocols and standards used throughout the Internet.

LO3: Discuss a variety of Internet and WWW applications and related technologies.

LO4: Evaluate the opportunities and threats created by interconnecting computers via the Internet

Assessment and Weights

- On-line quizzes & Group Assignment - 40%
- Final Examination (3 Hour paper) - 60%

Learning Resources

❖**Textbook and Resources**

- Presten Gralla and Michael Troller, How the Internetworks, Que, (8th Edition), 2006.0789736268 978-0789736260

❖**Recommended Additional Resources**

- Introduction to Computers, Peter Norton, 7th or latest edition, Tata McGraw-Hill

❖**Course website at LMS**

HNDIT2042
Data Communication and Computer Networks

Week 1 - The Internet and World Wide Web

Sub topics

- The Evolution of the Internet
- Growth of the World Wide Web

What is Internet?

- The largest network of networks in the world.
- Uses TCP/IP protocols and packet switching .
- Runs on any communications substrate.

What is internet?

- A network of networks, joining many government, university and private computers together and providing an infrastructure for the use of E-mail, bulletin boards, file archives, hypertext documents, databases and other computational resources
- The vast collection of computer networks which form and act as a single huge network for transport of data and messages across distances which can be anywhere from the same office to anywhere in the world.

What is a Communication Network?

A communications network is a network of links and nodes arranged so that messages may be passed from one part of the network to another

- What are nodes and links?
  - People and roads
  - Telephones and switches
  - Computers and routers
- What is a message?
  - Information

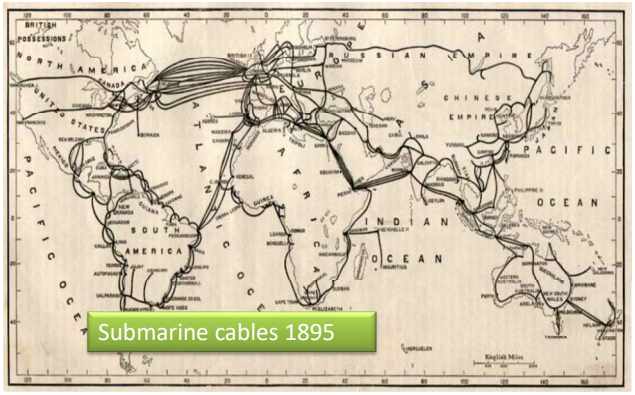
Networks are Old

- 2400 BC: courier networks in Egypt
- 550 BC: postal service invented in Persia

Problems:
- Speed
- Reliability
- Security

Submarine Cables + The Telegraph

- 1850 – first submarine cables laid
- by 1900 the first global communications network!



Towards Electric Communication

- 1837: Telegraph invented by Samuel Morse
  - Distance: 10 miles
  - Speed: 10 words per minute
  - In use until 1985!
- Key challenge: how to encode information?
  - Originally used unary encoding

    A • B •• C ••• D •••• E •••••
  - Next generation: binary encoding

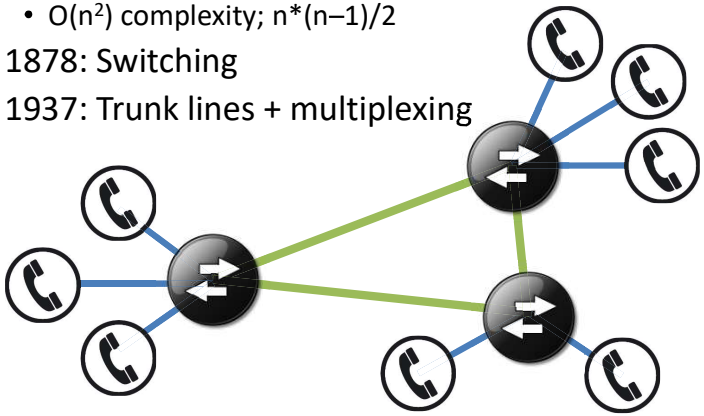
    A •– B –••• C –•–• D –•• E •

Telegraph

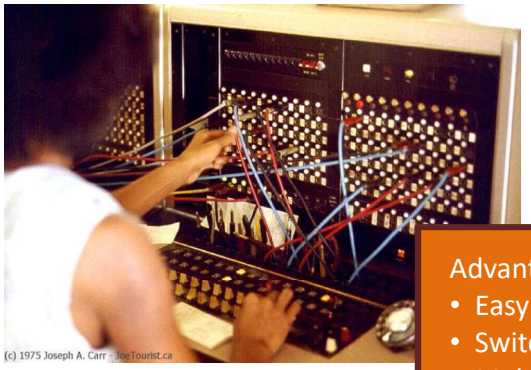
- Victorian Internet
- Invented in the 1840s.
- Signals sent over wires that were established over vast distances
- Used extensively by the U.S. Government during the American Civil War, 1861 - 1865
- Morse Code was dots and dashes, or short signals and long signals
- The electronic signal standard of +/- 15 v. is still used in network interface cards today.

Telephony

- 1876 – Alexander Graham Bell invents the telephone
- Key challenge: how to scale the network?
  - Originally, all phones were directly connected
    - $O(n^2)$ complexity; $n*(n-1)/2$
  - 1878: Switching
  - 1937: Trunk lines + multiplexing



Telephony

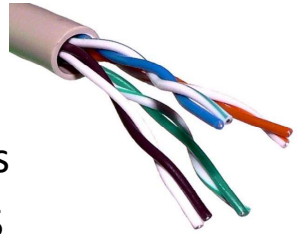


Advantages
- Easy to use
- Switching mitigates complexity
- Makes cable management tractable

Problems
- Manual switching
- 1918: cross country call took 15 minutes to set up

Growth of the Telephone Network

- 1881: Twisted pair for local loops
- 1885: AT&T formed
- 1892: Automatic telephone switches
- 1903: 3 million telephones in the US
- 1915: First transcontinental cable
- 1927: First transatlantic cable
- 1937: first round-the-world call
- 1946: National numbering plan

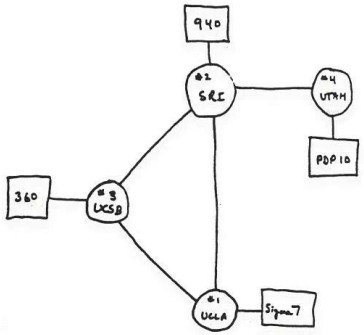


at&t

Crazy idea: Packet switching

- Telephone networks are circuit switched
  - Each call reserves resources end-to-end
  - Provides excellent quality of service
- Problems
  - Resource intense (what if the circuit is idle?)
  - Complex network components (per circuit state, security)
- Packet switching
  - No connection state, network is store-and-forward
  - Minimal network assumptions
  - Statistical multiplexing gives high overall utilization

The World's Most Successful Computer Science Research Project



THE ARPA NETWORK

DEC 1969

4 NODES

FIGURE 6.2 Drawing of 4 Node Network (Courtesy of Alex McKenzie)

History of the Internet

- 1961: Kleinrock @ MIT: packet-switched network
- 1962: Licklider's vision of Galactic Network
- 1965: Roberts connects computers over phone line
- 1967: Roberts publishes vision of ARPANET
- 1968 - DARPA (Defense Advanced Research Projects Agency) contracts with BBN (Bolt, Beranek & Newman) to create ARPAnet
- 1969: BBN installs first interface Msg Processor at UCLA
- 1970: Network Control Program (NCP)
- 1972: Public demonstration of ARPANET
- 1972: Kahn @ DARPA advocates Open Archite
- 1974: Vint Cerf @ Stanford writes TCP

More Internet History

- 1974: Cerf and Kahn paper on TCP (IP kept separate)
- **1980: TCP/IP adopted as defense standard**
- **1983: ARPANET and MILNET split**
- 1983: Global NCP to TCP/IP flag day
- 198x: Internet melts down due to congestion
- **1986: Van Jacobson saves the Internet (BSD TCP)**
- 1987: NSFNET merges with other networks
- 1988: Deering and Cheriton propose multicast
- **1994: NSF backbone dismantled, private backbone**
- 1999-present: The Internet boom and bust … and boom
- 2007: Release of iPhone, rise of Mobile Internet

What is next?

Internet Applications Over Time

- 1972: Email
- 1973: Telnet – remote access to computing
- 1982: DNS – "phonebook" of the Internet
- 1985: FTP – remote file access
- 1989: NFS – remote file systems
- 1991: The World Wide Web (WWW) goes public
- 1995: SSH – secure remote shell access
- 1995-1997: Instant messaging (ICQ, AIM)
- 1998: Google
- 1999: Napster, birth of P2P
- 2001: Bittorrent
- 2004: Facebook
- 2005: YouTube
- 2007: The iPhone

What is next?

Internet Growth Trends

- 1977: 111 hosts on Internet
- 1981: 213 hosts
- 1983: 562 hosts
- 1984: 1,000 hosts
- 1986: 5,000 hosts
- 1987: 10,000 hosts
- 1989: 100,000 hosts
- 1992: 1,000,000 hosts
- 2001: 150 – 175 million hosts
- 2002: over 200 million hosts
- By 2010, about 80% of the planet will be on the Internet

Takeaways

- Communication is fundamental to human nature
- Key concepts have existed for a long time
  - Speed/bandwidth
  - Latency
  - Switching
  - Packets vs. circuits
    - Encoding
    - Cable management
    - Multiplexing
    - Routing
- The Internet has changed the world
  - Promise of free ($) and free (freedom) communication
  - Shrunk the world
- What made the Internet so successful? Stay tuned!

Thank You

What is Big Data?

- Reference file

HNDIT2042
Data Communication
and Computer Networks

Week 2 – Client Server Architecture

Sub topics

- Models Architectures
- Client-Server model
- Intranet/Internet /Extranet

Client – Server Architecture

- Every computer or process in a network can act as a server or client in a client-server architecture.
- Powerful computers, known as client servers, are used just to manage network traffic, disk drives, and printers.
- Clients use their workstations or personal computers to run their apps.
- The servers' main function is to supply resources like equipment, files, and processing power.

Client

- Any computer that makes a request to the server is a client.
- For instance, when we visit a website, we ask for the page from its domain. So, in this case, we play the client.

Server

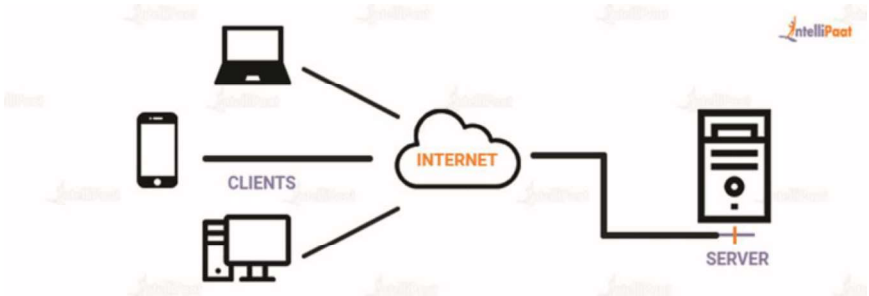
- The server is the computer created to fulfill client requests.
- For instance, when we visit a website ,the client queries the server for the web page, which is subsequently returned to them by the server.

Client server Architecture

- Client server architecture is a computing model in which the server hosts, delivers, and manages most of the resources and services requested by the client.
- It is also known as the networking computing model or client server network as all requests and services are delivered over a network.
- The client-server architecture or model has other systems connected over a network where resources are shared among the different computers.

Client server Architecture

- A server is the one who provides requested services.
- Clients are the ones who request services.



Client server architecture -example

- **Mail servers**

Email servers are used for sending and receiving emails. There are different software that allow email handling.

- **File servers**

File servers act as a centralized location for files. The centrally stored files can be accessed by multiple users from any devices.

  - Google Docs.

- **Web servers**

Web servers are high-performance computers that host different websites. The server site data is requested by the client through high-speed internet.

Components of client server architecture

- Three components are required to make client server architecture work. The three components are workstations, servers, and networking devices.

Components of client server architecture

- **Workstations**

  Workstations are also called client computers. Workstations work as subordinates to servers and send them requests to access shared files and databases.

  A server requests information from the workstation and performs several functions as a central repository of files, programs, databases, and management policies. Workstations are governed by server-defined policies.

Components of client server architecture

- **Servers**

  Servers are defined as fast processing devices that act as centralized repositories of network files, programs, databases, and policies.

  Servers have huge storage space and robust memory to deal with multiple requests, approaching simultaneously from various workstations.

  Servers can perform many roles, such as mail server, database server, file server, and domain controller, in client server architecture at the same time.

Components of client server architecture

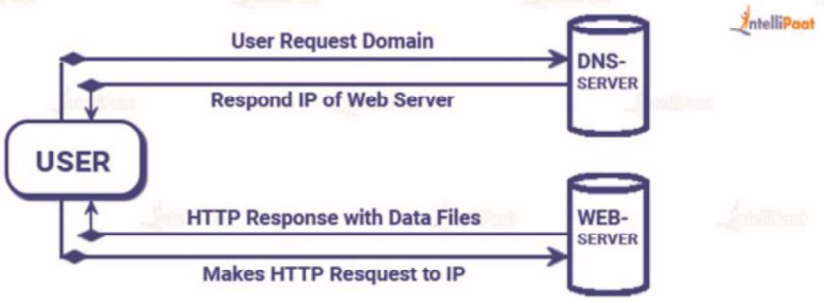
- **Networking devices**

  Networking devices are a medium that connects workstations and servers in client server architecture.

  Many networking devices are used to perform various operations across the network.

  For example, a hub is used for connecting a server to various workstations . Repeaters are used to effectively transfer data between two devices. Bridges are used to isolate network segmentation.

How does client server architecture work?



Accessing Web server

How does client server architecture work?

- The user enters the uniform resource locator (URL) of the website or file and the browser sends a request to the domain name system (DNS) server.
- The DNS server looks for the address of the web server and the DNS server responds with the IP address of the web server.
- After the DNS server responds, the browser sends over an HTTP or HTTPS request to the web server's IP, which was provided by the DNS server.
- The server then sends over the necessary files of the website.
- Finally, the browser renders the files and the website is displayed.

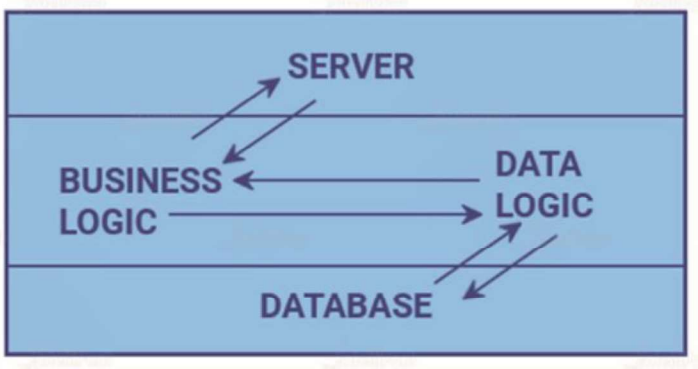
Types of client server architecture

- **1-tier architecture**
- **2-tier architecture**
- **3-tier architecture**
- **N-tier architecture**

1-tier architecture

- . 1-tier architecture consists of several layers, such as presentation layer, business layer, and data layer, that are combined with the help of a unique software package.
- The data present in this layer is usually stored in local systems or on a shared drive.

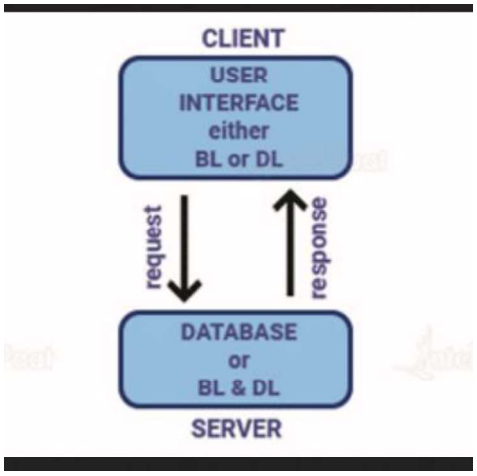
1-tier architecture



2-tier architecture

- the user interface is stored on the client's side and the database is stored on the server, while database logic and business logic is maintained either on the client's side or on the server's side.

2-tier architecture



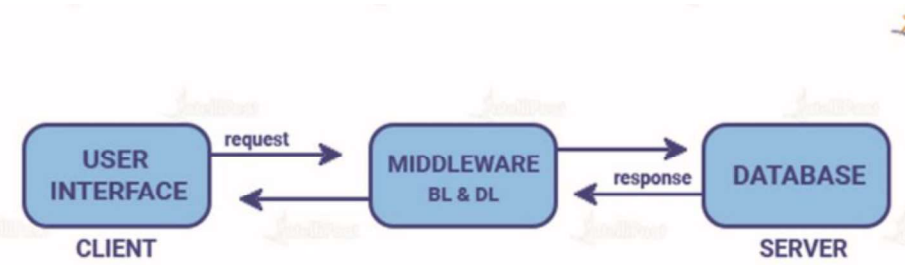
3-tier architecture

- no intermediary
- a middleware lies between the client and the server.
- If the client places a request to fetch specific information from the server, the request will first be received by the middleware. It will then be dispatched to the server for further actions.
- The same pattern will be followed when the server sends a response to the client.
- .

3-tier architecture

- The framework of 3-tier architecture is categorized into three main layers, **presentation layer, application layer, and database tier.**
- All three layers are controlled at different ends. While the presentation layer is controlled at the client's device, the middleware and the server handle the application layer and the database tier respectively.
- Due to the presence of a third layer that provides data control, 3-tier architecture is more secure, has invisible database structure, and provides data integrity.

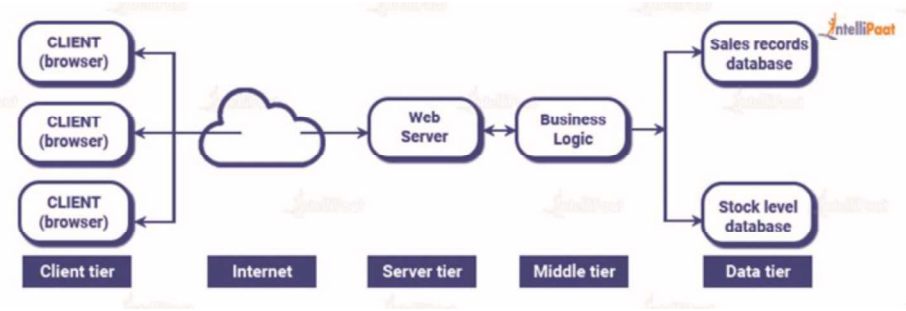
3-tier architecture



N-tier architecture

- N-tier architecture is also called multi-tier architecture.
- It is the scaled form of the other three types of architecture.
- This architecture has a provision for locating each function as an isolated layer that includes presentation, application processing, and management of data functionalities.

N-tier architecture



Characteristics of Client-server Architecture

- A mechanism of requests and responses powers the architecture. The client sends a request to the server, and the server returns data in response to the information requested.
- The architecture uses a common contact protocol so that devices can simply communicate with one another. Every data transport protocol is available at the application layer.
- A server may only be able to handle a limited number of client requests at once. It uses a method targeting priority to respond to each and every query.

Characteristics of Client-server Architecture

- By assaulting the server with duplicate requests, denial of service attacks makes it difficult for it to respond to legitimate client requests.
- Scalability is a crucial feature of client-server systems. They can be resized either horizontally or vertically. Adding or removing client workstations while barely affecting performance is known as horizontal scaling. Vertical scaling refers to upgrading to a more powerful server.
- The environment is frequently multivendor and heterogeneous. Client and server operating systems and hardware platforms typically differ from one another. A well-defined set of common application program interfaces (APIs) and remote procedure calls (RPCs) is used by client and server processes to communicate with one another.

Difference between peer-to-peer network and client server architecture

Client server architecture	Peer-to-peer architecture
It has specific clients and servers.	There is no differentiation between clients and servers.
It has centralized data management.	It has its own data and applications.
The purpose is to share information.	Its main goal is to maintain connection among peers.
Data is provided only in response to a request.	In this network, peers have the authority to request as well as provide a service.
It is suitable for small as well as large networks.	It is suitable for less users, less than 10 devices.

Advantages and disadvantages of client-server architecture

Advantages
The centralized network has complete leverage to control the processes and activities.
All devices in the network can be controlled centrally.
Users have the authority to access any file, residing in the central storage, at any time.
It provides a good user interface, easy file finding procedure, and management system for organizing files.
Easy sharing of resources across various platforms is possible.

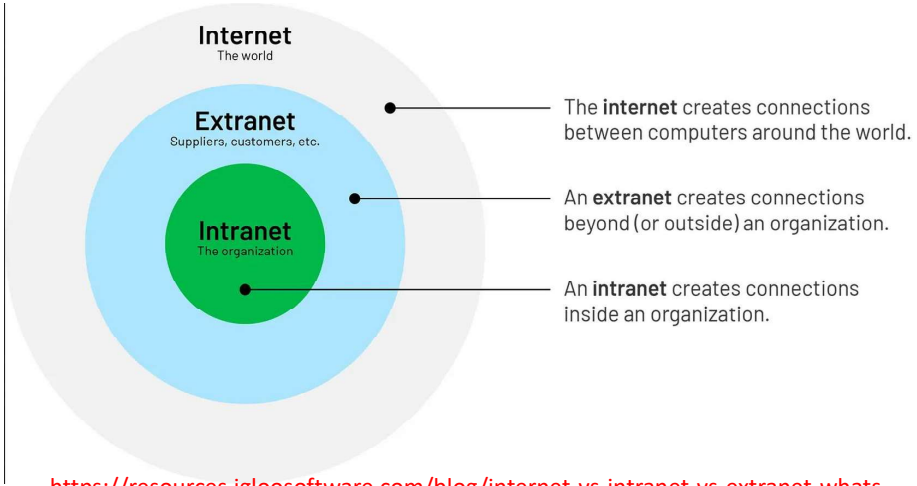
Advantages and disadvantages of client-server architecture

	Disadvantages
	If the primary server goes down, the entire architecture is disrupted.
	It is expensive to operate because of the cost of heavy hardware and software tools.
	This architecture requires particular OSs related to networking.
	Too many users at once can cause the problem of traffic congestion.
	It requires highly technical stuff, such as server machines, for maintenance of the network.

What is internet, extranet, & intranet?

- The **internet** is a globally-connected network of computers that enables people to share information and communicate with each other.
- An **intranet**,is a private and internal network that enables people to store, organize, and share information within an organization.
- An **extranet** is a web portal that is accessible by an organization and its external vendors, partners, customers, or any other users that require access to restricted information.

What is internet, extranet, & intranet?



https://resources.igloosoftware.com/blog/internet-vs-intranet-vs-extranet-whats-the-difference/

Thank You

OSI Model & TCP/IP

Out Line

- Introduction OSI
- OSI History
- OSI Layers
- Introduction TCP/IP
- TCP/IP Layers
- Layering Considered Harmful?

Introduction OSI

- The **Open System Interconnection Reference Model** (OSI Reference Model or **OSI Model**) is an abstract description for layered communications and computer network protocol design.
- It divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.

OSI History

- In 1978, the International Standards Organization (ISO) began to develop its OSI framework architecture.
- OSI has two major components: an abstract model of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols.

OSI History

- The concept of a 7 layer model was provided by the work of Charles Bachman, then of Honeywell.
- Various aspects of OSI design evolved from experiences with the Advanced Research Projects Agency Network (ARPANET) and the fledgling Internet.

OSI Layers

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability, Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Layer1: Physical Layer

- The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.
- This includes the layout of pin, voltages, cable specification, hubs, repeaters, network adapters, host bus adapters, and more.

Layer1: Physical Layer

- The major functions and services performed by the Physical Layer are:
  - Establishment and termination of a connection to a communication medium.
  - Participation in the process whereby the communication resources are effectively shared among multiple users. For example, flow control.
  - Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Layer1: Physical Layer con.

- The same applies to local-area networks, such as Ethernet, token ring ,

  FDDI(Fiber Distributed Data Interface),

  ITU-T(International Telecommunication Union Telecommunication Standardization Sector) G.hn and IEEE802.1I.
- Personal area networks such as Bluetooth and IEEE 802.15.4.

Layer 2: Data Link Layer

- The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.
- Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system.
- The data link layer is divided into two sub-layers by IEEE.

Layer 2: Data Link Layer

- One is Media Access Control (MAC) and another is Logical Link Control (LLC).
- Mac is lower sub-layer, and it defines the way about the media access transfer, such as CSMA/CD/CA(Carrier Sense Multiple Access/Collision Detection/Collision Avoidance)
- LLC provides data transmission method in different network. It will re-package date and add a new header.

Layer 3: Network Layer

- The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer.

Layer 3: Network Layer

- The Network Layer performs
  - network routing functions,
  - perform fragmentation and reassembly,
  - report delivery errors.
- Routers operate at this layer—sending data throughout the extended network and making the Internet possible.

Layer 4: Transport Layer

- The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.
- The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

Layer 5: Session Layer

- The Session Layer controls the dialogues (connections) between computers.
- It establishes, manages and terminates the connections between the local and remote application.
- It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.

Layer 5: Session Layer

- The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 6: Presentation Layer

- The Presentation Layer establishes a context between Application Layer entities, in which the higher-layer entities can use different syntax and semantics, as long as the presentation service understands both and the mapping between them.
- This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa.
- This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems.
- It is sometimes called the syntax layer.

Layer 7: Application Layer

- The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.
- Application layer functions typically include:
  - identifying communication partners,
  - determining resource availability,
  - synchronizing communication.

Layer 7: Application Layer

- Identifying communication partners
  - Determines the identity and availability of communication partners for an application with data to transmit.
- Determining resource availability
  - Decide whether sufficient network or the requested communication exist.
- Synchronizing communication
  - All communication between applications requires cooperation that is managed by the application layer.

Layer 7: Application Layer

- Some examples of application layer implementations include
  - Hypertext Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - Simple Mail Transfer Protocol (SMTP)

OSI Feature

- Open system standards over the world
- Rigorously defined structured, hierarchical network model
- Complete description of the function
- Provide standard test procedures

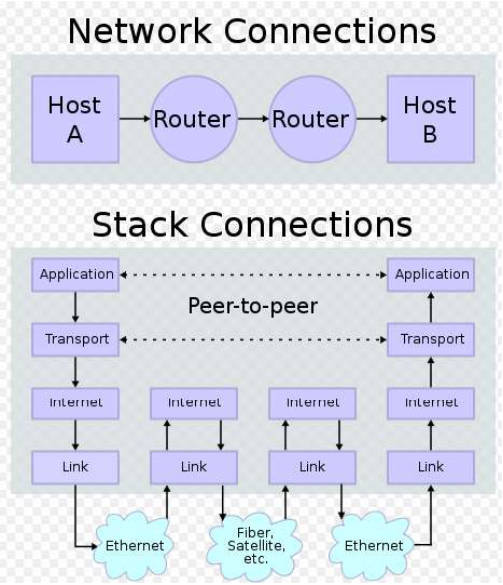
Introduction TCP/IP

- The **Internet Protocol Suite** (commonly known as **TCP/IP**) is the set of communications protocols used for the Internet and other similar networks.
- It is named from two of the most important protocols in it:
  - the Transmission Control Protocol (TCP) and
  - the Internet Protocol (IP), which were the first two networking protocols defined in this standard.

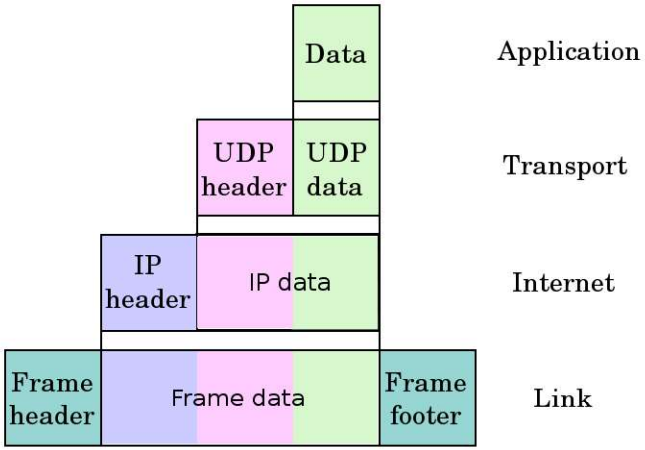
TCP/IP Layers

OSI	TCP/IP
Application Layer	Application Layer TELNET, FTP, SMTP, POP3, SNMP, NNTP, DNS,NIS, NFS, HTTP, …
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer TCP , UDP , …
Network Layer	Internet Layer IP , ICMP, ARP, RARP, …
Data Link Layer	Link Layer FDDI, Ethernet, ISDN, X.25,…
Physical Layer	

TCP/IP Stack



TCP/IP Encapsulation



TCP/IP Some Protocol

Layer	Protocol
Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SMPP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6), ICMP, IGMP, and ICMPv6
	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP

References

- http://en.wikipedia.org/wiki/OSI_model
- http://en.wikipedia.org/wiki/Internet_Protocol_Suite
- http://lips.lis.ntu.edu.tw/YTCHIANG/STUDY/others/tcpiposi.htm
- RFC 3439

HNDIT2042
Data Communication
and Computer Networks

Week 3 –*Internet - Access Methods –Part 1*

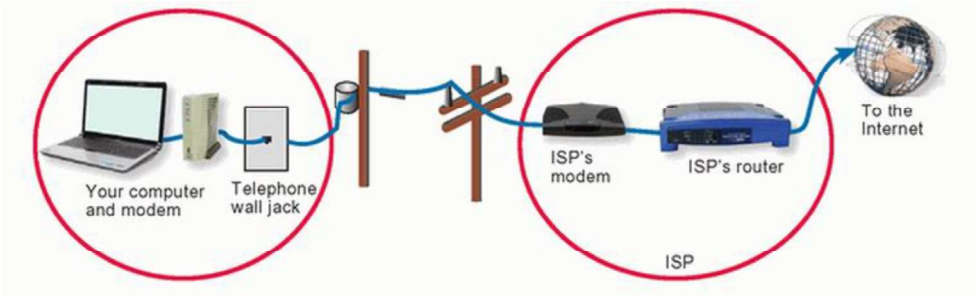
Sub topics

- Types of Internet connection
- Communication Media
- Proxy Server

Types of Internet connection

- Dial-UP
- Digital Subscriber Line(DSL)
- ADSL
- ISDN
- Cable Modem
- Leased Line
- Fiber optic
- Satellite
- Wireless
- Mobile /cellular

Dial Up



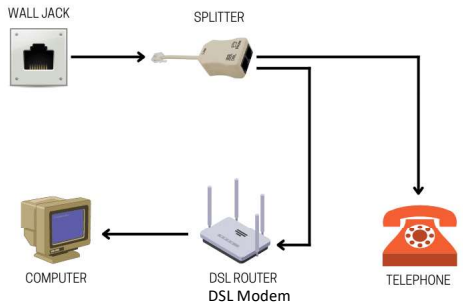
Dial -up

- Dial-up access is really just like a phone connection
- Connection through modem and a public switched telephone network(PSTN).
- It uses analog telephone lines
- Encoding & Decoding of analog signals is done by modem
- Using a dial-up line to transmit data is similar to using the telephone to make a call

Dial -Up

- Advantages
  - Low Cost
  - Availability
- Disadvantages
  - Low Speed
  - Requires phone line
  - Route busy

DSL



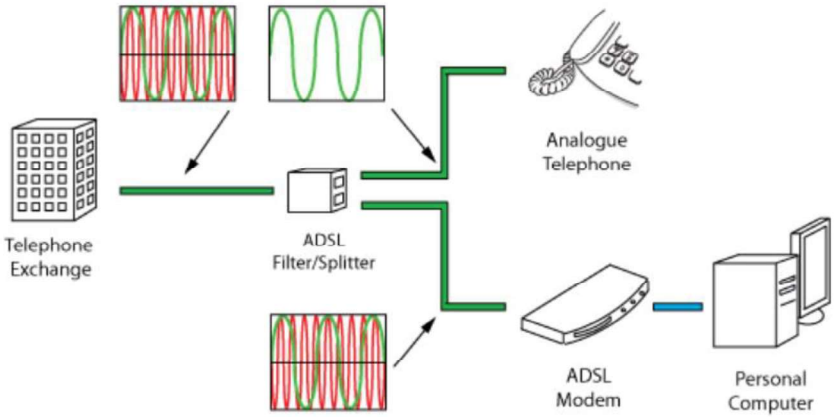
DSL

- Digital Subscriber Line
- generic term that encompasses all types of digital subscriber lines
- High-speed data service that works over copper telephone lines
- DSL is considered a "symmetrical" technology (same download and upload speeds)
- Price not much more than the price of dial up, but twice the speed .

DSL

- Advantages
  - DSL simultaneously keeps your Internet connection and phone lines open
  - Downloads are faster than uploads
  - DSL uses the existing wiring infrastructure of your telephone line
- Disadvantages
  - Large amount of uploading is not possible
  - DSL is limited to a certain perimeter
  - Compared to dial up ,it is expensive

ADSL



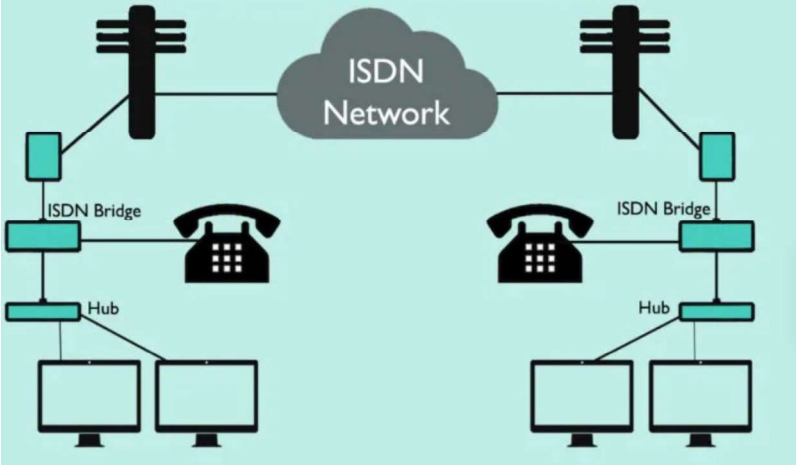
ADSL

- Technology used for delivering high-speed internet access over traditional copper telephone lines
- specific type of DSL technology that is designed to provide faster download speeds than upload speeds.
- It is called "asymmetric" because it has different download and upload speeds.
- ADSL uses frequency division multiplexing (FDM) to split the telephone line into separate voice and data channels, allowing for simultaneous phone and internet use.
- widely used technology for home and small business internet connections

ADSL

- Advantages
  - Very fast download speeds
  - Transfers data digitally, therefore no need to translate data from analogue to digital and vice versa.
  - ADSL connections are always on – no connection time.
- Disadvantages
  - Not available to everyone, need ADSL coverage in your area.
  - Hardware costs are higher

ISDN



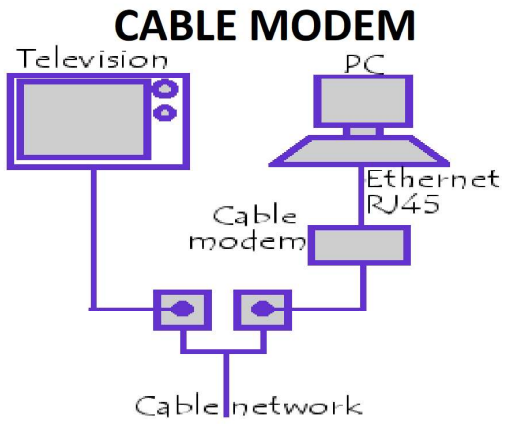
ISDN

- Integrated Services Digital Network
- Standard for digital telecommunications that allows fast digital dialup connections
- It put together speech and information on the same line

ISDN

- Advantages
  - Multiple digital channels
  - Speedy
  - Can be used for other activities Eg. Video conferencing
- Disadvantages
  - It is very costly than other typical telephone system

Cabel Modem



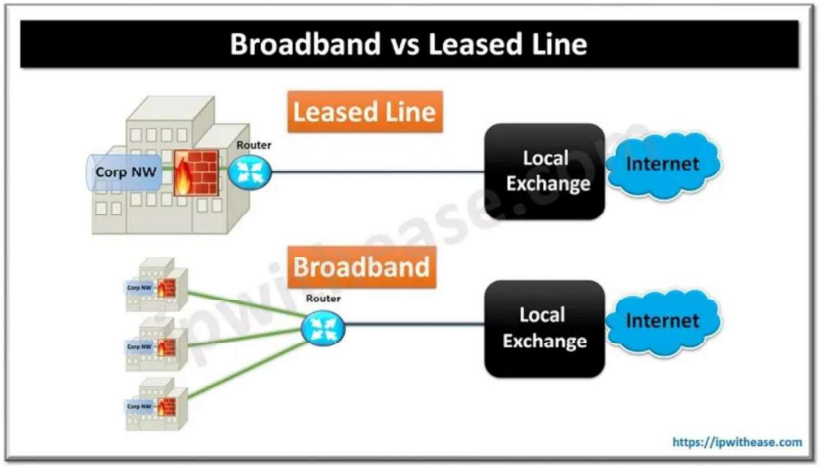
Cable Modem

- Cable modems provide Internet access using the same cables that transmit cable television
- uses a special cable, known as a coaxial cable, and a modem.
- Internet access over cable modem is delivered to homes by cable television lines.
- Most cable companies provide you with the modem and a network card that must be installed on your computer.
- With cable Internet, the cable company becomes the Internet service provider.
- Cable modem connections are faster than dial-up and DSL connections.

Cable Modem

- Advantages
  - High connection speed
  - Convenient
  - Does not affect your phone line
  - Easy setup with self installation kit
- Disadvantages
  - Higher price than dialup and DSL connection
  - Higher security risk than dialup or DSL
  - Not available to all cable TV networks
  - speed can be affected by the number of users on the same network.

LEASED LINE



Leased Line

- A leased line is a high-speed internet connection between two locations.
- The service involves renting a dedicated cable from the telecom to connect two offices or branches together, enabling users to transfer large volumes of data and giving a consistent connection to the internet.
- offer the same functionality as a dedicated line, but at a fraction of the cost and with added flexibility.
- telephone line that is dedicated to a particular business.
- only pay a monthly bill based on usage

Leased Line

- Advantages
  - Dedicated connection between customer premises and provider local exchange
  - Bandwidth is dedicated to a customer
  - Symmetric speed
  - High performance
  - High reliability
  - Greater speed
  - Public IP are generally provided
- Disadvantages
  - Higher cost

Fiber Optic

- fastest type of internet connection available today.
- It uses fiber-optic cables to transmit data, and it can provide speeds of up to 1 Gbps or more.
- Fiber-optic internet is not as widely available as other types of internet connections, and it can be more expensive.

Fiber Optic

- Advantages
  - High speed
  - Reliability
  - Security
  - Distance
  - scalability
- Disadvantages
  - Cost
  - Accessibility
  - Maintenance
  - Fragility
  - Compatibility:

Satellite

Satellite

- Satellite internet is a wireless connection that uses a satellite dish to communicate with a satellite in orbit.
- It can be useful in rural or remote areas where other types of internet connections are not available, but it can be expensive and can suffer from latency issues.
- Data is being sent from the satellite to a user's equipment and then translated and decoded.
- Equipment required-mini dish satellite receiver and satellite modem

Satellite

- Advantages
  - High speed internet access
  - Does not tie up with local phone service or cable TV subscription
  - Connection speed is not affected by phone or cable wiring
- Disadvantages
  - More expensive than DSL and cable
  - Large setup fee. Expensive equipment upfront. Has to be setup by trained technician.

Wireless OR Wi-Fi

- Use of radio waves to transmit data wirelessly between devices that are connected to a local area network (LAN).
- Wi-Fi technology uses a wireless access point, such as a router, to create a network that enables multiple devices, such as smartphones, laptops, and tablets, to connect and communicate with each other.
- The speed and range of a WiFi network depend on several factors
  - type of WiFi standard being used (such as 802.11ac or 802.11ax)
  - the distance between devices,
  - any obstacles or interference in the environment.

Wireless OR Wi-Fi

- Advantages
  - Convenience
  - Mobility
  - Cost-effective
  - Flexibility
- Disadvantages
  - Security concerns
  - Interference
  - Limited range
  - Health concern

Mobile/ cellular

- Mobile internet uses cellular networks to provide internet access on mobile devices such as smartphones and tablets.
- Mobile internet speeds can vary depending on the network coverage and the number of users on the network.
- It can be a useful option for people who need internet access while on the go.

Broadband ?

- Broadband is a brand name for high-speed Internet access, and internet services provided by telecom companies.
- The term broadband is used to differentiate these services from traditional dial-up connections.
- Broadband is the connection of two or more home computers to the Internet. This is possible because of the much higher bandwidth (capacity for transmitting data) of the Internet.
- In a traditional connection, the user is allocated a single telephone line, shared with the telephone and cable TV. With broadband, the user gets a dedicated line that is used especially for the Internet.

Activity 1

- Find the internet downloading /uploading speeds on above internet connection.

Integrated Services Digital Network
ISDN

- Services
- History
- Subscriber Access
- Layers
- BISDN

Services

- Goal: provide fully integrated digital services to users. These services fall into three categories:
  - Bearer Services: Provide the means to transfer information without the network manipulating the content of that information. (Layers 1, 2, and 3 of OSI).
  - Teleservices: The may alter the contents of the data (layers 4-7 of the OSI model).
  - Supplementary Services: Provide additional functionality to the bearer services and teleservices such as call waiting, reverse charging, and message handling.

Figure 15-1

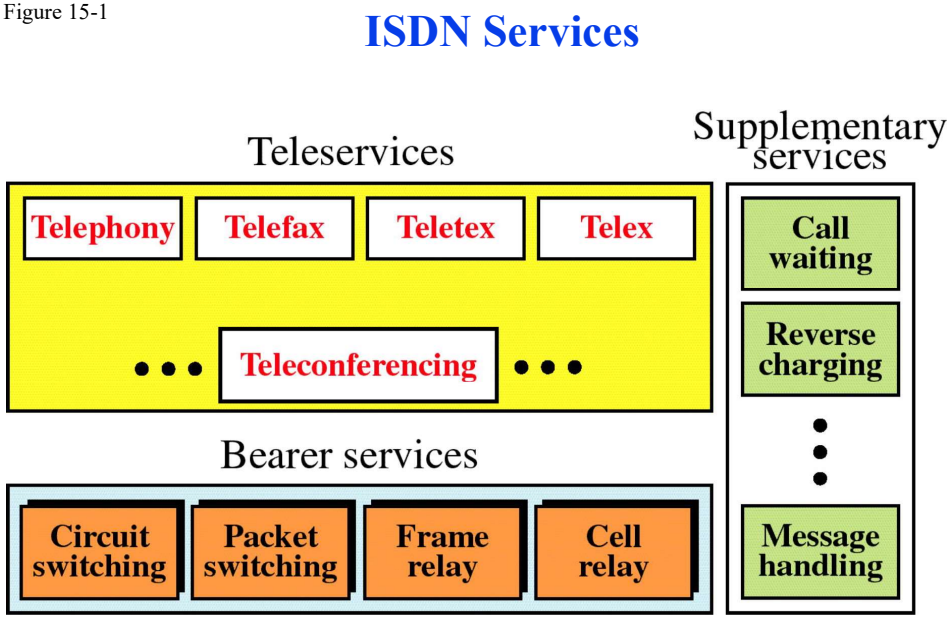


Figure 15-5

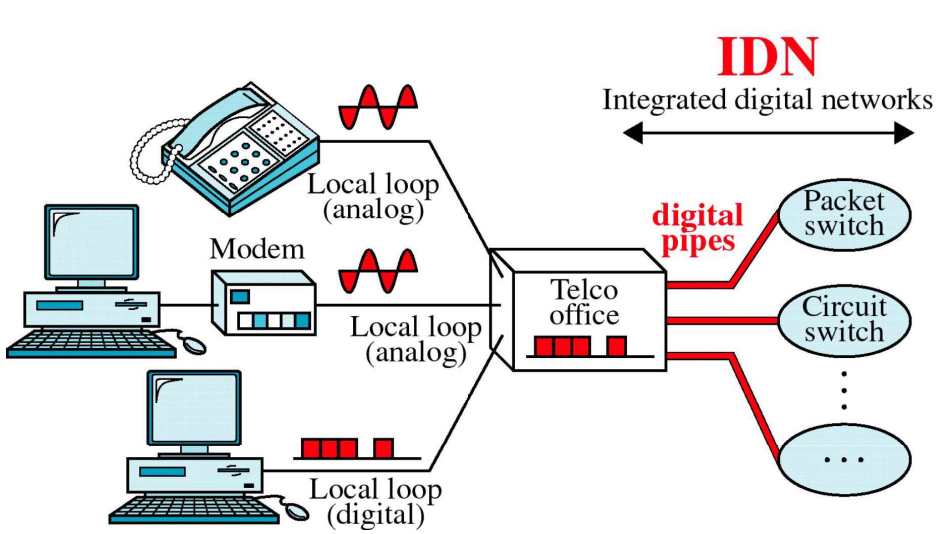
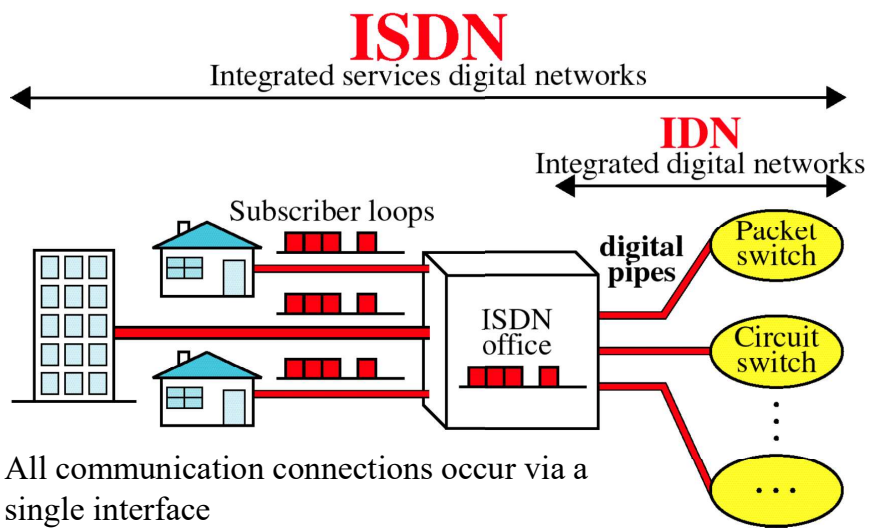


Figure 15-6

Integrated Services Digital Network



All communication connections occur via a single interface

Mobile Communication

Wireless Comes of Age

- Guglielmo Marconi invented the wireless telegraph in 1896
  - Communication by encoding alphanumeric characters in analog signal
  - Sent telegraphic signals across the Atlantic Ocean
- Communications satellites launched in 1960s
- Advances in wireless technology
  - Radio, television, mobile telephone, mobile data, communication satellites
- More recently
  - Wireless networking, cellular technology, mobile apps, Internet of Things

Cellular telephone

- Started as a replacement to the wired telephone
- Early generations offered voice and limited data
- Current third and fourth generation systems
  - Voice
  - Texting
  - Social networking
  - Mobile apps
  - Mobile Web
  - Mobile commerce
  - Video streaming

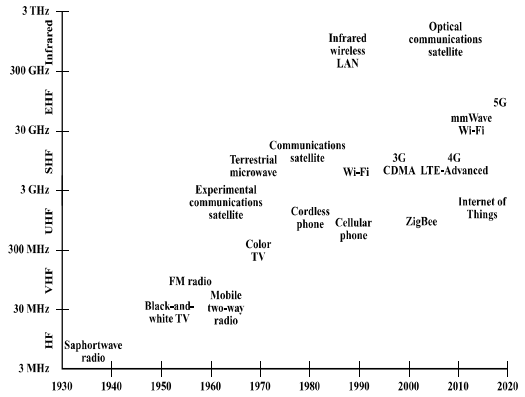
Cellular telephone

- Started as a replacement to the wired telephone
- Early generations offered voice and limited data
- Current third and fourth generation systems
  - Voice
  - Texting
  - Social networking
  - Mobile apps
  - Mobile Web
  - Mobile commerce
  - Video streaming

Wireless Impact

- Profound
- Shrinks the world
- Always on
- Always connected
- Changes the way people communicate
  - Social networking
- Converged global wireless network

Figure 1.1 Some Milestones in Wireless Communications



Global cellular network

- Growth
  - 11 million users in 1990
  - Over 7 billion today
- Mobile devices
  - Convenient
  - Location aware
  - Only economical form of communications in some places

Global cellular network

- Generations
  - 1G – Analog
  - 2G – Digital voice
    - Voice services with some moderate rate data services
  - 3G – Packet networks
    - Universal Mobile Phone Service (UMTS)
    - CDMA2000
  - 4G – New wireless approach (OFDM)
    - Higher spectral efficiency
    - 100 Mbps for high mobility users
    - 1 Gbps for low mobility access
    - Long Term Evolution (LTE) and LTE-Advanced

Mobile device revolution

- Originally just mobile phones
- Today's devices
  - Multi-megabit Internet access
  - Mobile apps
  - High megapixel digital cameras
  - Access to multiple types of wireless networks
    - Wi-Fi, Bluetooth, 3G, and 4G
  - Several on-board sensors
- Key to how many people interact with the world around them

Mobile device revolution

- Better use of spectrum
- Decreased costs
- Limited displays and input capabilities
- Tablets provide balance between smartphones and PCs
- Long distance
  - Cellular 3G and 4G
- Local areas
  - Wi-Fi
- Short distance
  - Bluetooth, ZigBee

Future trends

- LTE-Advanced and gigabit Wi-Fi now being deployed. LTE (Long-Term Evolution) is a fourth-generation (4G) wireless standard that provides increased network capacity and speed for cellphones and other cellular devices compared with third-generation (3G) technology.
- Machine-to-machine communications
  - The "Internet of Things"
  - Devices interact with each other
    - Healthcare, disaster recovery, energy savings, security and surveillance, environmental awareness, education, manufacturing, and many others
  - Information dissemination
    - Data mining and decision support
  - Automated adaptation and control
    - Home sensors collaborate with home appliances, HVAC systems, lighting systems, electric vehicle charging stations, and utility companies.
  - Eventually could interact in their own forms of social networking

Future trends

- Machine-to-machine communications
  - 100-fold increase in the number of devices
  - Type of communication would involve many short messages
  - Control applications will have real-time delay requirements
    - Much more stringent than for human interaction

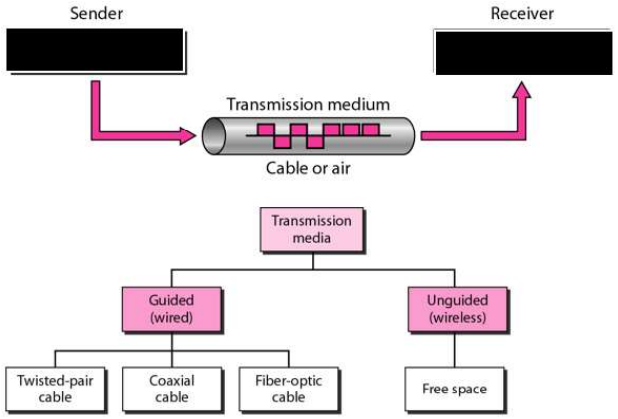
HNDIT2042
Data Communication and Computer Networks

Week 4 –*Internet - Access Methods-Part 2*

Communication channels and Transmission Media

- A communication channel is simply a medium through which a message is transmitted to its intended audience
- Transmission media describes the types of physical system used to carry a communication signal from one system to another.
- These can be **Physical** or **Wireless**

Transmission Media



Transmission Media

Physical Transmission Media

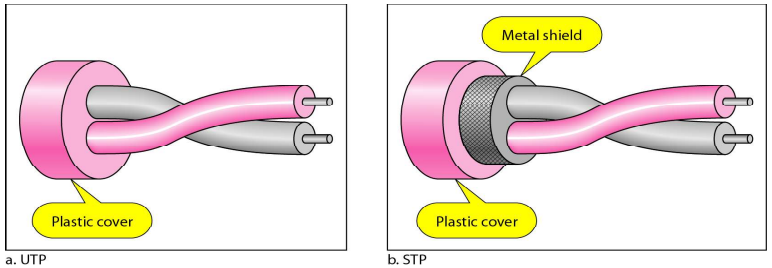
- These include wires, cables and any other tangible (touchable) materials used to send communication signals.
- These include;
  1. Twisted Pair cables
  2. Coaxial Cables
  3. Fibre optic cable

Twisted Pair Cables

- Consists of one or more pairs of insulated strands of copper wire twisted around one another
- The oldest, simplest, and most common type of conducted media is twisted pair wires.
- Importance of twists
  - Improve resistance to interference
  - Limit the influence of crosstalk

Twisted Pair Cables

- Two types.
  - Shielded Twisted Pair Cables (STP)
  - Unshielded Twisted Pair Cables (UTP)

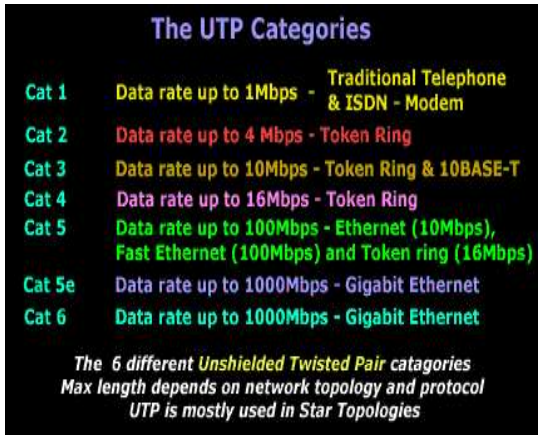


a. UTP b. STP

Unshielded twisted cable (UTP)

- These are the most popular type of cable around the world.
- They come in 6 different types, and depending on what you want to achieve, you will need to employee the appropriate type of cable.

- Contains one or more pairs of insulated wires within an enclosing insulating sheath
- Follows the ANSI/EIA/TIA 568 standard
- Prone to crosstalk



Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

UTP Characteristics

Table 3-4 10BaseT Ethernet characteristics

Characteristic	Value
Maximum cable length	100 meters (328 feet)
Bandwidth	10 Mbps
Bend radius	TP not subject to bend radius limitations
Installation/maintenance	Easy to install, no need to reroute; the most flexible
Cost	Least expensive of all cabling options
Connector type	RJ-45 for device and wall-plate connections
Interference rating	Low: most susceptible of all electrical cable types

Unshielded Twisted cable (UTP)

Note:

- Can be affected by interference as there is no protective metal shield

A device known as a Registered Jack (RJ) connectors are used to interface between UTP and the interface cards of a computer.

RJ-45 is an 8-position connector used for network cabling usually on Ethernet connections.

Characteristics of UTP

- Speed 10,100,1000 Mbps.
- Least expensive.
- Maximum cable length is 100 m.
- Media connector size is small.
- Easy to install

Shielded twisted Pair (STP)

Note:

They are more expensive compared to UTPs

Can't be affected by interference as they have a protective metal shield

- Encloses each pair of wires within a foil shield, as well as within an enclosing insulating sheath
- Supports higher bandwidth over longer distances than UTP
- Has no set of standards

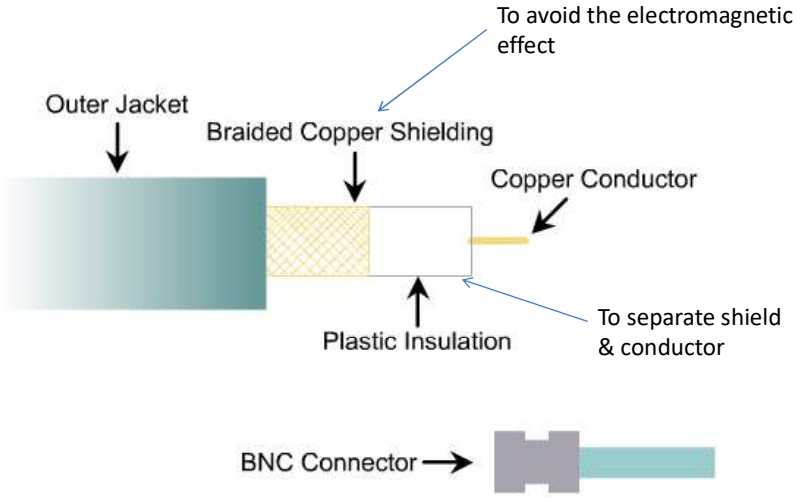
Characteristics of STP

- Speed 10-100 Mbps.
- Moderately expensive .
- Maximum cable length is 100 m.
- Similar in construction of the UTP.

More…

- Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.).
- If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution.

Coaxial cable



Coaxial cable

- has a single copper conductor at its center.
- A plastic layer provides insulation between the center conductor and a braided metal shield.
- The metal shield helps to block any outside interference .
- difficult to install.
- support greater cable lengths between network devices than twisted pair cable.

Coaxial cable

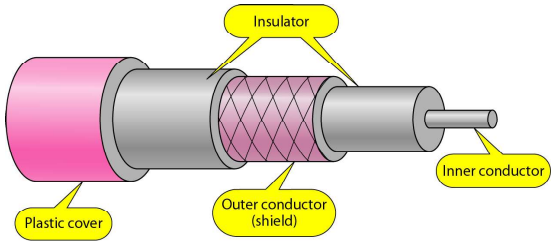
The two types of coaxial

- Thin coaxial cable is also referred to as thinnet.
  - 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals.
- Thick coaxial cable is also referred to as thicknet.
  - 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals.

Characteristics of Co –axial Cables

- Speed 10-100 Mbps.
- Inexpensive.
- Maximum cable length is 500 m.
- Can be run longer distances than shielded twisted pair(STP), unshielded twisted pair(UTP) without the need for repeaters.
- Media & connector size is Medium

Coaxial cable



Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Thinwire Ethernet Cable

Characteristic	Value
Maximum cable length	185 meters (607 feet)
Bandwidth	10 Mbps
Bend radius	360 degrees/ft
Installation/maintenance	Easy to install and reroute; flexible
Cost	Cheapest form of coax cable; prefabricated cables average $1/foot
Connector type	British Naval Connector* (BNC)
Interference rating	Good: lower than thicknet, higher than TP

Thickwire Ethernet Cable

Table 3-3 Thickwire Ethernet characteristics

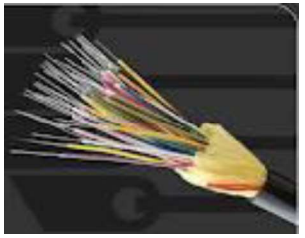
Characteristic	Value
Maximum cable length	500 meters (1640 feet)
Bandwidth	10 Mbps
Bend radius	30 degrees/ft
Installation/maintenance	Hard to install and reroute; rigid
Cost	More expensive than thinwire, cheaper than fiber
Connector type	BNC
Interference rating	Good: lowest of all electrical cable types

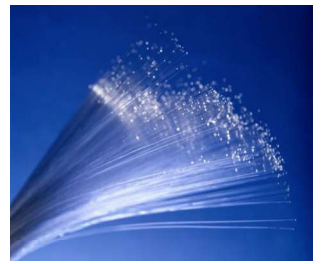
Fiber Optic Cables

- It's a network cable that contains strands of glass fibre inside an insulated casing.
- It consists of a centre glass core surrounded by several layers of protective materials. They are designed to carry data for long distances and at very high bandwidth (gigabit speed)
- They carry communications signals

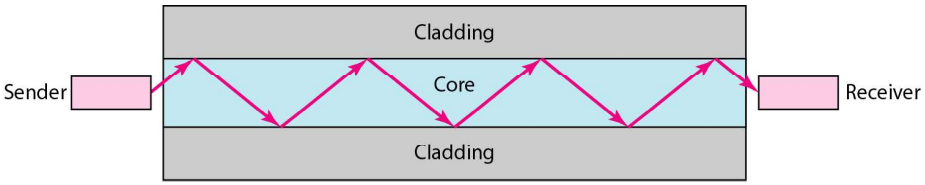
  using pulses of light rather than electronic

  signals (thereby eliminating the problem of electrical interference)





Optical fiber



Primary Types of Fiber-optic Cables

- Single-mode cables
  - Include only one glass fiber at the core
  - Cost more
  - Work with laser-based emitters but span the longest distances
- Multi-mode cables
  - Incorporate two or more glass fibers at the core
  - Cost less
  - Work with light emitting diodes (LEDs) but span shorter distances

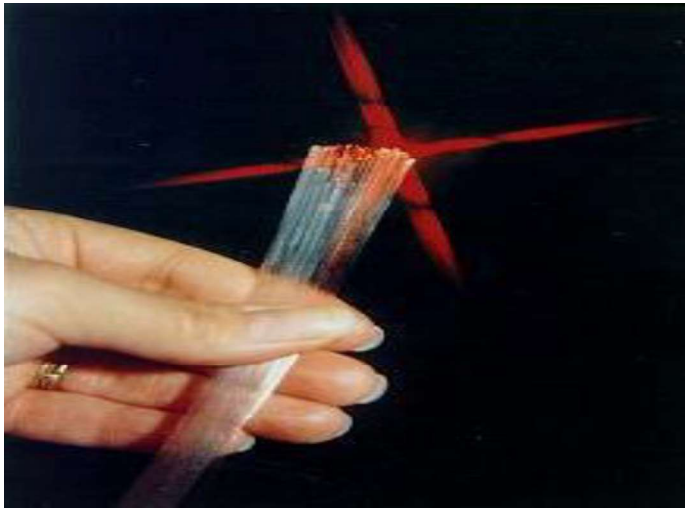
Fiber-optic Cable Advantages

- Immune to interference
- Highly secure; eliminates possibility of electronic eavesdropping
- Good medium for high-bandwidth, high-speed, long-distance data transmissions

Disadvantages of Fibre Optic Cables

1. Expensive as compared to other media
   —Buying and installation
2. Harder to install and modify.
   —Special equipment required
3. Physical Damage

Fiber optic



Fiber-optic Cable Characteristics

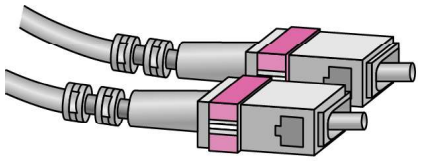
Table 3-5 Fiber-optic cable characteristics

Characteristic	Value
Maximum cable length	2 km (6562 feet)–100 km (62.14 miles)
Bandwidth	100 Mbps–1 Gbps
Bend radius	30 degrees/ft
Installation/maintenance	Difficult to install and reroute, sensitive to strain and bending
Cost	Most expensive of all cabling options
Connector type	Several types: ST, SC, MIC, and SMA
Interference rating	None: least susceptible of all cable types

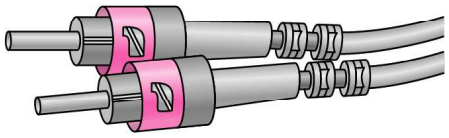
Fiber-optic Media Connectors

- ST (straight tip)
- SC (straight connection)
- MIC (medium interface connector)
- SMA (subminiature type A)

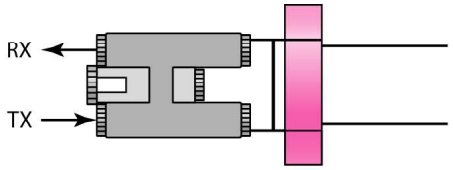
Fiber-optic Cable Connectors



SC connector



ST connector



MT-RJ connector

Comparison of General Cable Characteristics

Table 3-6 Comparison of general cable characteristics

Type	Maximum Length	Bandwidth	Installation	Interference	Cost
UTP	100m	10–100 Mbps	Easy	High	Cheapest
STP	100m	16–1000 Mbps	Moderate	Moderate	Moderate
10Base2	185m	10 Mbps	Easy	Moderate	Cheap
10Base5	500m	10 Mbps	Hard	Low	Expensive
Fiber	2–100 km	100 Mbps–10 Gbps	Very hard	None	Most expensive

General Cable Characteristics

- Bandwidth rating
- Maximum segment length
- Maximum number of segments per internetwork
- Maximum number of devices per segment
- Interference susceptibility
- Connection hardware
- Cable grade
- Plenum rating
- Bend radius
- Material costs
- Installation costs

Primary Techniques for Sending Signals across a Cable

- Baseband transmission
- Broadband transmission

Baseband Transmission

- Uses digital signals sent over a cable without modulation
- Sends binary values (0s and 1s) as pulses of different voltage levels
- Entire bandwidth of the cable is used to transmit a single data signal
- Limits any single cable strand to half-duplex transmission

continued

Baseband Transmission

- Signal flow can be bi-directional
- Uses repeaters to restore the signal to its original strength and quality before retransmitting it to another cable

Broadband Transmission

- An analog transmission technique which may use multiple communication channels simultaneously
- Each data channel is represented by modulation on a particular frequency band, for which sending or receiving equipment must be tuned
- Signal flow is one-way only; two channels are necessary for computers to send/receive data

continued

Broadband Transmission

- Uses amplifiers to detect weak signals, strengthen those signals, and then rebroadcast them
- Primary approaches to supporting two-way broadband communications
  - Mid-split broadband
  - Dual-cable broadband
- Offers higher bandwidths, but generally more expensive than baseband systems

The Importance of Bandwidth

- The faster the connection, the better

Cable Selection Criteria

- Bandwidth
- Budget
- Capacity
- Environmental considerations
- Placement
- Scope
- Span

Transmission Media

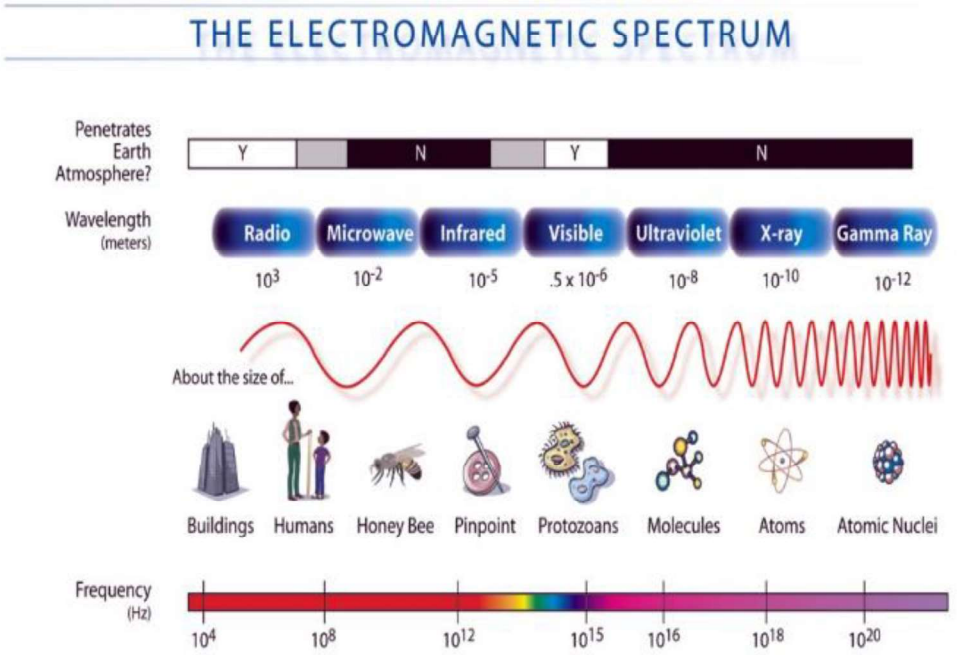
- Wireless Media-Intangible Media
  - Depends on transmission at some kind of electromagnetic frequency through the atmosphere to carry data transmissions from one networked device to another
  - Appears most frequently in conjunction with wired networks

Capabilities of the Wireless World

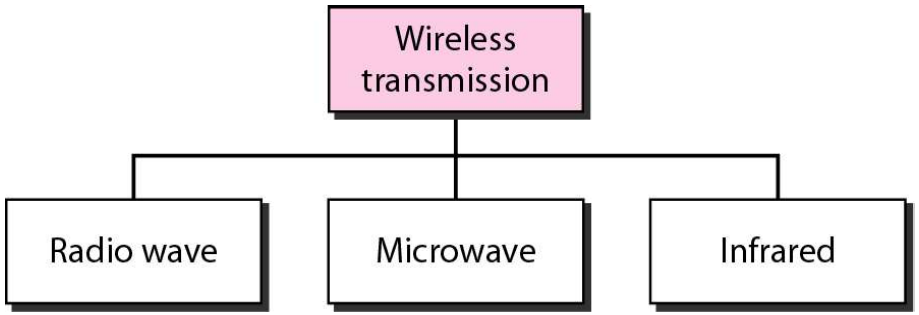
- Creates temporary connections to existing wired networks
- Establishes back-up or contingency connectivity for existing wired networks
- Extends a network's span beyond the reach of wire- or fiber-optic-based cabling
- Permits certain users to roam with their machines, within certain limits

Wireless Media

- Transmission of waves take place in the electromagnetic (EM) spectrum.
- The carrier frequency of the data is expressed in cycles per second called hertz(Hz).
- Low frequency signals can travel for long distances through many obstacles but can not carry a high bandwidth of data
- high frequency signals can travel for shorter distances through few obstacles and carry a narrow bandwidth.
- Also the noise effect on the signal is inversely proportional to the power of the radio transmitter.



Wireless Transmission Waves



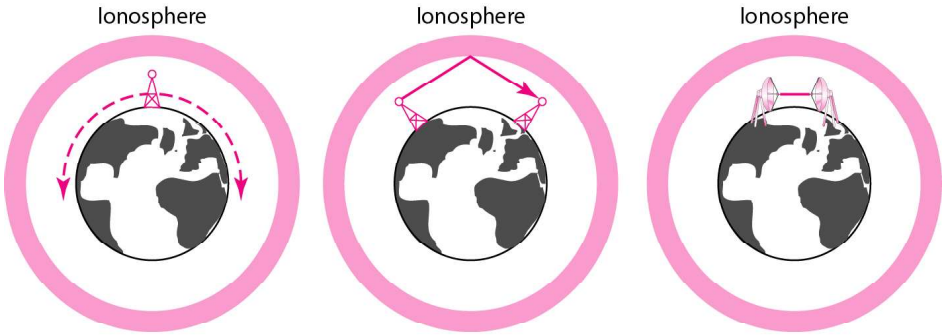
Different types of wireless communication media

- Radio waves
  - used for cellular networks, Wi-Fi, Bluetooth, and other wireless communication technologies.
- Microwave
  - cellular networks, Wi-Fi networks, and satellite communications.
- Infrared
  - used for remote controls and some short-range communication

Wireless Propagation

- Signal travels along three routes
  - Ground wave
    - Follows contour of earth
    - Up to 2MHz
    - AM radio
  - Sky wave
    - Amateur radio, BBC world service, Voice of America
    - Signal reflected from ionosphere layer of upper atmosphere
  - Line of sight
    - Above 30Mhz
    - May be further than optical line of sight due to refraction

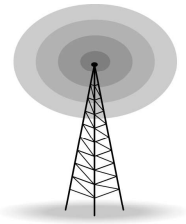
Propagation Methods



Antenna

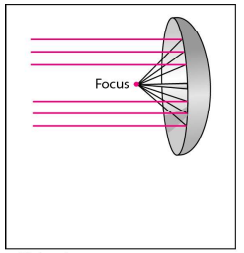
Omni directional Antenna

Radio waves are used for multicast communications, such as radio and television,

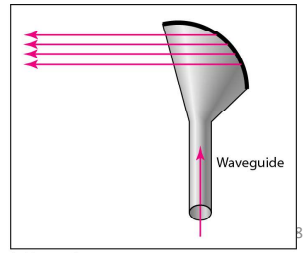


Unidirectional Antennas

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.



a. Dish antenna



b. Horn antenna

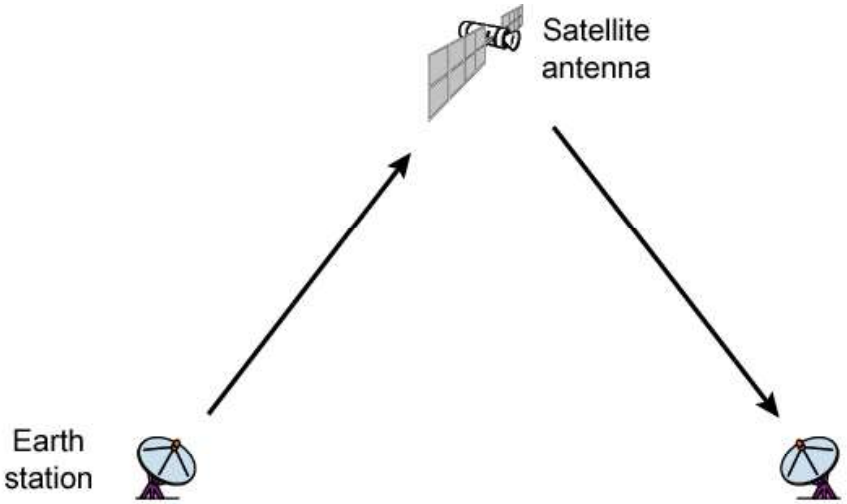
Terrestrial Microwave

- Parabolic dish
- Focused beam
- Line of sight
- Long haul telecommunications
- Higher frequencies give higher data rates

Satellite Microwave

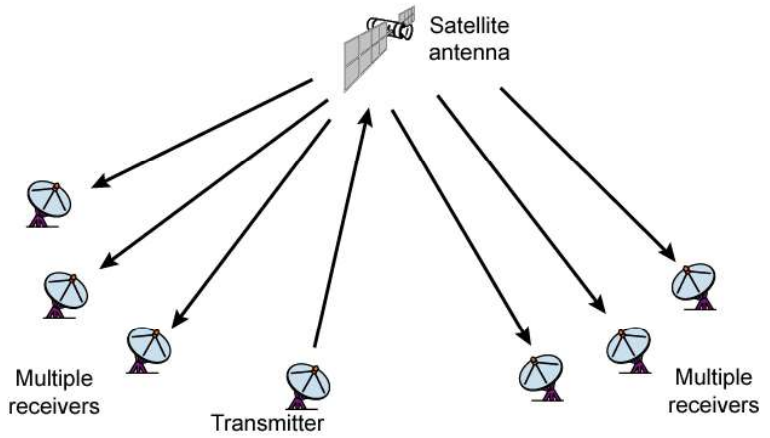
- Satellite is relay station
- Satellite receives on one frequency, amplifies or repeats signal and transmits on another frequency
- Requires geo-stationary orbit
  - Height of 35,784km
- Television
- Long distance telephone
- Private business networks

Satellite Point to Point Link



(a) Point-to-point link

Satellite Broadcast Link



(b) Broadcast link

Advantages of Wireless Communication

- Mobility
- Flexibility
- Cost-effectiveness
- Easy installation and setup

Challenges of Wireless Media

- Interference: radio waves can be disrupted by physical obstacles, other devices, or environmental factors.
- Security: wireless transmissions can be intercepted or hacked if not properly secured.
- Speed: wireless networks may not be as fast as wired networks.

Applications of wireless media

- Cellular networks: allow for mobile phone communication over long distances.
- Wi-Fi: allows for wireless internet access in homes, offices, and public spaces.
- Bluetooth: allows for short-range device connectivity, such as wireless headphones or speakers.
- GPS: allows for location tracking and navigation.

Proxy Server

- A proxy server is an intermediary server that acts as a gateway between a client computer and another server.
- When a client computer requests resources from another server, it sends the request to the proxy server instead of directly to the target server.
- The proxy server then forwards the request to the target server on behalf of the client.

Proxy Server

- A proxy server is an intermediary server that acts as a gateway between a client computer and another server.
- When a client computer requests resources from another server, it sends the request to the proxy server instead of directly to the target server.
- The proxy server then forwards the request to the target server on behalf of the client.

Why Proxy Server?

- Anonymity: By using a proxy server, the client's IP address is hidden from the target server, providing some level of anonymity.
- Content Filtering: Proxy servers can be used to filter content, blocking access to certain websites or types of content.
- Cache: Proxy servers can cache frequently accessed resources, improving the speed of access for clients.
- Security: Proxy servers can be used to filter out malicious traffic, providing an extra layer of security.

IoT (Internet of things)

"

Content

1. Introduction
2. Benefits of IoT
3. Application and use of IoT
4. IoT challenges
5. What needs to be done?
6. Top IoT technologies and trends
7. Future of IoT
8. Q&A

Introduction – what is IoT?

- The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction - ***IoTAgenda***
- A ***thing*** in the IoT can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.
- IoT is a sensor network of billions of *smart devices* that connect people, systems and other applications to collect and share data.

Why IOT?

- Organizations in a *variety of industries* are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

IoT ecoystem

- An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments.
- IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally.

Top 10 Strategic IoT Technologies and Trends - GARTNER

1) **Trend No. 1: Artificial Intelligence (AI):** "Data is the fuel that powers the IoT and the organization's ability to derive meaning from it will define their long term success."
2) **Trend No. 2: Social, Legal and Ethical IoT:** These include ownership of data and the deductions made from it, algorithmic bias, privacy and compliance with regulations such as the General Data Protection Regulation. "Successful deployment of an IoT solution demands that it's not just technically effective but also socially acceptable."
3) **Trend No. 3: Infonomics and Data Broking:** The theory of infonomics takes monetization of data further by seeing it as a strategic business asset to be recorded in the company accounts. By 2023, the buying and selling of IoT data will become an essential part of many IoT systems.

Top 10 Strategic IoT Technologies and Trends – GARTNER (cont'd)

4) **Trend No. 4: The Shift from Intelligent Edge to Intelligent Mesh:** The shift from centralized and cloud to edge architectures is well under way in the IoT space. These mesh architectures will enable more flexible, intelligent and responsive IoT systems — although often at the cost of additional complexities.
5) **Trend No. 5: IoT Governance:** As the IoT continues to expand, the need for a governance framework that ensures appropriate behaviour in the creation, storage, use and deletion of information related to IoT projects will become increasingly important.
6) **Trend No. 6: Sensor Innovation:** The sensor market will evolve continuously through 2023. New sensors will enable a wider range of situations and events to be detected.

Top 10 Strategic IoT Technologies and Trends – GARTNER (cont'd)

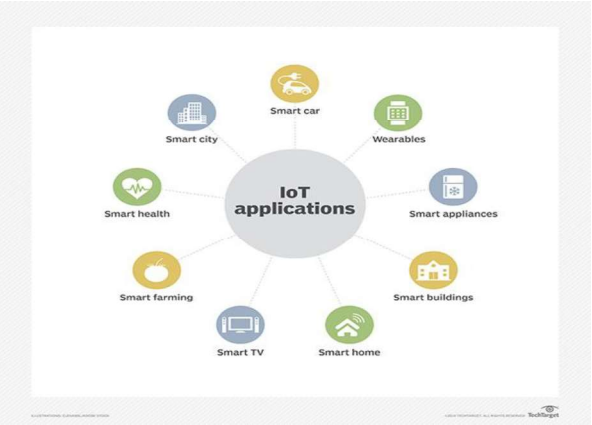
7) **Trend No. 7: Trusted Hardware and Operating System:** '.. by 2023, we expect to see the deployment of hardware and software combinations that together create more trustworthy and secure IoT systems…'.
8) **Trend 8: Novel IoT User Experiences:** User experience driven by 4 factors**:** new sensors, new algorithms, new experience architectures and context, and socially aware experiences.
9) **Trend No. 9: Silicon Chip Innovation:** By 2023, it's expected that new special-purpose chips will reduce the power consumption required to run IoT devices.
10) **Trend No. 10: New Wireless Networking Technologies for IoT:** IoT networking involves balancing a set of competing requirements. In particular they should explore 5G, the forthcoming generation of low earth orbit satellites, and backscatter networks.

Benefits of IoT

IoT offers a number of benefits to organizations, enabling them to:

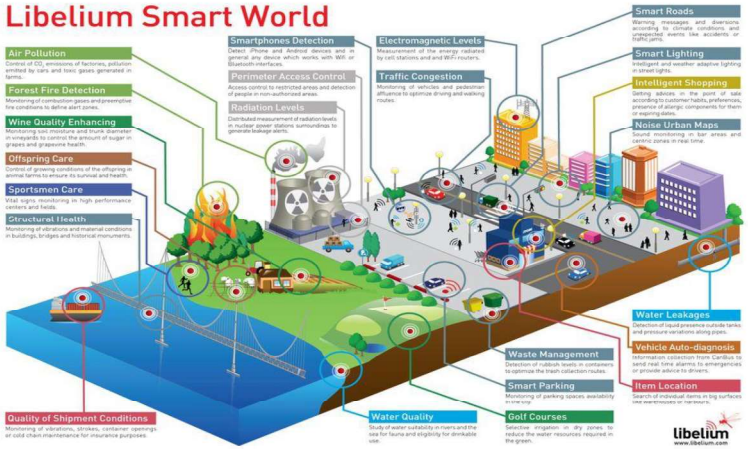
1. Monitor their overall business processes;
2. Improve the customer experience;
3. Save time and money;
4. Enhance employee productivity;
5. Integrate and adapt business models;
6. Make better business decisions; and
7. Generate more revenue.

Consumer and enterprise IoT applications



Source: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

The smart world of the future – using Iot



Source: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#ef2433f1d091

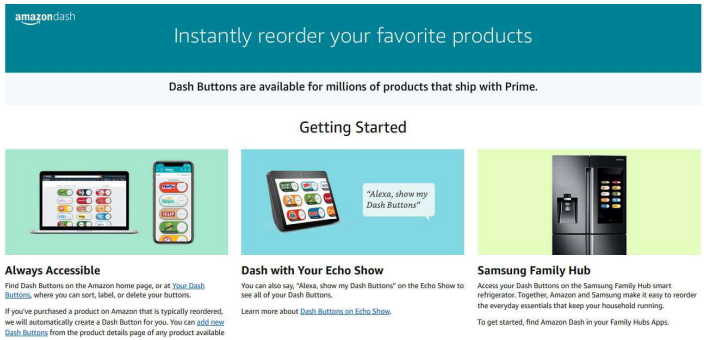
Sample: consumer iot products & Services

1. Helmet Concussion Sensor
2. Medical Alert Watch
3. Smart Fitness Clothing and Smart Running Shoes
4. **One-Button Product Purchases:** "Order at the click of a button!" Amazon has taken that phrase literally and produced physical branded buttons called *Amazon Dash* that link to products in your home. Say you run out of laundry powder. You can press your Dash button for Tide and Amazon will reorder your Tide Powder product for you. No need to sign onto the Web, fumble with payment methods, or retype credit card numbers.
5. Garden Sensors
6. Smart Televisions

Helmet concussion sensor

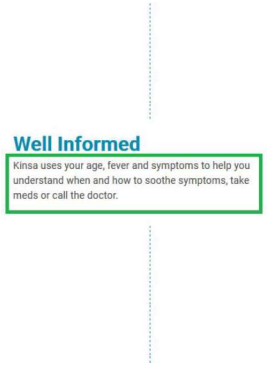
https://www.amazon.com/Shockbox-LM2004-EXT-MultiSport-Helmet-Sensor/dp/B00DVHA1LM?imprToken=NXcTrCppNfgrAo2MA1K7ig&slotNum=2&SubscriptionId=AKIAIO22DD3AFUSKXUKQ&tag=makeusw-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=B00DVHA1LM

Amazon DASH



https://www.amazon.com/b?ie=UTF8&node=17729534011

Kinsa thermometer



Monitoring your temperature and can call your doctor as necessary

Smart farming: Use of iot to improve agriculture

- In IoT-based smart farming, a system is built for monitoring the crop field with the help of sensors (light, humidity, temperature, soil moisture, etc.) and automating the irrigation system. The farmers can monitor the field conditions from anywhere. This is highly efficient compared to the traditional/conventional approach.
- In terms of environmental issues, IoT-based smart farming provides great benefits including: better and efficient water usage, and optimization of inputs and treatments.
- Therefore, smart farming based on IoT technologies enables growers and farmers to reduce waste and enhance productivity.
- Some of the IoT applications in this area are:
  i. Precision farming
  ii. Agricultural drones
  iii. Livestock monitoring
  iv. Smart greenhouses

Industrial Iot (iiot)

- Industrial IoT (IIoT) focusses on the use of cyber-physical systems to monitor the physical factory processes and make data-based automated decisions.
- While the physical systems are made the intelligent using IoT, the real-time communication, and cooperation both with each other and with humans is established via the wireless web
- IIoT brings in the concept of 'a *connected factory leads to a smart factory*'.

Iiot in manufacturing

1. **Digital/connected factory**: IoT enabled machinery can transmit operational information to the partners like original equipment manufacturers and to field engineers.
2. **Facility management:** The use of IoT sensors in manufacturing equipment enables condition-based maintenance alerts.
3. **Production flow monitoring:** IoT in manufacturing can enable the monitoring of production lines starting from the refining process down to the packaging of final products.
4. **Inventory management:** IoT applications permit the monitoring of events across a supply chain.

Iiot in manufacturing (cont'd)

5. **Plant Safety and Security:** IoT combined big data analysis can improve the overall workers' safety and security in the plant. .
6. **Quality control:** IoT sensors collect aggregate product data and other third-party syndicated data from various stages of a product cycle.
7. **Packaging Optimization**: By using IoT sensors in products and/or packaging, manufacturers can gain insights into the usage patterns and handling of product from multiple customers.
8. **Logistics and Supply Chain Optimization**: The Industrial IoT (IIoT) can provide access to real-time supply chain information by tracking materials, equipment, and products as they move through the supply chain.

IOT CHALLENGES

Security, privacy and data sharing issues

- Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. And manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.
- However, hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.
- Challenges with IIoT:
  i. Security of data – same as above
  ii. Reliability and stability – of IIoT sensors
  iii. Connectivity of all the systems in IIoT setup – no maintenance envisioned?
  iv. Blending legacy systems – IIoT is new in the market

P Class	Default Subnet	Network bits	Host bits	Total hosts	Valid hosts
A	255.0.0.0	First 8 bits	Last 24 bits	16, 777, 216	16, 777, 214
B	255.255.0.0	First 16 bits	Last 16 bits	65,536	65,534
C	255.255.255.0	First 24 bits	Last 8 bits	256	254

CIDR [Classless Inter Domain Routing]

CIDR is a slash notation of subnet mask. CIDR tells us number of on bits in a network address.

- **Class A has default subnet mask 255.0.0.0. that means first octet of the subnet mask has all on bits. In slash notation it would be written as /8, means address has 8 bits on.**
- **Class B has default subnet mask 255.255.0.0. that means first two octets of the subnet mask have all on bits. In slash notation it would be written as /16, means address has 16 bits on.**
- **Class C has default subnet mask 255.255.255.0. that means first three octets of the subnet mask have all on bits. In slash notation it would be written as /24, means address has 24 bits on.**

Class C Subnetting

Default subnet mask of class C is 255.255.255.0. CIDR notation of class C is /24, which means 24 bits from IP address are already consumed by network portion and we have 8 host bits to work with. We cannot skip network bit, when we turned them on. Subnetting moves from left to right. So Class C subnet masks can only be the following:

CIDR	Decimal	Binary
/25	128	10000000
/26	192	11000000
/27	224	11100000
/28	240	11110000
/29	248	11111000
/30	252	11111100

One of the addresses in a block is 167.199.170.82/27. Find the number of addresses in the network, the first address, and the last address.

Solution

The value of n is 27. The network mask has twenty-seven 1s and five 0s. It is 255.255.255.240.

a. The number of addresses in the network is 232 − n = 32.

b. We use the AND operation to find the first address (network address). The first address is 1

Address in binary:	10100111 11000111 10101010 01010010
Network mask:	11111111 11111111 11111111 11100000
First address:	10100111 11000111 10101010 01000000

67.199.170.64/27.

/28

CIDR /28 has subnet mask 255.255.255.240 and 240 is 11110000 in binary. We used four host bits in network address.

N = 4
H = 4
Total subnets (2^N) :- $2^4 = 16$
Block size (256 - subnet mask) :- 256 - 240 = 16
Valid subnets (Count blocks from 0) :-0,16,32,48,64,80,96,112,128,144,160,176,192,208,224,240
Total hosts (2^H) :- $2^4 = 16$
Valid hosts per subnet (Total host - 2) :- 16 - 2 = 14

Network ID

First address of subnet is called network ID. This address is used to identify one segment or broadcast domain from all the other segments in the network.

Block Size

Block size is the size of subnet including network address, hosts addresses and broadcast address.

Broadcast ID

There are two types of broadcast, direct broadcast and full broadcast.

1. **Direct broadcast or local broadcast** is the last address of subnet and can be hear by all hosts in subnet.
2. **Full broadcast** is the last address of IP classes and can be hear by all IP hosts in network. Full broadcast address is 255.255.255.255

The main difference between direct broadcast and full broadcast is that routers will not propagate local broadcasts between segments, but they will propagate directed broadcasts.

IP Addressing(IPv4) & Subnetting

Static IP Address

- A static IP address is explicitly allocated to a device rather than one that a DHCP server has assigned. Because it does not change, it is called static.
- Static IP addresses can be configured on routers, phones, tablets, desktops, laptops, and any other device that can use an IP address. This can be done either by the device itself handing out IP addresses or by manually typing the IP address into the device.

Dynamic IP Address

- Dynamic IP address that you can use for a limited time. If a dynamic address isn't in use, it can be allocated to another device automatically. DHCP or PPPoE are used to assign dynamic IP addresses.

IP addresses –IPv4

- The IP Address identifies a system's location on the network in the same way a street address identifies a house on a city block
- Just as a street address must identify a unique residence, an IP address must be unique and have uniform format
- Each IP address has two parts
  - Network ID
  - Host ID

Network ID

- Identifies a physical network
- All hosts on the same network require the same network ID, which should be unique to the internet work

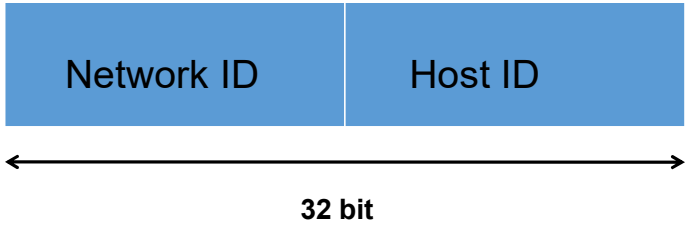
Host ID

- Identifies a workstation, server, router or other TCP/IP host within a network
- Host ID must unique to the network ID

Network ID & Host ID

- There are two formats for referencing an IP address
  - Binary
  - Dotted decimal notation
- Each IP address is 32 bits long and is composed of four 8 bit fields, called octets
- Octets are separated by periods and represent a decimal number in the range 0-255
- The 32 bits of the IP address are allocated to the network ID & host ID
- The human readable format of an IP address is referred to as dotted decimal notation

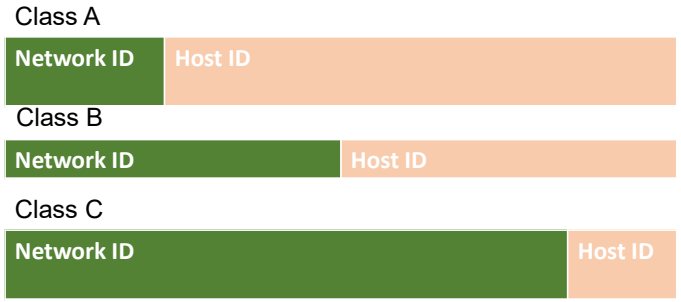
IP address



Eg. 131.107.3.24

Classes of IP address

Class	IP address	Network ID	Host ID
A	**w.x.y.z**	**w**	**x.y.z**
B	**w.x.y.z**	**w.x**	**y.z**
C	**w.x.y.z**	**w.x.y**	**z**



Classes of IP Address

- Class A
  - Class A addresses are assigned to networks with a very large number of hosts
  - The high order bit in a class A address is always set to zero.
  - The next 7 bits complete the network ID
  - The remaining 24 bits represent the host ID
  - Allows 126 networks
  - Approximately 17 millions hosts per network

Classes of IP Address

- Class B
  - Class B addresses are assigned to medium sized to large networks
  - The two high order bit in a class B address is always set to binary 1 0.
  - The next 14 bits complete the network ID
  - The remaining 16 bits represent the host ID
  - Allows 16384 networks
  - Approximately 65000 hosts per network

Classes of IP Address

- Class C
  - Class C addresses are used for small networks
  - The three order bit in a class A address is always set to binary 1 1 1 0.
  - The next 21 bits complete the network ID
  - The remaining 8 bits represent the host ID
  - Allows 2 million networks
  - Approximately 254 hosts per network

Note:

- **The network ID cannot be 127**

Classes of IP address

Class	Number of Networks	Number of Hosts per network
A (0-127)	**126 (2^7 - 2)**	**16,777,214 (2^{24} - 2) 16 million**
B (128-191)	**16382 (2^{14} - 2)**	**65534 (2^{16} - 2)**
C (192-223)	**2,097,150 (2^{21} - 2) 2Million**	**254 (2^8 - 1)**

Class A	Network ID 0_ _ _ _ _ _ _	Host ID (24 bits)
Class B	Network ID 10 _ _ _ _ _ _._ _ _ _ _ _ _ _	Host ID(16 bits)
Class C	Network ID 110_ _ _ _ _ . _ _ _ _ _ _ _ _ . _ _ _ _ _ _ _ _	Host ID (8 bits)

IP Address

- Public
- Private

- Dynamic
- static

Subnet mask

- The subnet mask used in the TCP/IP configuration for a network tells the OS which part of an IP address is the network portion and which part identifies the host.
- Using a subnet mask, a computer or other device can know if an IP address of another computer is on its network or another network

Packets in network

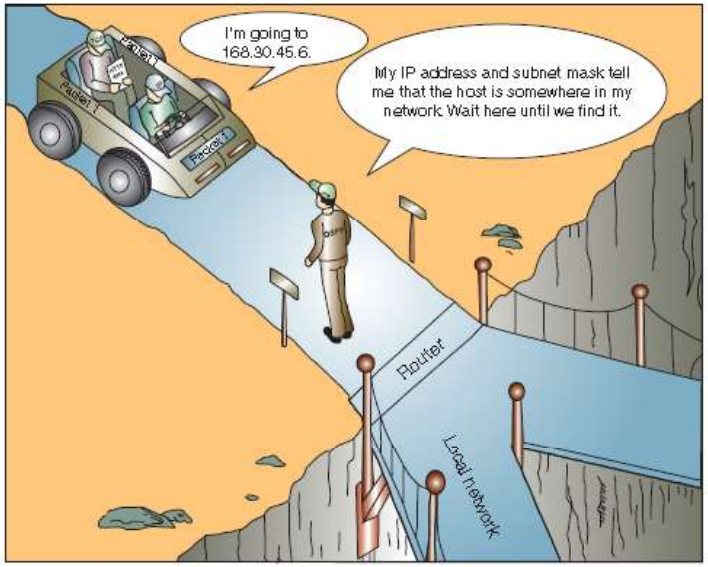


Figure 17-37 A host (router, in this case) can always determine if an IP address is on its network

Subnet mask

- A subnet mask is a group of ones followed by a group of zeros.
- The ones in a subnet mask say, “On our network, this part of an IP address is the network part,”
- and the group of zeros says, “On our network, this part of an IP address is the host part.”

Class	Subnet Mask	Address	Network ID	Host ID
Class A	11111111.00000000.00000000.00000000	89.100.13.78	89	100.13.78
Class B	11111111.11111111.00000000.00000000	190.78.13.250	190.78	13.250
Class C	11111111.11111111.11111111.00000000	201.18.20.208	201.18.20	208

Table 17-5 Default subnet masks for classes of IP addresses

Subnet mask

These three subnet masks would be displayed in a TCP/IP configuration window like this:

- Subnet mask of 11111111.00000000.00000000.00000000 is displayed as 255.0.0.0
- Subnet mask of 11111111.11111111.00000000.00000000 is displayed as 255.255.0.0
- Subnet mask of 11111111.11111111.11111111.00000000 is displayed as 255.255.255.0

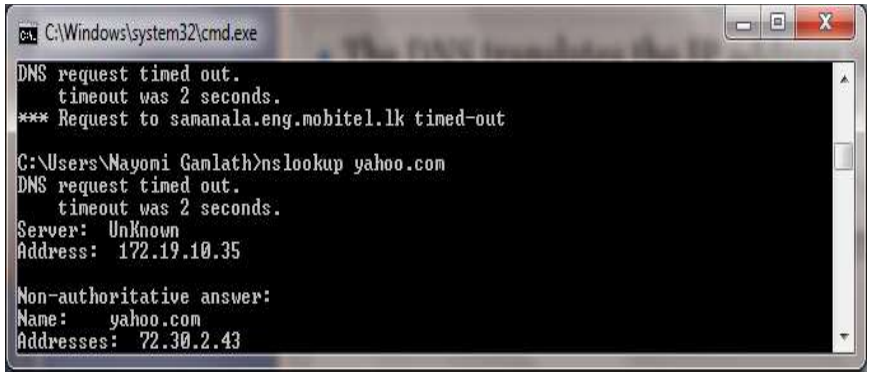
- Subnet masks that contain all ones or all zeros in an octet are called **classful subnet masks**
- the three subnet masks shown above are classful subnet masks.
- A **classless subnet mask can** have a mix of zeros and ones in one octet such as 11111111.11111111.11110000.00000000, which can be written as 255.255.240.0.
- These types of classless subnet masks are used to segment large corporate networks into sub networks, or subnets

Gateway

- a computer or a network that allows or controls access to another computer or network (telecommunication)
- a link between two computer programs allowing them to share information and bypass certain protocols on a host computer(computer program)

DNS- Domain Name System

- The DNS translates the IP address into the domain name and domain name into the IP address.
- The list of the IP addresses and the domain names are distributed throughout the internet.
- Example :www.yahoo.com



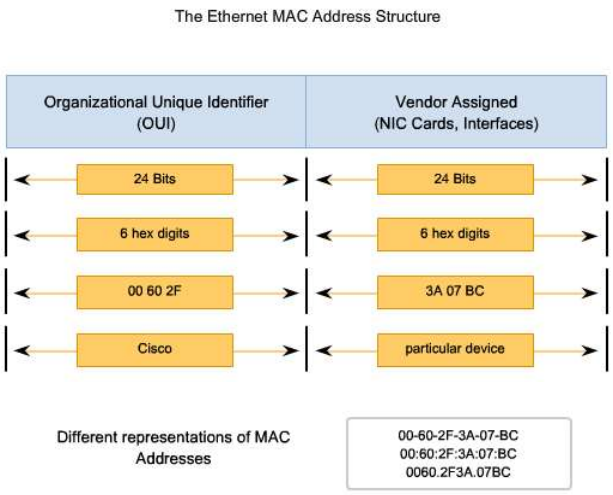
Internet Protocol version 6 (IPv6)

- IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2128, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) .
- An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Components in Address format :
- There are 8 groups and each group represents 2 Bytes (16-bits).
- Each Hex-Digit is of 4 bits
- Delimiter used – colon (:)

MAC Address (Physical Address)

- All devices connected to an Ethernet LAN have MAC-addressed interfaces.
- Different hardware and software manufacturers might represent the MAC address in different hexadecimal formats
- The address formats might be similar to 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, or 0005.9A3C.7800.
- MAC addresses are assigned to workstations, servers, printers, switches, and routers - any device that must originate and/or receive data on the network.

MAC address



Network Protocols

Protocols

- In order for computers to communicate with one another, they must agree on a set of rules for who says what, when they say it, and what format they say it in
- This set of rules is a protocol
- Different programs can use different protocols
- Protocols may be in ASCII (characters) or in binary
- Some common protocols are HTTP (for web pages), FTP (for file transfer), and SMTP (Simple Mail Transfer Protocol)

TCP/IP

- The Internet (and most other computer networks) are connected through TCP/IP networks
- TCP/IP is actually a combination of two protocols:
  - IP, Internet Protocol, is used to move packets (chunks) of data from one place to another
    - Places are specified by IP addresses: four single-byte (0..255) numbers separated by periods
    - Example: 192.168.1.1
  - TCP, Transmission Control Protocol, ensures that all necessary packets are present, and puts them together in the correct order
- TCP/IP forms a "wrapper" around data of *any* kind
- The data uses its own protocol, for example, FTP

TCP

- TCP (Transmission Control Protocol)
  - Datagrams
  - Connection Oriented
  - End to End error checking
  - Source Port, Destination Port
    - Sockets, Well Known Ports
  - HTTP, SMTP, TELNET,FTP

UDP (user datagram protocol)

- Connectionless
- One Way
- Fast, Simple
- No guarantee of delivery
- NFS, DNS, DHCP, NTP, TALK

ICMP (Internet control message protocol)

- Error Messages
- Intended for the TCP/IP software itself
- PING (host unreachable messages)
- Simple Headers

Application Protocols

- SMTP: Simple Mail Transport Protocol
- HTTP: Hyper Text Transport Protocol
- HTTPS: Hyper Text Transport SSL (Secure)
- SNMP: Simple Network Management Protocol
- FTP: File Transfer Protocol
- Telnet: Interactive login
- SSH: Secure Shell telnet
- DNS: Domain Name Service

FTP

- File Transfer Protocol (TCP)
  - User authentication
  - Anonymous
- used to transfer computer files between a client and server on a computer network.
- built on a client-server model architecture and uses separate control and data connections between the client and the server.
- GET/PUT/DEL/CWD

client-server

- Client-server is a relationship in which one program, the client, requests a service or resource from another program, the server. The label client-server was previously used to distinguish distributed computing by PCs from the monolithic, centralized computing model used by mainframes.
- Client –server communicating protocols: HTTP, HTTPS

HTTP

- Hyper text Transfer Protocols
- HTTP is a pull protocol, the user pulls information from a remote site.
- Protocol consists of GET and POST commands to transfer data.

HTTPS

- Secure communication over a computer network
- HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer.
- The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Email Client

- Email clients are web-based or desktop apps that allow you to manage email accounts from different email service providers.
- Outlook, for example, also has a desktop version that allows you to connect @outlook accounts and email accounts provided by other hosting platforms.
- **Emails are accessible without internet access.** Email clients allow you to access an "offline" feature, which allows you to view, reply or write professional emails without being connected to the internet on your desktop or mobile. Webmail does offer this but this is a built-in feature for desktop email clients. But you'll only have access to your emails that were updated before you disconnect from the internet so keep that in mind.
- **Easily customize your email client.** Unlike webmail, most email clients allow you to customize the layout, color and other features so the user experience is more personalized.
- **Emails can be backed up to the computer**

Email Gateway

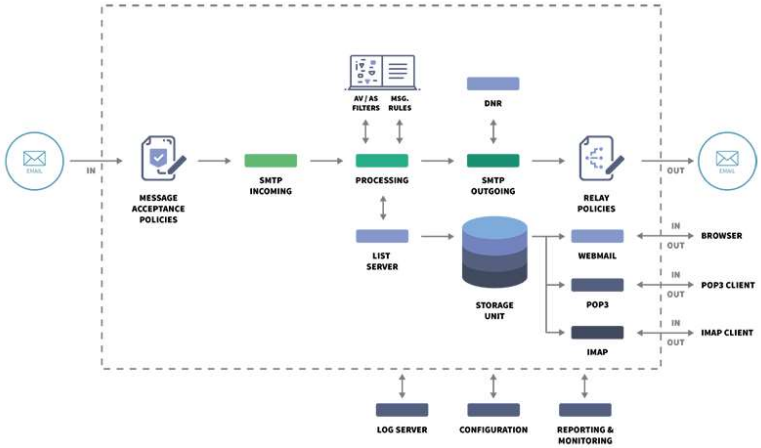
- **Email Gateway**, or a **Secure Email Gateway (SEG)**, is a mail server that analyzes an organization's incoming and outgoing emails before they reach the internal mail server. All emails pass through this Email Gateway and are checked for potential security threats. An Email Gateway, hence, acts as a firewall for emails.

Email Server

- An email server, also called a mail server, is essentially a computer system that sends and receives emails. When you send an email, it goes through a series of servers to reach its final destination. While this process is lightning fast and efficient, there is a significant amount of complexity behind sending and receiving emails.

- Email communication involves complex protocols and processes. Usually, the email server is a computer or machine that has a complete system with different applications or services. Based on the type of action they perform, email servers can be categorized into incoming and outgoing email servers.

How Does An Email Server Work?



Why Use Desktop Email Clients?

- Easily Manage Multiple Emails (with Different Domains)
- Access Your Email Offline
- Security Features and Encryption
- Seamlessly Integrate With Desktop Apps

Webmail

- A webmail is a web-based email service that allows you to use email features using your website browser.
- Most email services provide a webmail app as an interface for managing email. But you can only manage emails associated with this particular email service. For example, Gmail's webmail allows you to manage Gmail accounts only.
- This email provider can be a third party or a site provided by your ISP. You can access email features, and the website provider provides extensions.

Features of Webmail

- Easy access without downloading software. Unlike email clients that you have to download to access, you can use a webmail provider without the need for software installation.
- Access emails only via the internet. As the name suggests, "web" mail can only be accessed via your webmail website browser. This means that you'll always need an internet connection in order to access the full features of your emails.
- Access emails within your web browser. Webmail allows you to access your emails when browsing your website provider, for example, Google and Gmail.
- Emails can be backed up in the email server. Webmails are automatically backed up by the email server or website provider, so you don't have to manually backup your emails.
- Emails are automatically scanned for viruses by the service provider. When using webmail your emails and their attachments are automatically scanned by the website service provider.

SMTP

Simple Mail Transfer Protocol

- The protocol is very simple
- SMTP is a push protocol, information is pushed to a remote site
- Uses port 25

POP3

- Post Office Protocol 3
- Most recent version of a standard protocol for receiving e-mail.
- Mail access client
- Uses port 110
- Messages are downloaded to client but can be stored on server.
- Does not easily allow multiple clients

IMAP

- Internet Mail Access Protocol
- Improved POP3
- Automatically assigns folders
- Leaves mail on server
- Only transfers as much as needed per message (headers, subject only on list)

DHCP

- If you have a web site, it must be hosted on a computer that is "permanently" on the Web
  - This computer must have a permanent IP address
  - There aren't enough IP addresses for the number of computers there are these days
- If you have no permanent web site, you can be given a *temporary* (dynamically allocated) IP address each time you connect to the Web

DHCP

- If you have a home or office network, only one computer needs a permanent IP address
  - The rest of the computers can be assigned *internal,* permanent IP addresses (not known to the rest of the world)
  - They can also be assigned internal IP addresses dynamically
- DHCP (Dynamic Host Configuration Protocol) is a way of assigning temporary IP addresses as needed

DNS

- Domain Name Service
- consists of different types of DNS messages that are processed according to the information in their message fields
- There are three types of DNS messages
  - Queries
  - Responses
  - Updates

ARP

- Address Resolution Protocol
- Protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.
- The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.

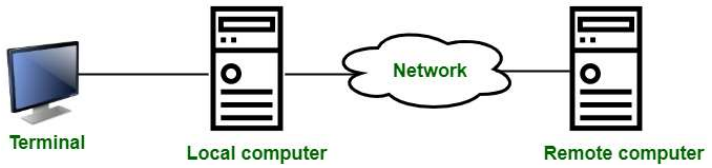
RARP

- **Reverse Address Resolution Protocol**
- used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its Link Layer or hardware address, such as a MAC address.

Remote Login

- Remote Login is a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring and result of processing from the remote computer to the local computer.

Remote Login



Telnet

- User command and an underlying TCP/IP protocol for accessing remote computers.
- Through **Telnet**, an administrator or another user can access someone else's computer remotely.

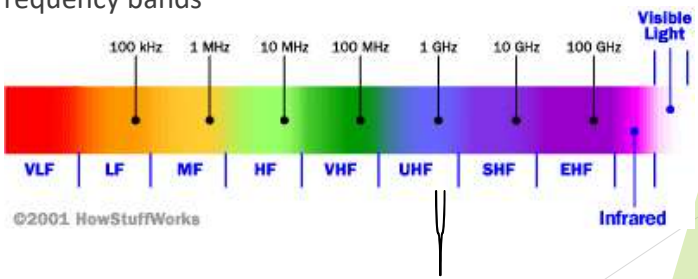
SSH

- A cryptographic network protocol for operating network services securely over an unsecured network.
- The best known example application is for remote login to computer systems by users.

Protocols & Standards in Mobile and Ubiquitous computing

Cellular Network Basics

- There are many types of cellular services; before delving into details, focus on basics (helps navigate the "acronym soup")
- Cellular network/telephony is a *radio*-based technology; radio waves are electromagnetic waves that *antennas* propagate
- Most signals are in the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz frequency bands

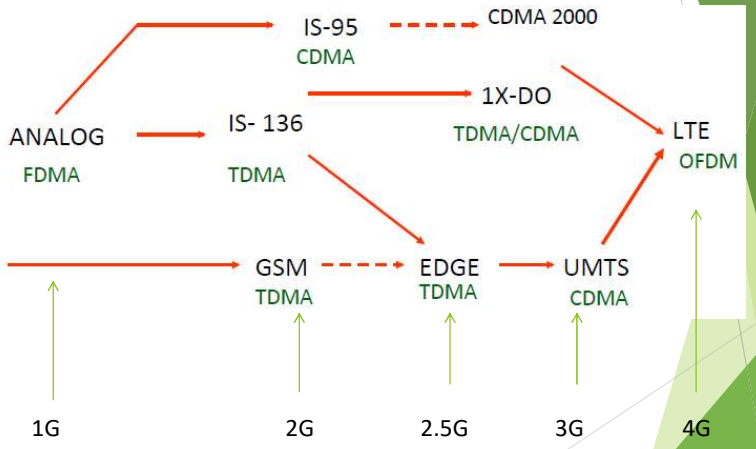


Cell phones operate in this frequency range (note the *logarithmic* scale)[2]

Cellular Network Generations

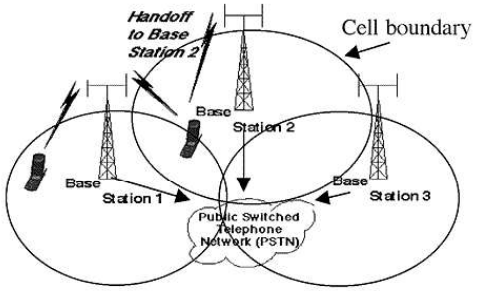
- It is useful to think of cellular Network/telephony in terms of *generations*:
  - 0G: Briefcase-size mobile radio telephones
  - 1G: *Analog* cellular telephony
  - 2G: *Digital* cellular telephony
  - 3G: *High-speed* digital cellular telephony (including *video telephony*)
  - LTE (4G): IP-based "anytime, anywhere" voice, data, and multimedia telephony at *faster* data rates than 3G

Evolution of Cellular Networks



Cellular Network

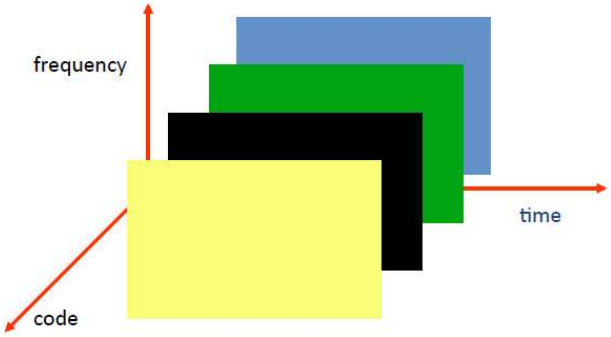
- Base stations transmit to and receive from mobiles at the assigned spectrum
  - Multiple base stations use the same spectrum (spectral reuse)
- The service area of each base station is called a cell
- Each mobile terminal is typically served by the 'closest' base stations
  - Handoff when terminals move



The Multiple Access Problem

- The base stations need to serve many mobile terminals at the same time (both downlink and uplink)
- All mobiles in the cell need to transmit to the base station
- Interference among different senders and receivers
- So we need multiple access scheme

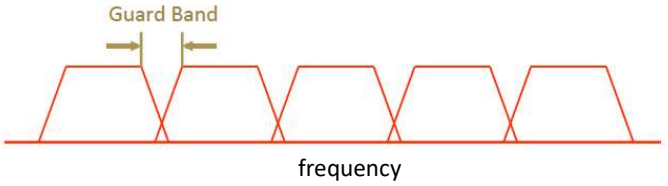
Multiple Access Schemes



3 orthogonal Schemes:

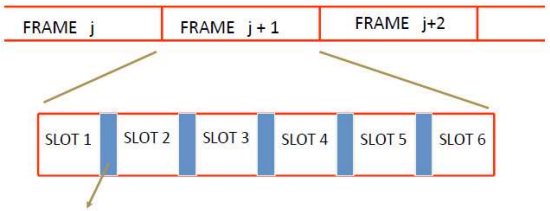
- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)

Frequency Division Multiple Access



- Each mobile is assigned a separate frequency channel for a call
- Guard band is required to prevent adjacent channel interference
- Usually, one downlink band and one uplink band
- Different cellular network protocols use different frequencies
- Frequency is precious and scare – we are running out of it
  - Cognitive radio

Time Division Multiple Access

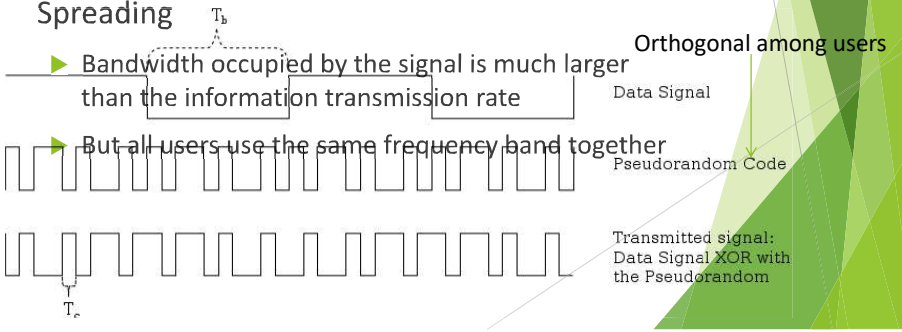


Guard time – signal transmitted by mobile terminals at different locations do no arrive at the base station at the same time

- Time is divided into slots and only one mobile terminal transmits during each slot
  - Like during the lecture, only one can talk, but others may take the floor in turn
- Each user is given a specific slot. No competition in cellular network
  - Unlike Carrier Sensing Multiple Access (CSMA) in WiFi

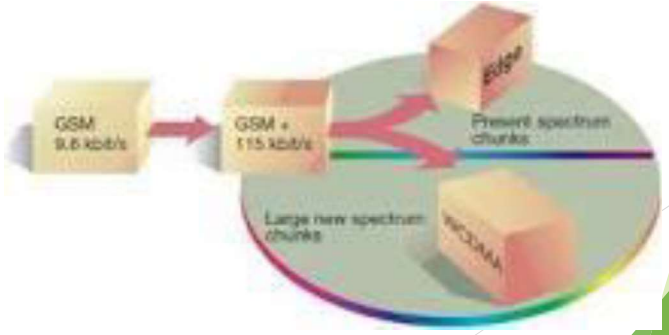
Code Division Multiple Access

- Use of orthogonal codes to separate different transmissions
- Each symbol of bit is transmitted as a larger number of bits using the user specific code – Spreading
  - Bandwidth occupied by the signal is much larger than the information transmission rate
  - But all users use the same frequency band together



Enhanced Data rates for GSM Evolution (EDGE)

- EDGE is an enhanced version of GSM and offers high-speed 3G built on GSM. It is a type of data system used on the GSM network used to allow improved data transmission rates. It can transmit three times more bits than GPRR in the same length of time.



3G

- GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load

4G

- 4G is the short name for fourth-generation wireless, the stage of broadband mobile communications that supersedes 3G (third-generation wireless) and is the predecessor of 5G (fifth-generation wireless).
- The 4G wireless cellular standard was defined by the International Telecommunication Union (ITU) and specifies the key characteristics of the standard, including transmission technology and data speeds.
- Each generation of wireless cellular technology has introduced increased bandwidth speeds and network capacity. 4G users get speeds of up to 100 Mbps, while 3G only promised a peak speed of 14 Mbps

High Speed Packet Access (HSPA)

- **High Speed Packet Access** (**HSPA**) is an amalgamation of two mobile protocols—High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA)—that extends and improves the performance of existing 3G mobile telecommunication networks using the WCDMA protocols.
- A further-improved 3GPP standard called Evolved High Speed Packet Access (also known as HSPA+) was released late in 2008, with subsequent worldwide adoption beginning in 2010.
- The newer standard allows bit rates to reach as high as 337 Mbit/s in the downlink and 34 Mbit/s in the uplink; however, these speeds are rarely achieved in practice

Ubiquitous computing

- Ubiquitous computing (or "ubicomp") is a concept in software engineering, hardware engineering and computer science where computing is made to appear anytime and everywhere.
- In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format.

Global positioning system (GPS)

- The global positioning system (GPS) is a network of satellites and receiving devices used to determine the location of something on Earth. Some GPS receivers are so accurate they can establish their location within one centimeter (0.4 inches). GPS receivers provide location in latitude, longitude, and altitude.

QR code

- A QR code (an initialism for quick response code) is a type of matrix barcode (or two-dimensional barcode)[1][2] invented in 1994 by Japanese company Denso Wave for use as labels for automotive parts.
- A barcode is a machine-readable optical image that can contain arbitrary information, often used as a label.
- In practice, QR codes often contain data for a locator, identifier, or tracker that points to a website or application.
- QR codes use four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to store data efficiently; extensions may also be used.

RFID (Radio Frequency Identification)

- An RFID (Radio Frequency Identification) system is made up of electromagnetically responsive tags that can be picked up by specialized readers.
- Each tag can be embedded with unique information and attached to objects in order to track their presence and movement.

Real Time Location System (RTLS)

- **RTLS stands for Real-Time Location System** and refers to any system that can accurately determine the location of a device in real time. It is also referred to as an indoor positioning system (IPS) which is used indoors for tracking, locating, and monitoring the activity of people and things. There are two major types of RTLS systems - Precision-based and Proximity-based RTLS system.
- **Precision-based RTLS** is implemented through either ultra-wideband or WiFi-based technologies. This allows tracking of assets to an exact location, making it useful for applications like inventory management. The drawback of precision RTLS is that it is very expensive and requires a great deal of infrastructure to drive its accuracy.
- **Proximity-based RTLS** systems are used in solutions that don't require exact locations. Proximity-based RTLS systems are less expensive and require far less infrastructure

World Wide Web Consortium (W3C)

- The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. Below we discuss important aspects of this mission, all of which further W3C's vision of One Web.
- W3C standards define an Open Web Platform for application development that has the unprecedented potential to enable developers to build rich interactive experiences, powered by vast data stores, that are available on any device.

Data Communications and Networking

1-1 DATA COMMUNICATIONS

Communication: sharing information. Sharing can be local (face to face) or remote (over distance)

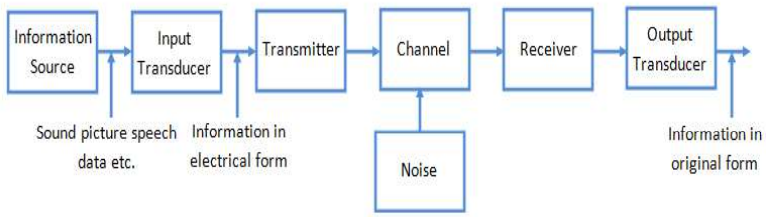
telecommunication (tele: far) means communication at a distance (telephone, television, telegraphy).

data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Communicating devices : made up of : H.W(physical equipments)and S.W

Block Diagram of Communication System



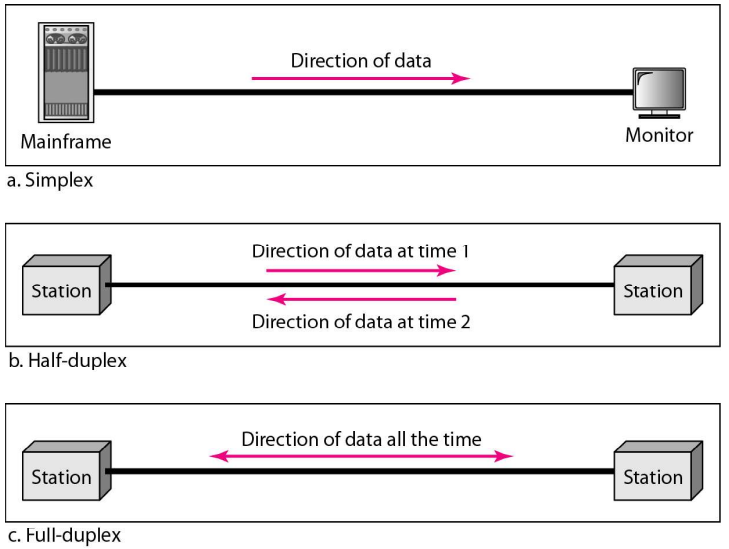
components of a communication system

•Information Source-function of information source is to produce required message which has to be transmitted

- **Input Transducer: when the message produced by the information source is not electrical in nature, an input transducer is used to convert it into a time-varying electrical signal. For example, in case of radio-broadcasting, a microphone converts the information or massage which is in the form of sound waves into corresponding electrical signal.**
- **Transmitter-function of the transmitter is to process the electrical signal from different aspects.For example in radio broadcasting the electrical signal obtained from sound signal**

- Channel and The Noise-channel means the medium through which the message travels from the transmitter to the receiver. In other words, we can say that the function of the channel is to provide a physical connection between the transmitter and the receiver.
- Receiver- main function of the receiver is to reproduce the message signal in electrical form from the distorted received signal. This reproduction of the original signal is accomplished by a process known as the demodulation or detection.
- Destination-Destination is the final stage which is used to convert an electrical message signal into its original form.For example in radio broadcasting, the destination is a loudspeaker which works as a transducer i.e. converts the electrical signal in the form of original sound signal.

Types of Data Communication



Network Criteria

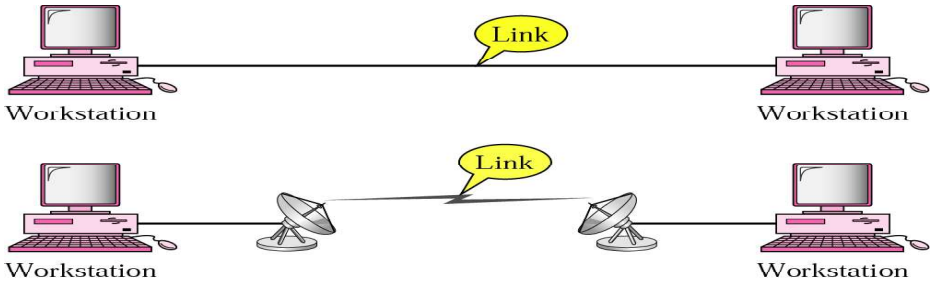
- **Performance**
  - **Depends on Network Elements**
  - **Measured in terms of Delay and Throughput**
- **Reliability**
  - **Failure rate of network components**
  - **Measured in terms of availability/robustness**
- **Security**
  - **Data protection against corruption/loss of data due to:**
    - **Errors**
    - **Malicious users (unauthorized access)**

Physical Structures

- **Type of Connection**
  - **Point to Point - single transmitter and receiver**
  - **Multipoint - multiple recipients of single transmission**
- **Physical Topology**
  - **Connection of devices**
  - **Type of transmission - unicast, mulitcast, broadcast**

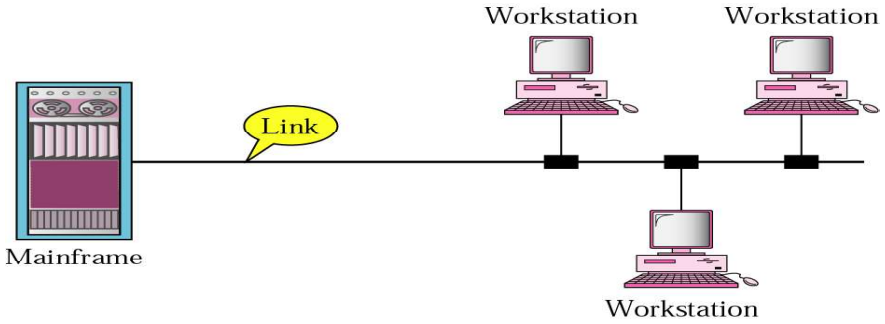
Physical Structures (Type of Connection)

- Point to Point - single transmitter and receiver

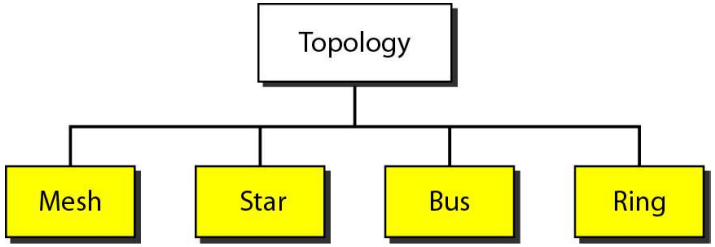


Physical Structures (Type of Connection)

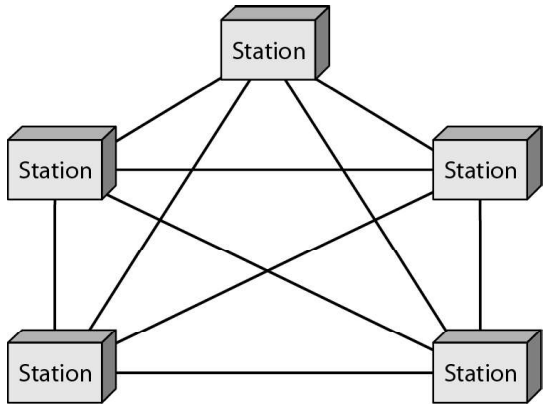
- Multipoint (multidrop) connection:



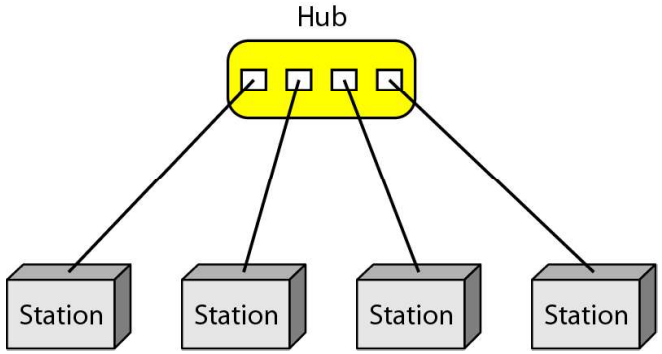
Categories of topology



A fully connected mesh topology (five devices)



A star topology connecting four stations



A bus topology connecting three stations

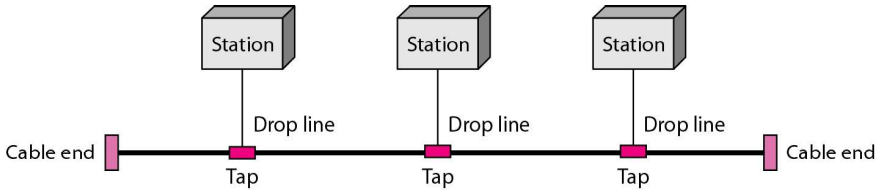


Figure 1.8 *A ring topology connecting six stations*

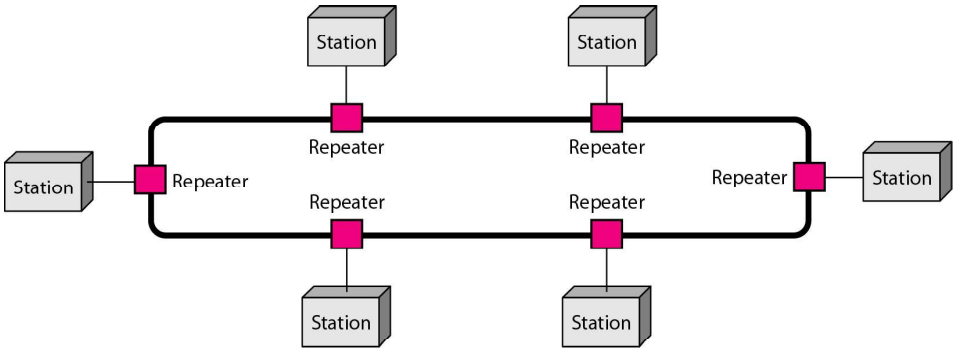
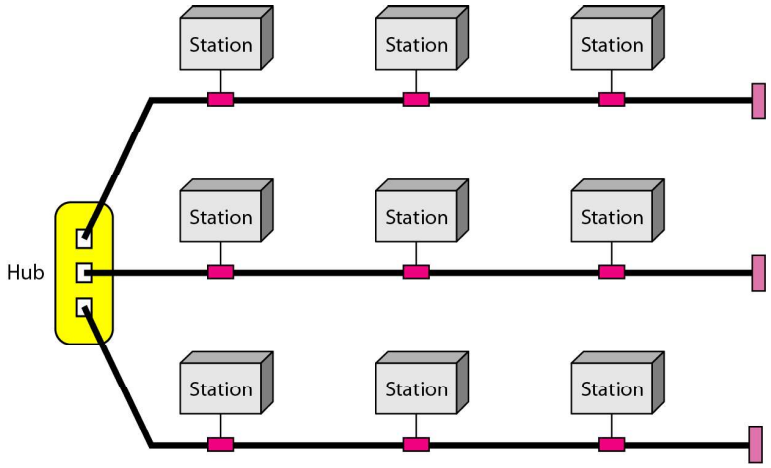


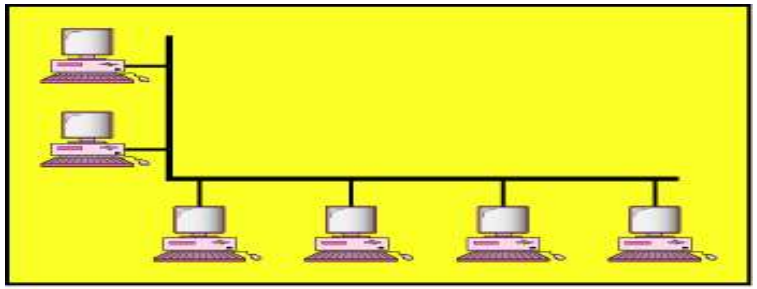
Figure 1.9 *A hybrid topology: a star backbone with three bus networks*



Categories of Networks

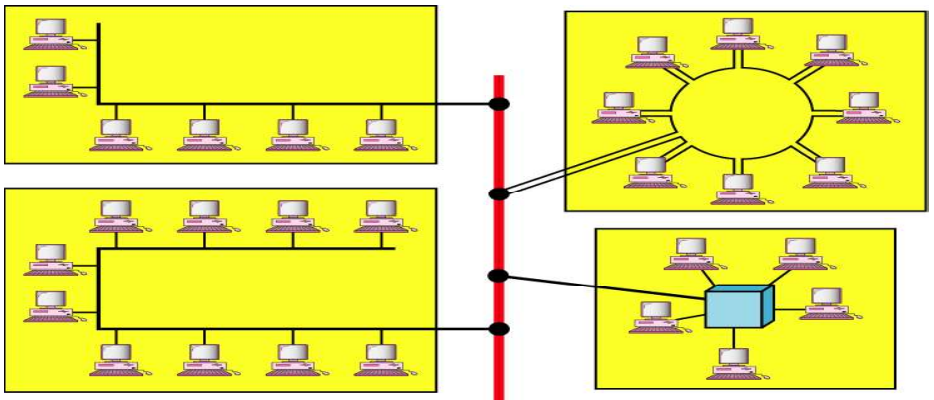
- Local Area Networks (LANs)
  - Short distances
  - Designed to provide local interconnectivity
- Metropolitan Area Networks (MANs)
  - Provide connectivity over areas such as a city, a campus
- Wide Area Networks (WANs)
  - Long distances
  - Provide connectivity over large areas

Single building LAN



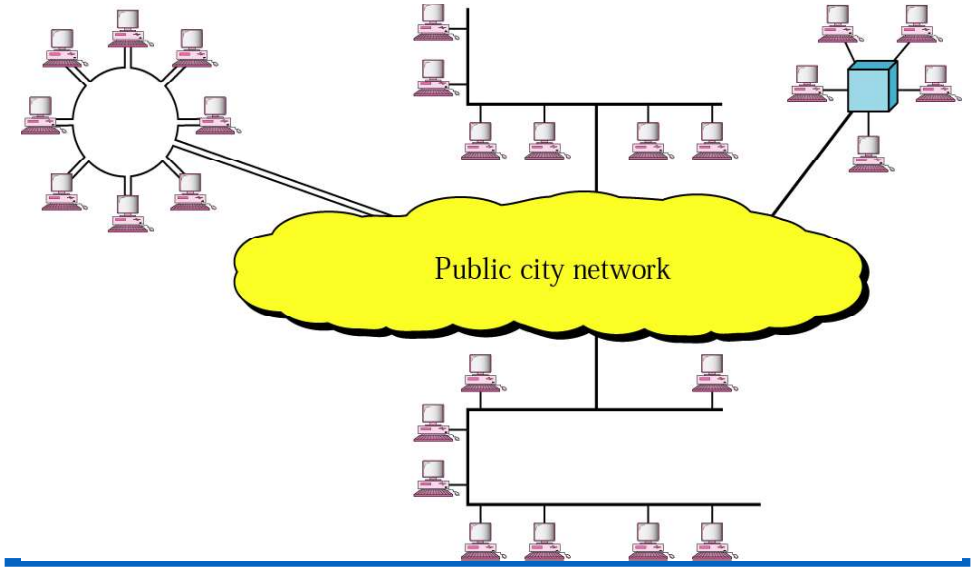
a. Single-building LAN

Multiple -building -LAN



b. Multiple-building LAN

MAN



Data Communication Applications

Application Category

- Human-machine interaction
  - Person-to-person
  - Person-to-machine or machine-to-person
  - Machine-to-machine
- Type of information
  - Voice or data
  - Structured or unstructured
  - Static image or dynamic image
- Timeliness
  - On-line
  - Real-time
  - Store-and forward
  - Batch

Evolution

- Telegraph
- Administrative message switching
- Computers

Telegraph

- Morse Code
- Dots and dashes
- Slow
- No error correction

Message Switching Systems

- Equipment: teletypewriters
- Types: torn tape message system
  - Point-to-point
  - Multipoint line
  - Collision, polling, address, and protocol
  - Control or master station and subordinate or slave station

Computers

- Benefits
  - Inquiry
  - File updating
  - Timesharing
- Types
  - Centralized
  - Distributed
  - Client-server

Applications - I

- Airline reservation system
  - American airline: Sabre system
  - United airline: Apollo reservation system
- Automatic teller machine
  - Swift: Society for Worldwide Interbank Financial Telecommunication
- Sales order entry
  - Point of sale
  - Universal product code

Applications - II

- Unstructured data application
  - Electronic mail
  - Ownership of content
  - Simple mail transfer protocol (SMTP)
    - No foreign characters
    - No executable files
    - Limited size
  - Multipurpose Internet mail extensions (MIME)

Applications - III

- Image application
  - Facsimile (FAX)
    - Simple for printed documentation
  - Television
    - Purpose
      - Security
      - Information
      - Conference
    - Types
      - Freeze-frame & full-motion
      - One-way & two-way

Internet, Intranet, Extranet

- Internet
  - Browser program
    - Netscape's Navigator
    - Microsoft's Internet Explorer
  - Uniform Resource Locator (URL)
  - World Wide Web (WWW)
  - Hypertext transfer protocol (http)
  - Internet service provider (ISP): tier 1, tier 2, tier 3
- Intranet
- Extranet

Consideration

- Response time
  - User expectation
  - consistency
- Security
- Planning for failures
  - Do nothing
  - Manual system
  - Back up computer & lines
  - Hot standby system
- Disaster Recovery
  - Mutual aid pact
  - Commercial service: Comdisco Disaster Recovery Services
  - **Planning & testing regularly**

Data & Signal

Objectives of Data Communications

- To provide a means of communication of data among source equipment and destination equipment Reliably, Efficiently, Securely and Cost effectively.

Data communication

- The data usable to a person or application are not in a form that can't be transmitted over a network.
- To be transmitted, data must be transformed to electromagnetic signal
- Data communication is the transmission of electronic data over some media.

Data

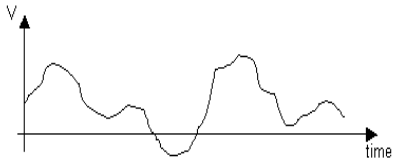
- Data can be Analog or Digital
- Analog Data
  - Are continuous and take continuous values
- Digital Data
  - Have discrete states and take discrete values

Signal

- Signals can be Analog and Digital
- An abstract element of information. (Data Represented)
- An electric current or **EMW**(Electro magnetic wave) used to convey information
- Analog Signal
  - Can have an infinite number of values in range
- Digital Signal
  - Can have only a limited number of values

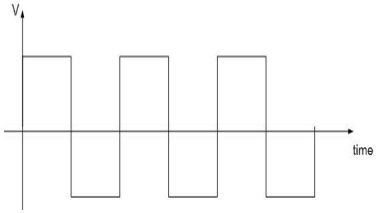
Analog Signal

- Signal intensity varies continuously over time.
- E.g. Speech



Digital Signal

- Signal intensity is constant for some period of time and then changes to another constant value. This transition takes place in a very short time.
- E.g. Binary Coded Speech



Analog ,Digital Signals

Analog

- Expensive
- Susceptible to noise
- Low attenuation
- Distortion not so effective

Digital

- Cheap
- Less Susceptible to noise
- High attenuation
- Distortion is effective

Periodic and Non periodic Signals

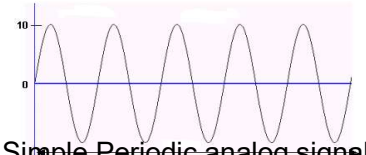
- Analog and digital Signal have two forms:
  - Periodic
    - Periodic signal completes pattern within a measurable time frame, called a **period**
    - Repeats that pattern over subsequent identical periods
    - Completion of one full pattern called **cycle**
  - Non periodic
    - Non periodic signal changes without exhibiting a pattern or cycle that repeat over times

In Data communication…

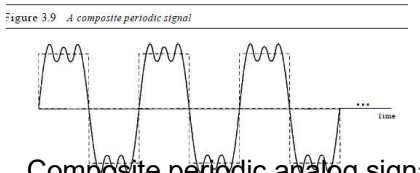
- In data communications, we commonly use **periodic analog signals** (need less bandwidth)& **non periodic digital signals** (they can represent variation in data)
- Sine wave (Sinusoidal Signal) is the most fundamental form of a periodic analog signal

Periodic Analog Signals

- Can be classified as **simple** or **composite.**
- A simple analog signal, **Sine wave** cannot be decomposed into simpler signals.
- A composite periodic analog signal is composed of multiple sine waves.



Simple Periodic analog signal



Composite periodic analog signal

Sine Wave/Periodic Analog Signal

- Periodic analog signal can be mathematically represented by the sinusoidal functions
  - **$S(t)=A\sin(2\pi ft)= A\sin(2\frac{\pi}{T}t)$**

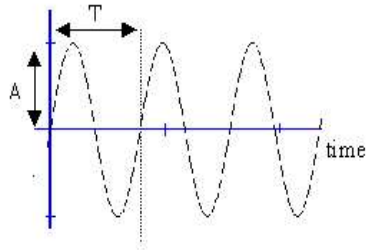
Or

- **$S(t)=A\sin(\omega t)$**

$\omega = 2\pi ft \quad f=1/T$

A=Peak Amplitude

ω =Angular Velocity (radians/sec)

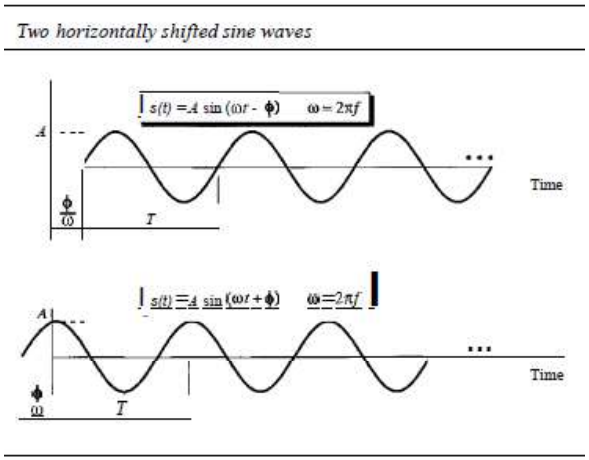


Horizontal Shifting of sine waves(phase)

- Shifting a sine wave to the left or right is a positive or negative shift, respectively

$$s(t)=A\sin(\omega t-\theta)$$

$$s(t)=A\sin(\omega t+\theta)$$

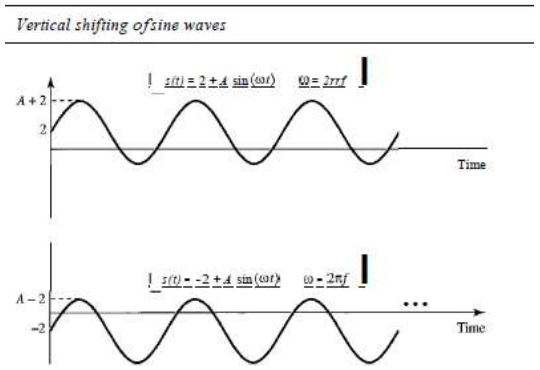


Vertical shifting of sine waves (phase)

- When a sine wave is shifted vertically, a constant is added to the instantaneous amplitude of signal

$$s(t)=2+A\sin(\omega t)$$

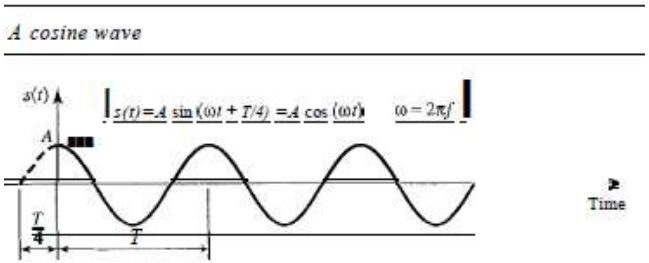
$$s(t)=-2+A\sin(\omega t)$$



Cosine wave

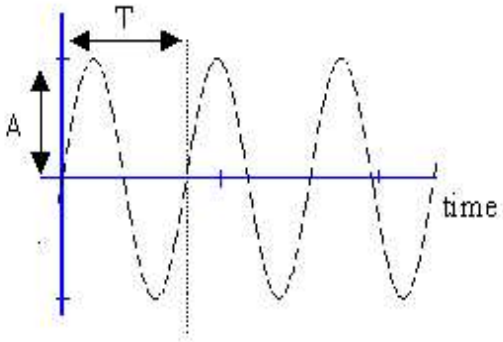
- Shifting a sine wave T/2 to the left, called cosine wave

$$s(t)=A\sin(\omega t+\pi/2)=A\cos(\omega t)$$



Parameters of sinusoidal signal/sine wave

- Peak Amplitude (A)
- Frequency(*f*)
- Period(T)



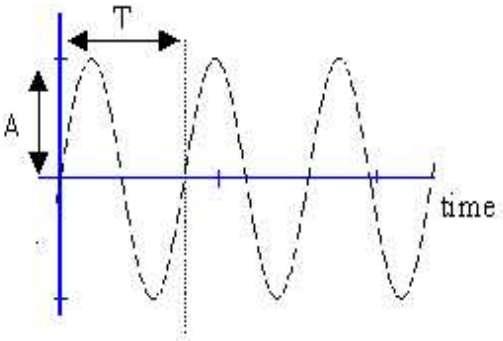
Parameters of sinusoidal signal/sine wave

- Peak Amplitude (A)
  - The maximum value / strength of the signal over time
- Period (T)
  - The amount of time that a wave takes for one repetition.
- Frequency (f)
  - Frequency is the rate at which the signal repeats. Expressed in Hertz (Hz), or cycles per second.

Parameters of sinusoidal signal/sine wave

- **T = 1 / f**
- **F = 1 / T**

- **T- seconds(s)**
- **f- Hz(Hertz)**



Exercise

(1)The power we use at home has a frequency of 60 Hz .Calculate the period of sine wave

$$T = \frac{1}{f} = \frac{1}{60} = 0.0166\ \text{s} = 0.0166 \times 10^{3}\ \text{ms}$$

(2) Express a period of 100 ms in microseconds.

$$100\ \text{ms} = 100 \times 10^{-3}\ \text{s} = 100 \times 10^{-3} \times 10^{6}\ \mu\text{s} = 10^{2} \times 10^{-3} \times 10^{6}\ \mu\text{s} = 10^{5}\ \mu\text{s}$$

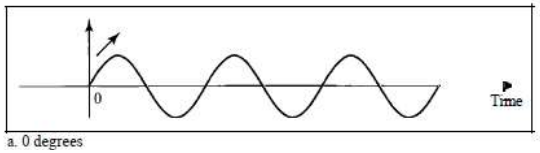
(2) The period of a signal is 100 ms. What is its frequency in kilohertz?

$$100\ \text{ms} = 100 \times 10^{-3}\ \text{s} = 10^{-1}\ \text{s}$$

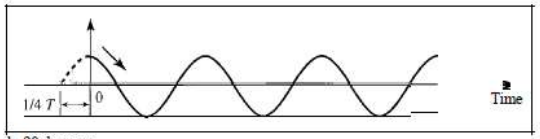
$$f = \frac{1}{T} = \frac{1}{10^{-1}}\ \text{Hz} = 10\ \text{Hz} = 10 \times 10^{-3}\ \text{kHz} = 10^{-2}\ \text{kHz}$$

Phase

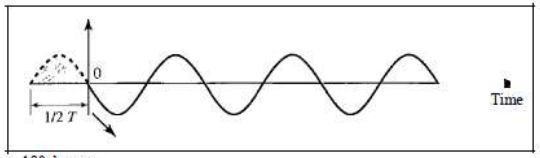
Three sine waves with the same amplitude andfrequency, but different phases



a. 0 degrees



b. 90 degrees



c. 180 degrees

A sine wave with a phase of 0° starts at time 0 with a zero amplitude. The amplitude is increasing.

2. A sine wave with a phase of 90° starts at time 0 with a peak amplitude. The amplitude is decreasing.

3. A sine wave with a phase of 180° starts at time 0 with a zero amplitude. The amplitude is decreasing.

Cycle

- A cycle is one complete movement of the wave from its start point and back to the same point again.

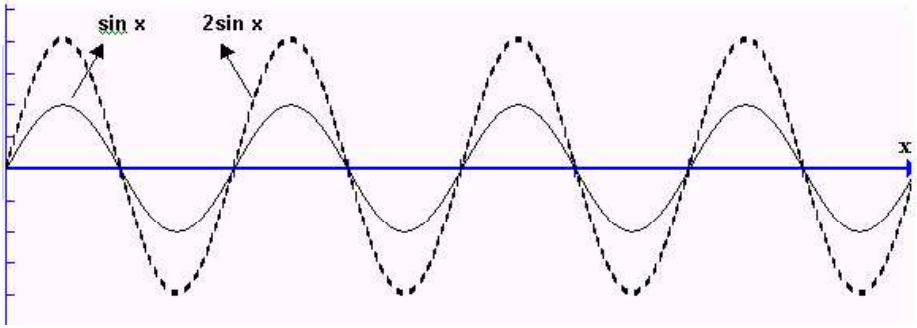
$\omega = 2\pi f$ $T = 2\pi / \omega$

Wavelength (λ)

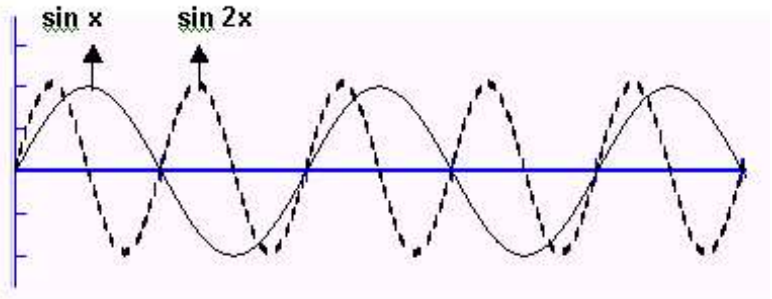
- Distance between identical points in the adjacent cycles of a wave.
- Wavelength= propagation speed × period
  = propagation speed / frequency
- The relationship among Velocity of propagation (v), Wave Length (λ) and Frequency (f) is given by

$V = f\lambda$

Effect of Increasing Amplitude



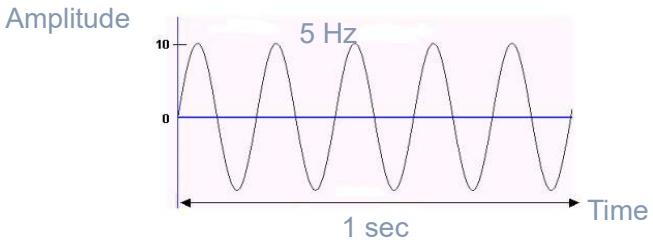
Effect of Increasing / Decreasing Frequency



Time Domain and frequency Domain

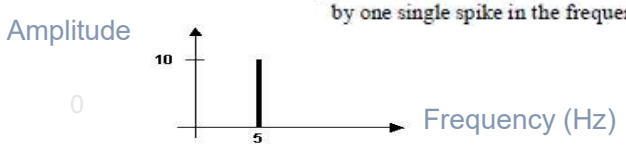
- The time domain plot of a signal shows the change of the amplitude of the signal over time.
- No prominence is given to the frequency or phase.
- Frequency domain plot shows the variation of the amplitude with frequency.

Time Domain and frequency Domain



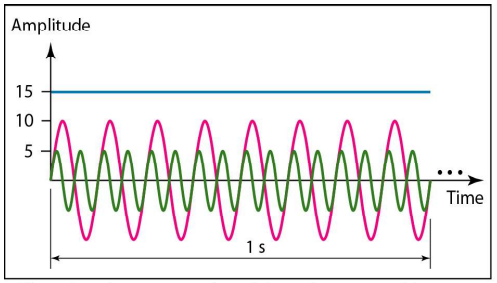
Time Domain Plot

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

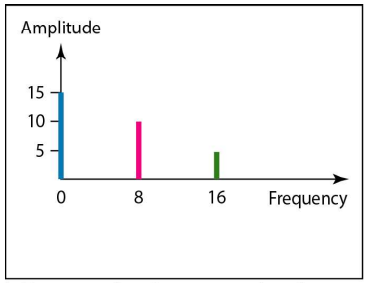


Frequency Domain Plot

The time domain and frequency domain of three sine waves



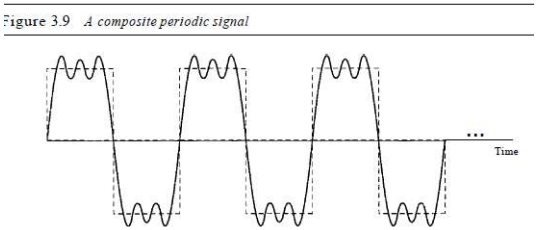
a. Time-domain representation of three sine waves with frequencies 0, 8, and 16



b. Frequency-domain representation of the same three signals

Composite Signals

- A single frequency sine wave is not useful in data communications
- A signal is not always consisting of a single frequency but a series of frequencies.
- A signal made of many simple sine waves



Composite Signals

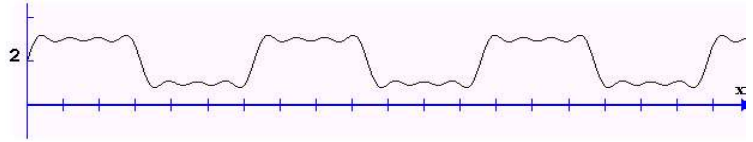
- Any periodic signal can be represented as a sum of sinusoidal known as Fourier series.

$$s(t) = \frac{A_0}{2} + \sum_{n=1}^{\infty} [A_n \cos(\varpi nt) + B_n \sin(\varpi nt)]$$

- $A_0/2$ is the D.C(direct current) component of the signal.

Composite Signals

- Consider the following periodic composite(non sinusoidal) signal.

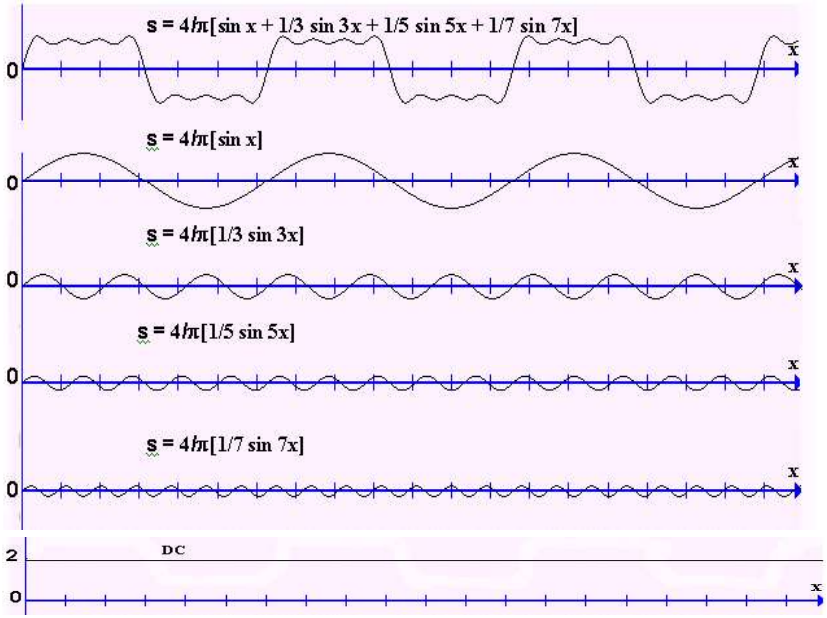


- It can be mathematically represented as follows

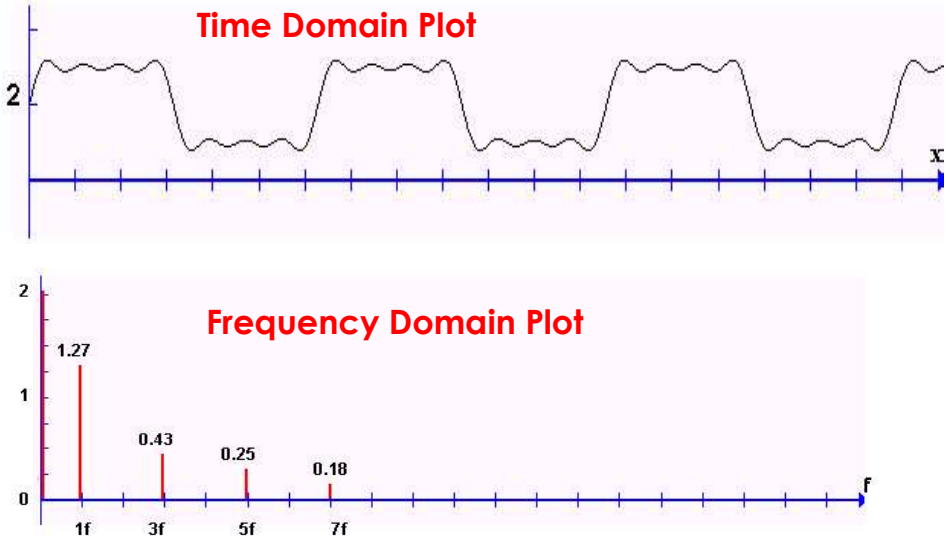
S(t) = 2 + π/4[sin x + 1/3sin3x + 1/5 sin 5x + 1/7 sin 7x]

- It can be decomposed in the following way, into its frequency components.

Composite Signals



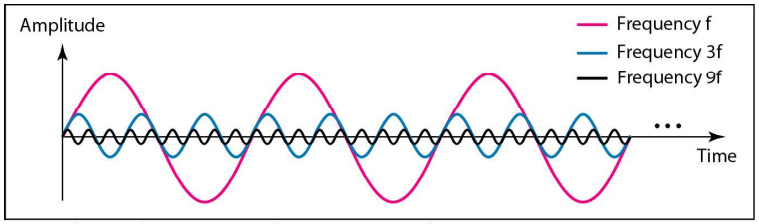
Composite Signals



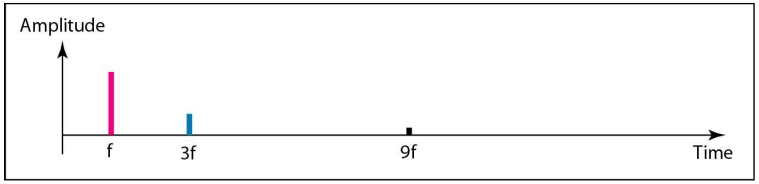
Composite signal

- A complex wave consists of an infinite number of sine waves of different amplitudes and frequency components.
- Periodic or non periodic
- Frequency components are multiples of the fundamental.
- In the above wave, it is odd multiples.
- The period of the whole signal is of the same period as the fundamental component.

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



a. Time-domain decomposition of a composite signal

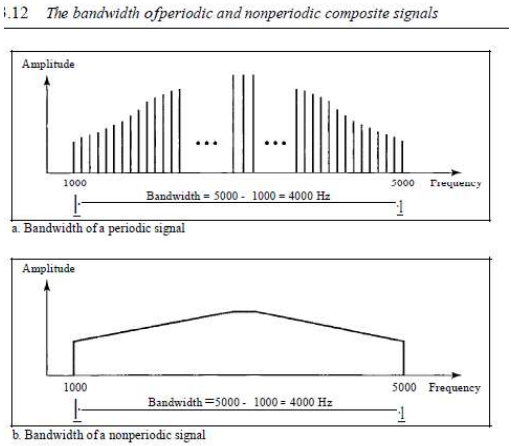


b. Frequency-domain decomposition of the composite signal

Bandwidth

The difference between the maximum frequency f_{max} and the minimum frequency f_{min} of a signal

$$BW = f_{max} - f_{min}$$



a. Bandwidth of a periodic signal

b. Bandwidth of a nonperiodic signal

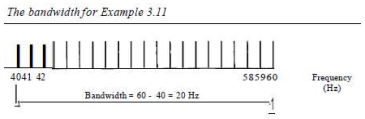
Example

(1) If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700,and 900 Hz, what is its bandwidth? Draw the spectrum, assuming all components have a maximum amplitude of 10 V

$$B = f_h - f_l = 900 - 100 = 800 \text{ Hz}$$

(2) A periodic signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum if the signal contains all frequencies of the same amplitude.

$$B = f_h - f_l \Rightarrow 20 = 60 - f_l \Rightarrow f_l = 60 - 20 = 40 \text{ Hz}$$

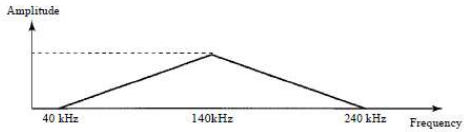


The bandwidth for Example 3.11

Example

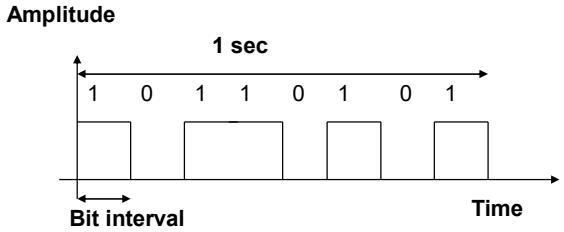
(3) A non periodic composite signal has a bandwidth of 200 kHz, with a middle frequency of 140 kHz and peak amplitude of 20 V. The two extreme frequencies have an amplitude of 0. Draw the frequency domain of the signal.

The lowest frequency must be at 40 kHz and the highest at 240 kHz



Digital Signals

- Most of digital signals are aperiodic.
- Period or frequency is not appropriate.
- Bit rate are used instead.



Digital Signal

- Bit Rate
  - The number of bits sent in 1 s (bps)
- Bit length
  - Bit length is the distance one bit occupies on the transmission medium
  - Bit length=propagation Speed ×bit duration
- Bit interval (same as bit length)
  - time required to send one single bit

Transmission impairment

•When a signal is transmitted over a communication channel, it is subjected to different types of impairments because of imperfect characteristics of a channel.

•Received and transmitted signals are not same

•These impairments introduce random modification in analog signals leading to distortion

•The impairments lead to error in the Bit values

Transmission impairment

Impairments can be categorized in to three types

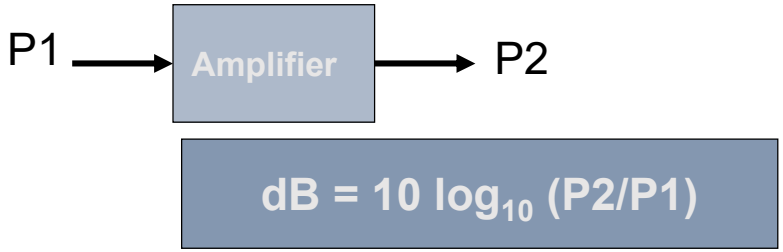
- Attenuation
- Distortion
- Noise

Attenuation

Irrespective of whether a medium is guided or unguided, the strength of a signal fall off with distance. This is known as attenuation.

Power Gain / Loss

Expressed in decibels (named in honor of Alexander Graham Bell).

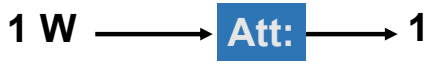


Example

Gain in dB = 10 Log (1000/1)

= 10 Log (10^3)

= 30 dB



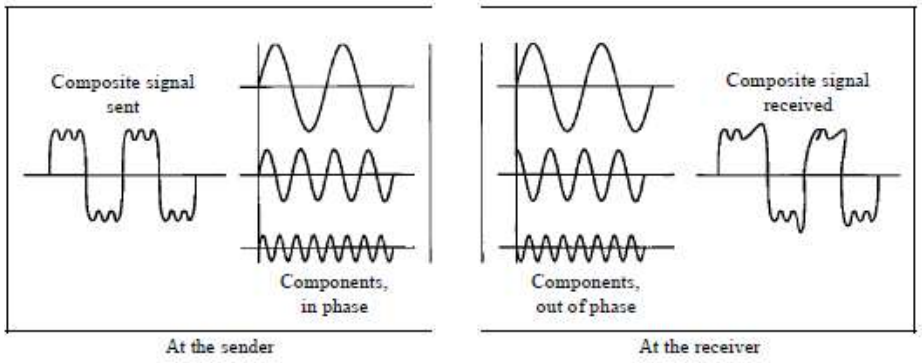
Loss in dB = 10 Log (1/1000)

= 10 Log (10^{-3})

= - 30 dB

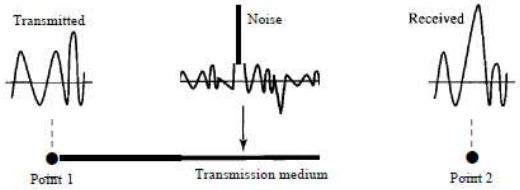
Distortion

•Signal changes its form or shape



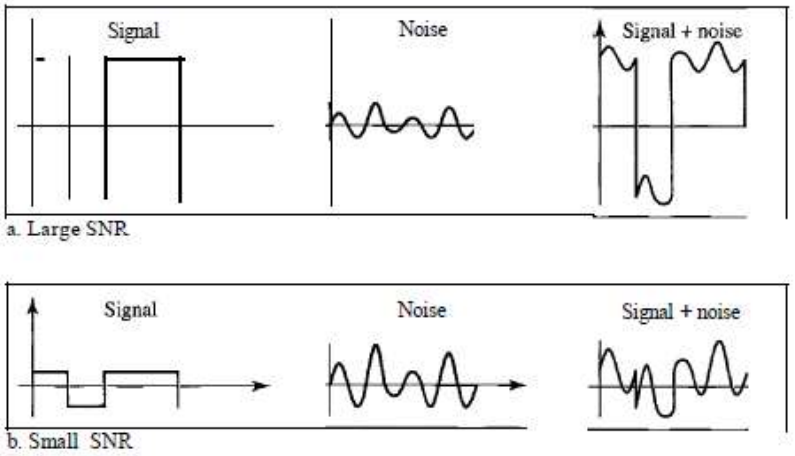
Noise

- Noise is another cause of impairment
- Several types of noise:
  - Thermal noise
  - Induced noise
  - Crosstalk
  - Impulse noise
- Corrupt the signal



Noise

3.30 *Two cases of SNR: a high SNR and a low SNR*



Signal Encoding Techniques

Encoding Techniques

- Digital data, digital signal
- Analog data, digital signal
- Digital data, analog signal
- Analog data, analog signal

1. Digital Data, Digital Signal

- Digital signal
  - —Discrete, discontinuous voltage pulses
  - —Each pulse is a signal element
  - —Binary data encoded into signal elements

Terms (1)

- Unipolar
  - —All signal elements have same sign
- Polar
  - —One logic state represented by positive voltage the other by negative voltage
- Data rate
  - —Rate of data transmission in bits per second
- Duration or length of a bit
  - —Time taken for transmitter to emit the bit

Terms (2)

- Modulation rate
  - —Rate at which the signal level changes
  - —Measured in baud = signal elements per second
- Mark and Space
  - —Binary 1 and Binary 0 respectively

Interpreting Signals

- Need to know
  - —Timing of bits - when they start and end
  - —Signal levels
- Factors affecting successful interpreting of signals
  - —Signal to noise ratio
  - —Data rate
  - —Bandwidth

Comparison of Encoding Schemes (1)

- Signal Spectrum
  - —Lack of high frequencies reduces required bandwidth
  - —Lack of dc component allows ac coupling via transformer, providing isolation
  - —Concentrate power in the middle of the bandwidth
- Clocking
  - —Synchronizing transmitter and receiver
  - —External clock
  - —Sync mechanism based on signal

Comparison of Encoding Schemes (2)

- Error detection
  - —Can be built in to signal encoding
- Signal interference and noise immunity
  - —Some codes are better than others
- Cost and complexity
  - —Higher signal rate (& thus data rate) lead to higher costs
  - —Some codes require signal rate greater than data rate

Encoding Schemes

- Nonreturn to Zero-Level (NRZ-L)
- Nonreturn to Zero Inverted (NRZI)
- Bipolar -AMI
- Manchester

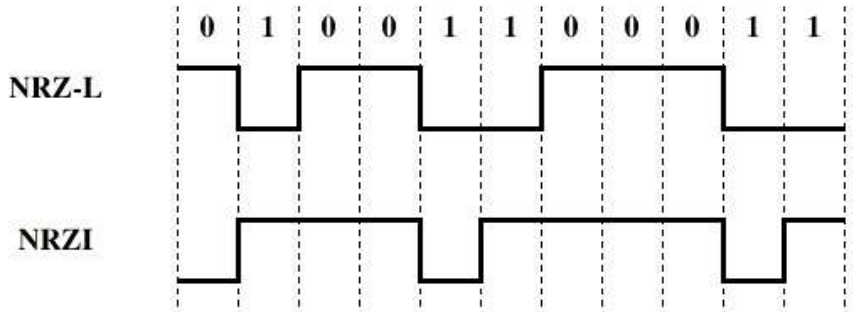
Nonreturn to Zero-Level (NRZ-L)

- Two different voltages for 0 and 1 bits
- Voltage constant during bit interval
  - —no transition I.e. no return to zero voltage
- e.g. Absence of voltage for zero, constant positive voltage for one
- More often, negative voltage for one value and positive for the other
- This is NRZ-L

Nonreturn to Zero Inverted

- Nonreturn to zero inverted on ones
- Constant voltage pulse for duration of bit
- Data encoded as presence or absence of signal transition at beginning of bit time
- Transition (low to high or high to low) denotes a binary 1
- No transition denotes binary 0
- An example of differential encoding

NRZ



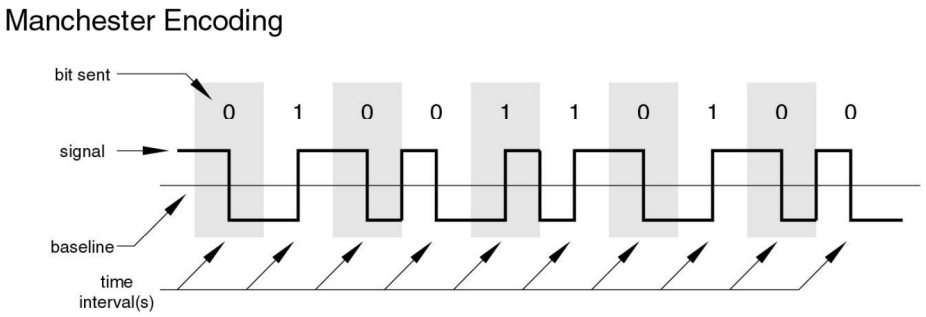
NRZ pros and cons

- Pros
  - —Easy to engineer
  - —Make good use of bandwidth
- Cons
  - —dc component
  - —Lack of synchronization capability
- Used for magnetic recording
- Not often used for signal transmission

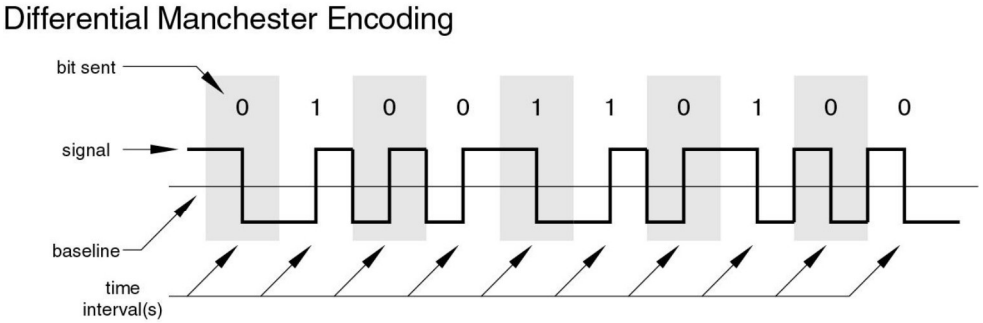
Biphase

- Manchester
  - — Transition in middle of each bit period
  - — Transition serves as clock and data
  - — Low to high represents one
  - — High to low represents zero
  - — Used by IEEE 802.3
- Differential Manchester
  - — Midbit transition is clocking only
  - — Transition at start of a bit period represents zero
  - — No transition at start of a bit period represents one
  - — Note: this is a differential encoding scheme
  - — Used by IEEE 802.5

Manchester Encoding

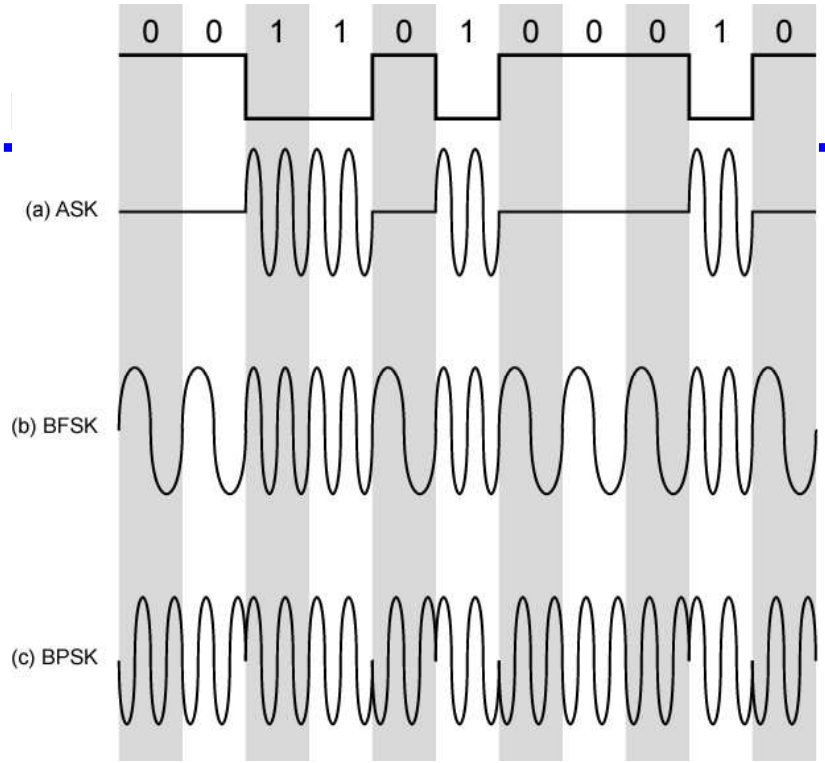


Differential Manchester Encoding



Biphase Pros and Cons

- Con
  - —At least one transition per bit time and possibly two
  - —Maximum modulation rate is twice NRZ
  - —Requires more bandwidth
- Pros
  - —Synchronization on mid bit transition (self clocking)
  - —No dc component
  - —Error detection
    - Absence of expected transition



Digital Data, Analog Signal

- Public telephone system
  - —300Hz to 3400Hz
  - —Use modem (modulator-demodulator)
- Amplitude shift keying (ASK)
- Frequency shift keying (FSK)
- Phase shift keying (PK)

Amplitude Shift Keying

- Values represented by different amplitudes of carrier
- Usually, one amplitude is zero
  - —i.e. presence and absence of carrier is used
- Susceptible to sudden gain changes
- Inefficient
- Up to 1200bps on voice grade lines
- Used over optical fiber

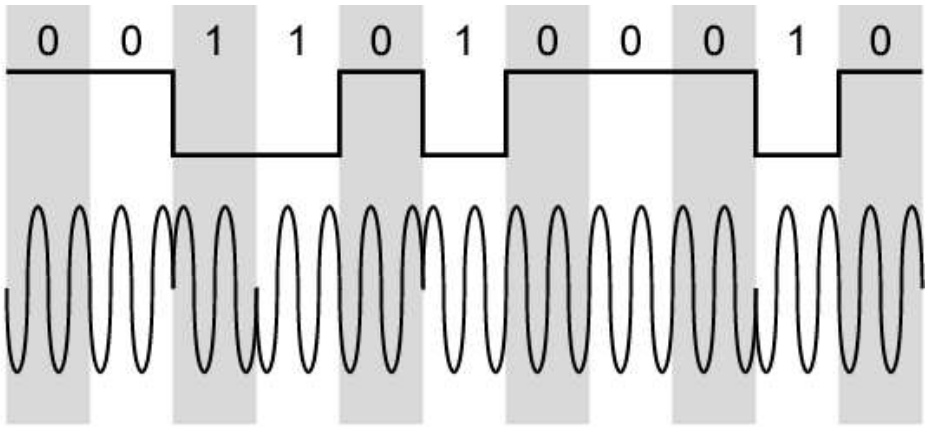
Binary Frequency Shift Keying

- Most common form is binary FSK (BFSK)
- Two binary values represented by two different frequencies (near carrier)
- Less susceptible to error than ASK
- Up to 1200bps on voice grade lines
- High frequency radio
- Even higher frequency on LANs using co-ax

Phase Shift Keying

- Phase of carrier signal is shifted to represent data
- Binary PSK
  - —Two phases represent two binary digits
- Differential PSK
  - —Phase shifted relative to previous transmission rather than some reference signal

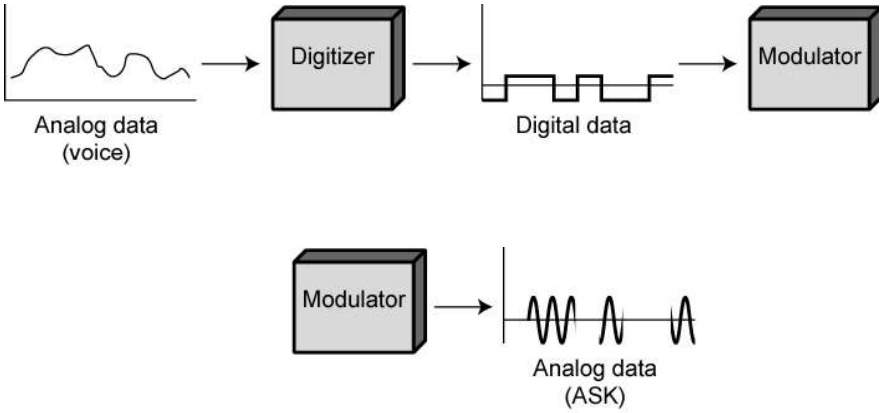
Differential PSK



2. Analog Data, Digital Signal

- Digitization
  - —Conversion of analog data into digital data
  - —Digital data can then be transmitted using NRZ-L
  - —Digital data can then be transmitted using code other than NRZ-L
  - —Digital data can then be converted to analog signal
  - —Analog to digital conversion done using a codec
  - —Pulse code modulation
  - —Delta modulation

Digitizing Analog Data



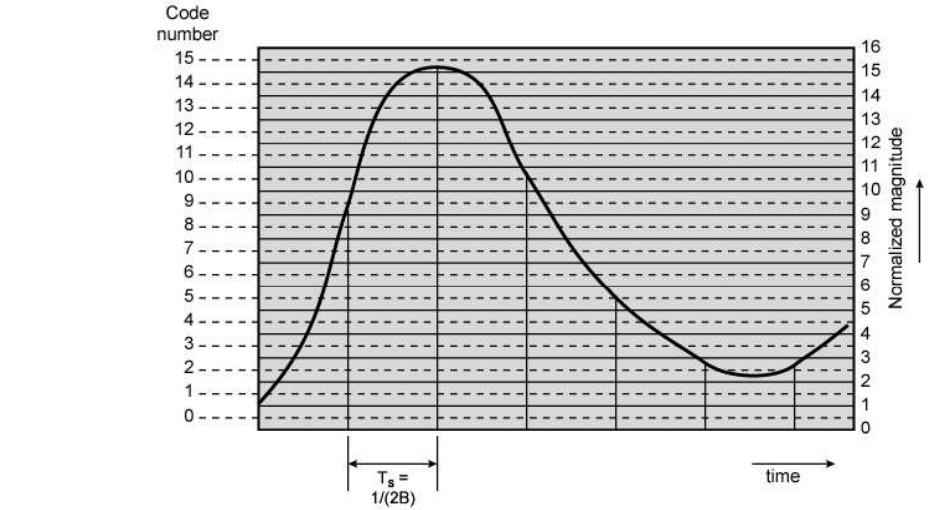
Pulse Code Modulation(PCM) (1)

- If a signal is sampled at regular intervals at a rate higher than twice the highest signal frequency, the samples contain all the information of the original signal
- Voice data limited to below 4000Hz
- Require 8000 sample per second
- Analog samples (Pulse Amplitude Modulation, PAM)
- Each sample assigned digital value

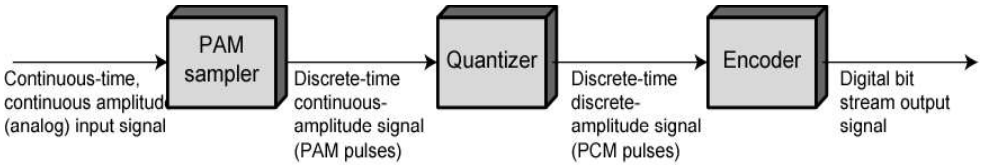
Pulse Code Modulation(PCM) (2)

- 4 bit system gives 16 levels
- Quantized
  - —Quantizing error or noise
  - —Approximations mean it is impossible to recover original exactly
- 8 bit sample gives 256 levels
- Quality comparable with analog transmission
- 8000 samples per second of 8 bits each gives 64kbps

PCM Example



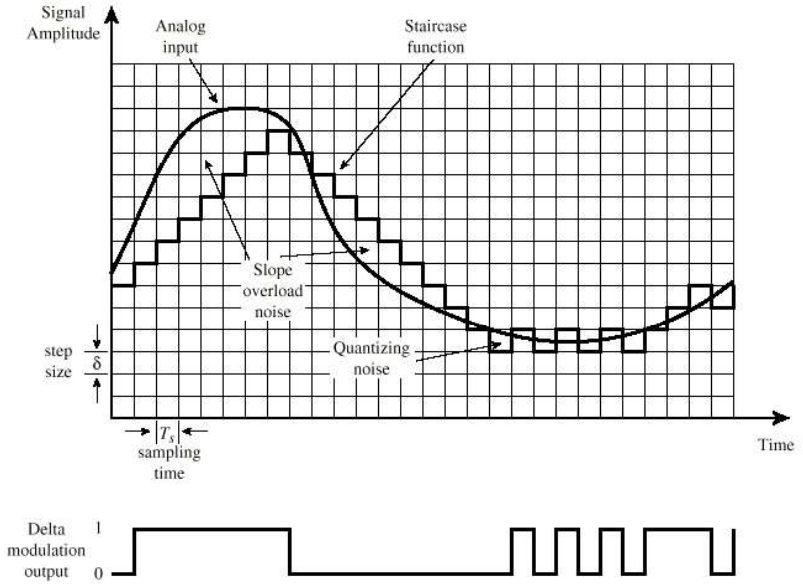
PCM Block Diagram



Delta Modulation

- Analog input is approximated by a staircase function
- Move up or down one level (δ) at each sample interval
- Binary behavior
  - —Function moves up or down at each sample interval

Delta Modulation - example



Delta Modulation - Performance

- Good voice reproduction
  - —PCM - 128 levels (7 bit)
  - —Voice bandwidth 4khz
  - —Should be 8000 x 7 = 56kbps for PCM
- Data compression can improve on this
  - —e.g. Interframe coding techniques for video

3. Digital Data, Analog Signal

- Main use is public telephone system
  - Was designed to receive, switch, and transmit analog signals
  - Has a frequency range of 300Hz to 3400Hz
  - Is not at present suitable for handling digital signals from the subscriber locations
  - Uses modem (modulator-demodulator) to convert digital data to analog signals and vice versa

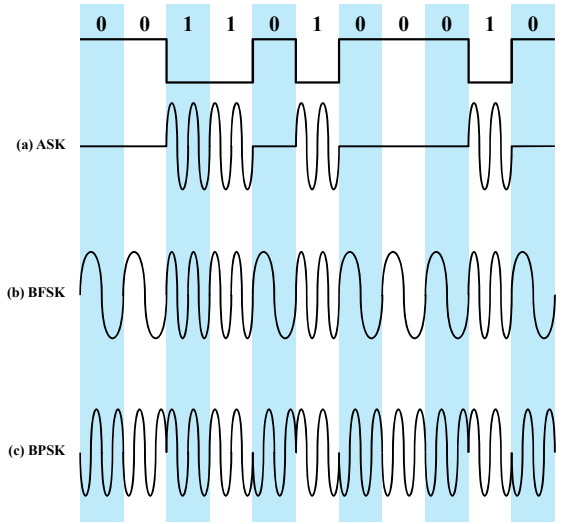


Figure 5.7 Modulation of Analog Signals for Digital Data

Amplitude Shift Keying (ASK)

- Encode 0/1 by different carrier amplitudes
  - Usually have one amplitude zero
- Susceptible to sudden gain changes
- Inefficient
- Used for:
  - Up to 1200bps on voice grade lines
  - Very high speeds over optical fiber

Phase Shift Keying (PSK)

- The phase of the carrier signal is shifted to represent data
- Binary PSK
  - Two phases represent the two binary digits
- Differential PSK
  - Phase shifted relative to previous transmission rather than some reference signal

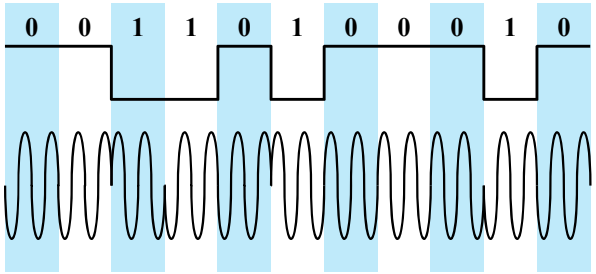
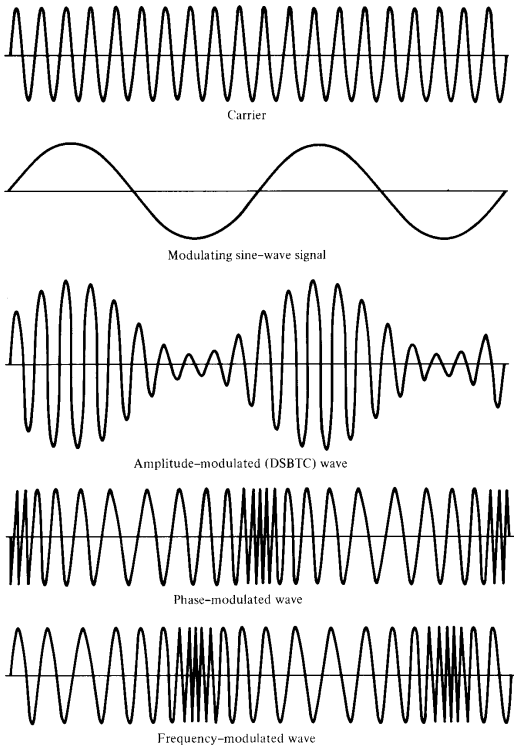


Figure 5.10 Differential Phase-Shift Keying (DPSK)

4. Analog Data, Analog Signals

- Why modulate analog signals?
  - —Higher frequency can give more efficient transmission
  - —Permits frequency division multiplexing (chapter 8)
- Types of modulation
  - —Amplitude
  - —Frequency
  - —Phase

Analog Modulation



Risk Analysis

What Is Risk?

- Risk is the likelihood that a loss will occur. Losses occur when a threat exposes a vulnerability.
- Organizations of all sizes face risks. Some risks are so severe they cause a business to fail. Other risks are minor and can be accepted without another thought.
- Organizations use risk management techniques to identify and differentiate severe risks from minor risks.
- When this is done properly, administrators and managers can intelligently decide what to do about any type of risk.
- Thus, the end result is a decision to avoid, transfer, mitigate, or accept a risk.

Cont…

- The common themes of these definitions are threat, vulnerability, and loss.
- Here's a short definition of each of these terms:

  - Threat—A threat is any activity that represents a possible danger.
  - Vulnerability—A vulnerability is a weakness.
  - Loss—A loss results in a compromise to business functions or assets.
- Risks to organizations can result in a loss that negatively affects the business.
- The overall goal is to reduce the losses that can occur from risk.

Examples of Business functions and possible risks:

- A Web site sells products on the Internet. If the Web site is attacked and fails, sales are lost.
- Authors write articles that must be submitted by a deadline to be published. If the author's PC becomes infected with a virus, the deadline passes and the article's value is reduced.
- Analysts compile reports used by management to make decisions.
- Data is gathered from internal servers and Internet sources. If network connectivity fails, analysts won't have access to current data. Management could make decisions based on inaccurate information.

Cont…

- A warehouse application is used for shipping products that have been purchased. It identifies what has been ordered, where the products need to be sent, and where they are located. If the application fails, products aren't shipped on time.

What Are the **Major Components** of Risk to an IT Infrastructure?

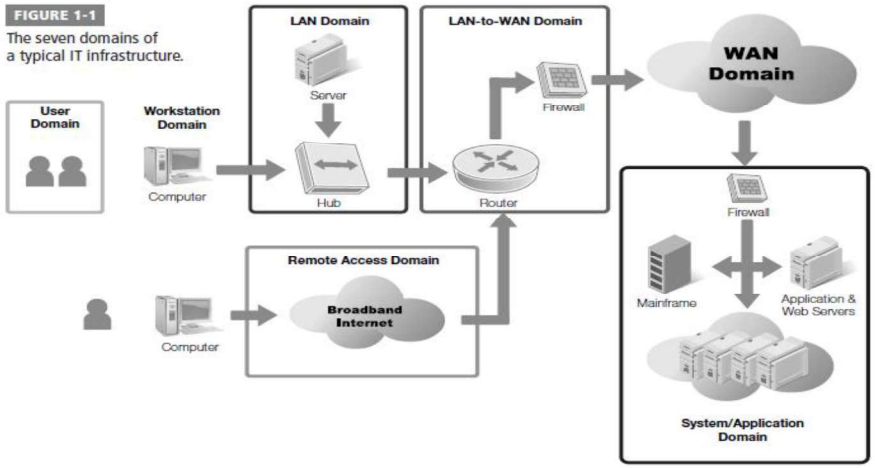


Figure 1.1 Domains of a typical IT infrastructure

Threats, Vulnerabilities, and Impact

• When a threat exploits a vulnerability it results in a loss. The impact identifies the severity of the loss.

• A threat is any circumstance or event with the potential to cause a loss. You can also think of a threat as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they may be controlled.

• Threats have independent probabilities of occurring that often are unaffected by an organizational action. As an example, an attacker may be an expert in attacking Web servers hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, a company can reduce or eliminate vulnerabilities to reduce the attacker's chance of success.

Cont…

• Threats are attempts to exploit vulnerabilities that result in the loss of confidentiality, integrity, or availability of a business asset.

• The protection of confidentiality, integrity, and availability are common security objectives for information systems.

• Figure 1.2 shows these three security objectives as a protective triangle. If any side of the triangle is breached or fails, security fails.

• In other words, risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources.

Cont…

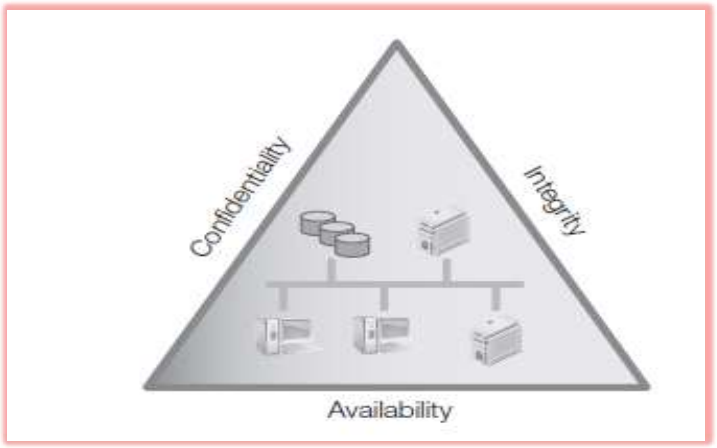


Figure 1.2 security objectives

Cont…

• A vulnerability is a weakness. It could be a procedural, technical, or administrative weakness.

• It could be a weakness in physical security, technical security, or operational security.

• It's only when an attacker is able to exploit the vulnerability that a loss to an asset occurs.

• Vulnerabilities may exist because they've never been corrected. They can also exist if security is weakened either intentionally or unintentionally.

• Example: Consider a locked door used to protect a server room. A technician could intentionally unlock it to make it easier to access. If the door doesn't shut tight on its own, it could accidentally be left open. Either way, the server room becomes vulnerable.

Risk Assessment

- critical component of process
  - else may have vulnerabilities or waste money
- ideally examine every asset vs risk
  - not feasible in practice
- choose one of possible alternatives based on organization's resources and risk profile
  - baseline
  - informal
  - formal
  - combined

Baseline Approach

- use "industry best practice"
  - easy, cheap, can be replicated
  - but gives no special consideration to org.
  - may give too much or too little security
- implement safeguards against most common threats
- baseline recommendations and checklist documents available from various bodies
- alone only suitable for small organizations

Informal Approach

- conduct informal, pragmatic risk analysis on organization's IT systems
- exploits knowledge and expertise of analyst
- fairly quick and cheap
- does address some org specific issues
- some risks may be incorrectly assessed
- skewed by analysts views, varies over time
- suitable for small to medium sized orgs

Detailed Risk Analysis

- most comprehensive alternative
- assess using formal structured process
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- costly and slow, requires expert analysts
- may be a legal requirement to use
- suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- combines elements of other approaches
  - initial baseline on all systems
  - informal analysis to identify critical risks
  - formal assessment on these systems
  - iterated and extended over time
- better use of time and money resources
- better security earlier that evolves
- may miss some risks early
- recommended alternative for most orgs

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems or processes
- hence determine applicability and significance of threat to organization
- need combination of threat and vulnerability to create a risk to an asset
- again can use lists of potential vulnerabilities in standards etc

Access Control

Access Control

- The process by which resources or services are granted or denied on a computer system or network
- There are four standard access control models as well as specific practices used to enforce access control

Access Control Terminology

- **Identification**
  - A user accessing a computer system would present credentials or identification, such as a username
- **Authentication**
  - Checking the user's credentials to be sure that they are authentic and not fabricated, usually using a password
- **Authorization**
  - Granting permission to take the action
- A computer user is granted **access**
  - To only certain services or applications in order to perform their duties
- **Custodian**
  - The person who reviews security settings
  - Also called **Administrator**

Access Control Terminology (continued)

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Table 7-1 Basic steps in access control

Access Control Terminology (continued)

Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End User	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Table 7-2 Roles in access control

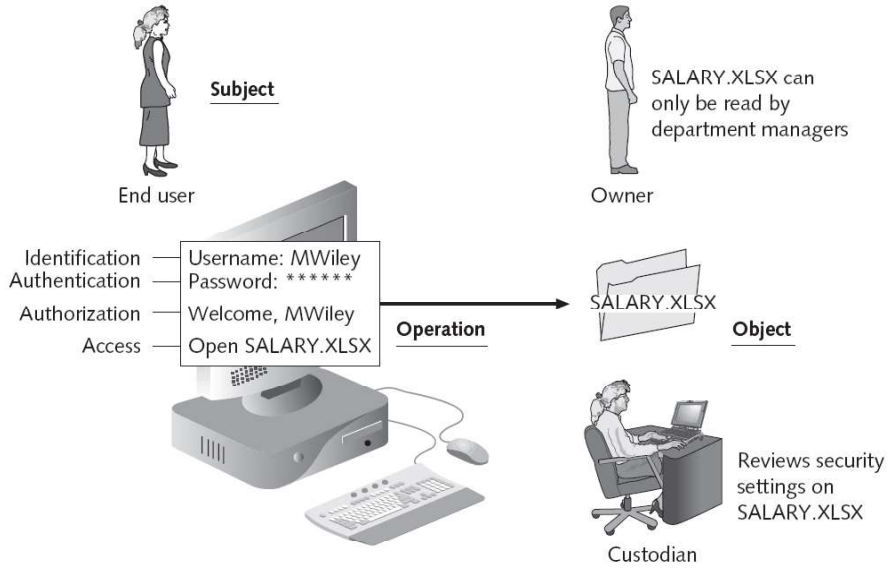


Figure 7-1 Access control process and terminology

Access Control Models

- Mandatory Access Control
- Discretionary Access Control
- Role-Based Access Control
- Rule-Based Access Control

Mandatory Access Control (MAC) model

- Most restrictive model—used by the military
- Objects and subjects are assigned access levels
- Unclassified, Classified, Secret, Top Secret
- The end user cannot implement, modify, or transfer any controls

Discretionary Access Control (DAC) model

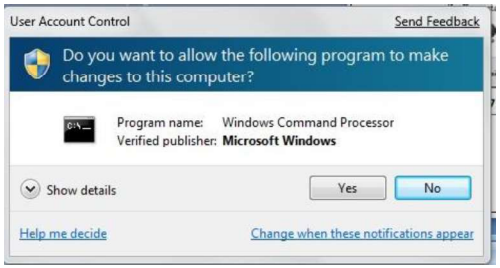
- The least restrictive--used by Windows computers in small networks
- A subject has total control over any objects that he or she owns
- Along with the programs that are associated with those objects
- In the DAC model, a subject can also change the permissions for other subjects over objects

DAC Has Two Significant Weaknesses

- It relies on the end-user subject to set the proper level of security
- A subject's permissions will be "inherited" by any programs that the subject executes

User Account Control (UAC)

- Asks the user for permission when installing software



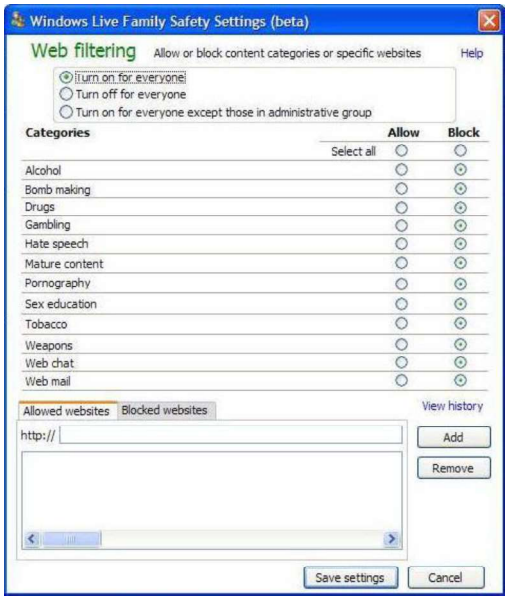
- Principle of **least privilege**
  - Users run with limited privileges by default
  - Applications run in standard user accounts
  - Standard users can perform common tasks

Role Based Access Control (RBAC) model

- Sometimes called **Non-Discretionary Access Control**
- Used in Windows corporate domains
- Considered a more "real world" approach than the other models
- Assigns permissions to particular roles in the organization, such as "Manager" and then assigns users to that role
- Objects are set to be a certain type, to which subjects with that particular role have access

Rule Based Access Control (RBAC) model

- Also called the **Rule-Based Role-Based Access Control (RB-RBAC)** model or **automated provisioning**
- Controls access with **rules** defined by a custodian
  - Example: Windows Live Family Safety



Access Control Models (continued)

Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

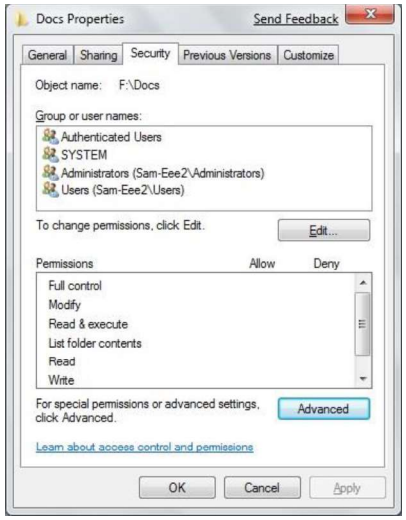
Table 7-3 Access control models

Logical Access Control Methods

Access Control Methods

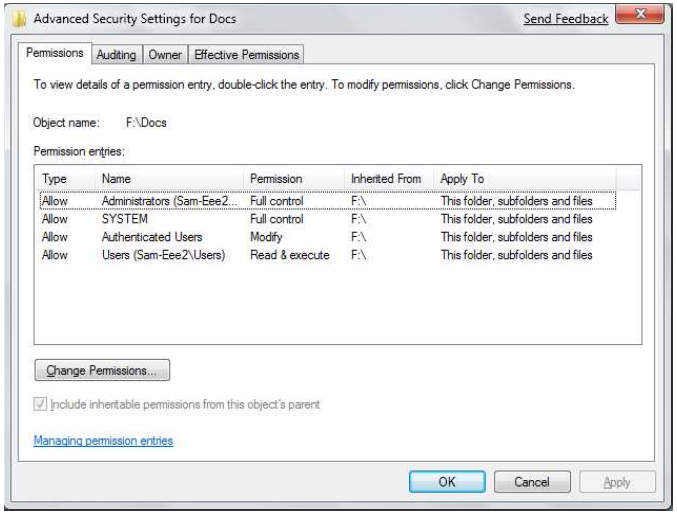
- The methods to implement access control are divided into two broad categories
  - **Physical access control** and
  - **Logical access control**
- Logical access control includes
  - Access control lists (ACLs)
  - Group policies
  - Account restrictions
  - Passwords

Access Control List (ACL)



- A set of permissions attached to an object
- Specifies which subjects are allowed to access the object
- And what operations they can perform on it
- Every file and folder has an ACL
- **Access control entry (ACE)**
  - Each entry in the ACL table in the Microsoft Windows, Linux, and Mac OS X operating systems

Advanced Security Settings in Windows 7 Beta



Group Policy

- A Microsoft Windows feature that provides centralized management and configuration of computers and remote users
- Using the Microsoft directory services known as Active Directory (AD)
- Group Policy is used in corporate domains to restrict user actions that may pose a security risk
- Group Policy settings are stored in **Group Policy Objects (GPOs)**

Account Restrictions

- **Time of day restrictions**
  - Limit when a user can log on to a system
  - These restrictions can be set through a Group Policy
  - Can also be set on individual systems
- **Account expiration**
  - The process of setting a user's account to expire
  - Orphaned accounts are user accounts that remain active after an employee has left an organization
    - Can be controlled using account expiration

Passwords

- The most common logical access control
- Sometimes referred to as a logical token
- A secret combination of letters and numbers that only the user knows
- A password should never be written down
  - Must also be of a sufficient length and complexity so that an attacker cannot easily guess it (password paradox)

Access Control Matrix

- Describes protection state precisely;
- Describes rights of each subject with respect to every other entity;
- State transitions change elements of matrix;

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

Physical Access Control

Physical Access Control

- Physical access control primarily protects computer equipment
  - Designed to prevent unauthorized users from gaining physical access to equipment in order to use, steal, or vandalize it
- Physical access control includes computer security, door security, mantraps, video surveillance, and physical access logs

Video Surveillance

- **Closed circuit television (CCTV)**
  - Using video cameras to transmit a signal to a specific and limited set of receivers
- Some CCTV cameras are fixed in a single position pointed at a door or a hallway
- Other cameras resemble a small dome and allow the security technician to move the camera 360 degrees for a full panoramic view

Physical Access Log

- A record or list of individuals who entered a secure area, the time that they entered, and the time they left the area
- Can also identify if unauthorized personnel have accessed a secure area
- Physical access logs originally were paper documents
  - Today, door access systems and physical tokens can generate electronic log documents

Network Performance

Speed

- Network speed, also known as data transfer rate, refers to **the speed at which data is transferred between two devices on a network**. It is usually measured in bits per second (bps) or bytes per second (Bps). Network speed can vary depending on the type of network, the devices used, and the distance between them

How to Measure Network Speed

- Speed Test Websites: This is a simple and easy-to-use method that can provide a quick estimate of your network speed. Speed test websites like Speedtest.net, Fast.com, or Google Speed Test allow you to check your network's download and upload speeds by sending and receiving data packets to and from a server.
- Network Performance Monitoring Tools: There are several network performance monitoring tools available that can provide detailed insights into network speed and other performance metrics. These tools can monitor network traffic, identify performance bottlenecks, and provide real-time alerts when performance issues arise.
- Command Line Tools: Command line tools like Ping, Traceroute, and IPERF are commonly used to measure network speed and performance. These tools send packets of data between devices and measure the time it takes for the packets to travel back and forth, providing a measure of network latency and throughput.
- Network Traffic Analysis: Network traffic analysis tools can be used to capture and analyze network traffic, providing insights into network speed, packet loss, and other performance metrics. These tools can help identify performance issues and optimize network configurations to improve speed and efficiency.

Bandwidth

- Bandwidth refers to **the maximum amount of data that can be transmitted over a network connection in a given period of time**. It is typically measured in bits per second (bps) or bytes per second (Bps). For example, a network connection with a bandwidth of 100 Mbps can transmit 100 million bits of data per second.

Measure Bandwidth

- Speed Test Websites: There are many free online tools that allow you to test your internet speed and measure your bandwidth. These websites typically work by downloading and uploading files of varying sizes and measuring the time it takes to complete the transfers.
- Network Performance Monitoring Software: You can use network performance monitoring software, like Obkio, to monitor your network bandwidth usage and overall network performance. These tools can provide real-time and historical data on your network bandwidth usage, as well as identify bottlenecks and other issues.
- Command-Line Tools: You can use tools like iperf or speedtest-cli to measure your bandwidth. These tools allow you to test your bandwidth between two devices on a network.
- Network Hardware: Some network hardware, like routers and switches, have built-in tools for measuring bandwidth. These tools may allow you to view real-time and historical data on your network usage, as well as configure quality of service (QoS) policies to prioritize certain types of traffic.

Throughput

- Throughput refers to **the actual amount of data that is successfully transmitted over a network connection in a given period of time**. It is also measured in bits per second or bytes per second. The throughput of a network connection can be affected by a number of factors, including network congestion, packet loss, and network latency.

Measure Throughput

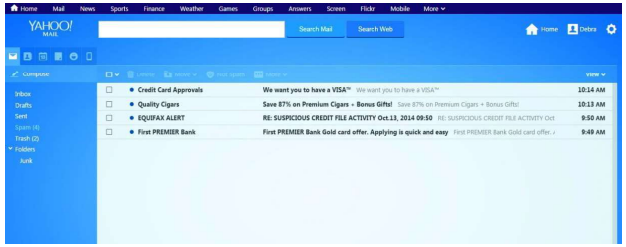
- Network Performance Monitoring Software: Network performance monitoring software like Obkio, can measure the throughput of your network over time. These tools provide real-time and historical data on network performance and can help identify trends and potential network issues related to throughput.
- Network Testing Tools: There are various network testing tools available that can measure the throughput of your network. One popular tool is iPerf, which can be used to measure both TCP and UDP throughput.
- Packet Capture Analysis: Packet capture analysis tools capture and analyze network traffic, which can be used to calculate the actual throughput. By analyzing the packet capture, you can calculate the total amount of data transferred over the network during a given time period and use that to calculate the throughput.
- Device or Application Monitoring: Many devices and applications have built-in monitoring tools that can be used to measure throughput. For example, some routers and switches have built-in tools to measure the throughput of individual ports, and some database management systems have tools to monitor the throughput of database queries.

Malware:
Spam and Cookies

- Includes different types of programs designed to be harmful or malicious
  - ✓Spam
  - ✓Adware and spyware
  - ✓Viruses
  - ✓Worms
  - ✓Trojan horses
  - ✓Rootkits

Malware: Pick Your Poison
Spam and Cookies

- Spam
  - Spamming is sending mass unsolicited emails
  - Messages are called spam
  - Other forms:
    - Fax spam
    - IM spam
    - Text spam



Malware: Pick Your Poison
Spam and Cookies

- Cookies
  - Installed without your permission
  - Help websites identify you when you return
    - Track websites and pages you visit to better target ads
  - May collect information you don't want to share

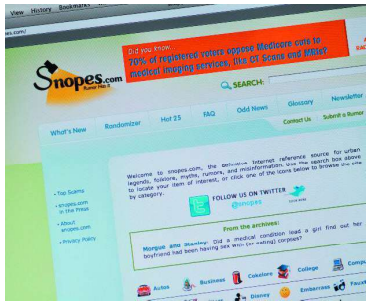
Adware and Spyware

- Adware
  - Pop-ups or banner ads
  - Generate income
  - Use CPU cycles and Internet bandwidth
  - Reduce PC performance

- Spyware
  - Malware
  - Secretly gathers personal information
  - Usually installed by accident
  - Browser hijacker

Malware:
Viruses, Worms, Trojans, and Rootkits

- Virus - A program that replicates itself and infects computers
  - ✓Needs a host file
  - ✓May use an email program to infect other computers
  - ✓The attack is called the payload
  - ✓Check to see if message is a hoax



Viruses, Worms, Trojans, and Rootkits

- Logic Bomb
  - Behaves like a virus
  - Performs malicious act
  - Does not replicate
  - Attacks when certain conditions are met
- Time Bomb
  - A logic bomb with a trigger that is a specific time or date
    - April Fool's Day
    - Friday the 13th

- Worms
  - Self-replicating
  - Do not need a host to travel
  - Travel over networks to infect other machines
  - Conficker worm
    - First released in 2008
    - Reemerged in 2010 with new behaviors

- Botnet
  - Network of computer zombies or bots controlled by a master
  - Fake security notifications
  - Denial-of-service attacks
    - Cripples a server or network by sending out excessive traffic
- Trojan horse
  - Appears to be legitimate program
  - Actually malicious
  - Might install adware, toolbar, keylogger, or open a backdoor

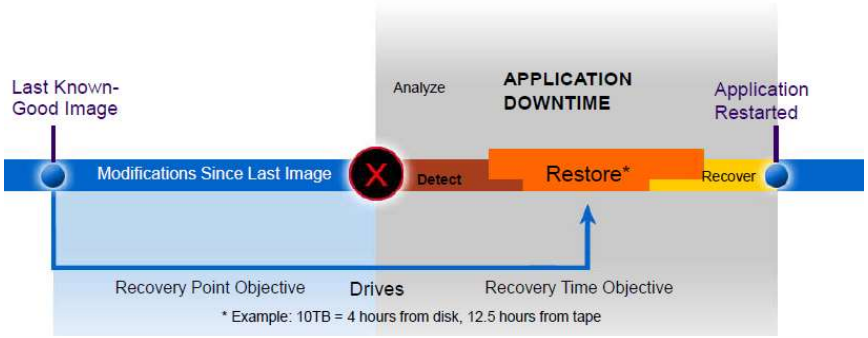
- Ransomware
  - Malware that prevents you from using your computer until you pay a fine or fee
  - Bitcoin is an anonymous, digital, encrypted currency
- Rootkit
  - Set of programs
  - Allows someone to gain control over system
  - Hides the fact that the computer has been compromised
  - Nearly impossible to detect
  - Masks behavior of other malware

Backup, Archive, and Replication

Introduction to Back & Restore

- The purpose of backup is to protect data from loss.
- The purpose of restore is to recover data that is temporarily unavailable due to some unexpected event.

Recovery Process



Why back is needed? Case Study

- **Ransomware**, which encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want.

Importance of Backup

- Determine which data is static and which is dynamic
  - Some OS installations are changed infrequently; few backups required
  - E-commerce may require continuous backups.
  - Understand the changing state of your client's data to determine an appropriate backup sched.
  - Organize with partitions

Importance of Backup

- Which Files Should Be Backed Up?
  - OS Binaries
  - Applications
  - Configuration Files
  - User files
  - Log files
- Backup of just user files is not enough.
- Should dump the log files, and configuration information

Proper Backup Procedure

- Choose your application
- Scheduling
- Implementation
- Inventory (content and media)
- Verify
- Automate
- Secure

Choose your Backup App

- Mac OS X :
  - Time Machine
- Linux/Unix :
  - tar (tape archive), cpio, dump
- MS Windows :
  - MS Windows XP & 7 includes Backup & Restore capability
  - Many commercial apps are available

Enterprise Level Backup Apps

- Paragon Backup & Recovery includes customer support
- Backup4All Professional
- GRBackPro7

Types of Backups

- Full Backup
- Partial backup
  - Differential Backup
  - Incremental Backup

Full Backup

- A complete backup means full backup of the entire server or computer system.
- If you are backing up of an entire server, then it includes all the volumes, directories and files.
- And if you are backing up your computer system, then it includes all the drives, directories and files.

Full Backup

Full Backup (Pros)

Pros

- Provides a complete copy of data
- Easy to manage:
  - Done less frequently than other types of backups due to cost and resource requirements:
    Monthly, Quarterly, semi-annually, annually.

Full Backup (Pros)

Cons

- Usually requires more media space than either differential or incremental.
- Takes a long time to recover the full backup to a new disk.

Differential backup

- In a differential backup only those files are backed which have changed or modified since the last full backup.
- This backup method is very useful when you require the latest updated data.
- If you are using the same media for consecutive differential backups, the files which are backed up earlier can be overwritten by their updated versions.

Differential backup

Differential Backup (Pros)

- Redundancy
- Usually takes up less time and space than a full backup.
- If the differential backup grows to the size of the last full backup, then schedule a new full backup.

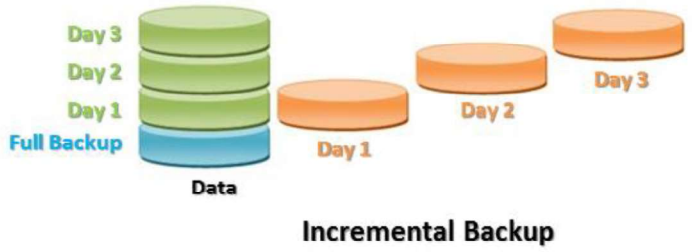
Differential Backup (Cons)

- Redundancy – potentially many unneeded copies of the same data.
- Subsequent differentials take longer and use more media space

Incremental backup

- In an incremental backup only those files are backed up which have changed or modified as well as those which are new since the last incremental backup.
- If you are using the same media for consecutive incremental backups, the files which are backed up earlier cannot be overwritten by their updated versions.

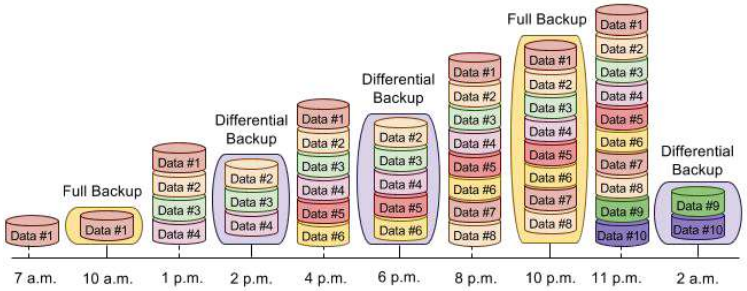
Incremental backup



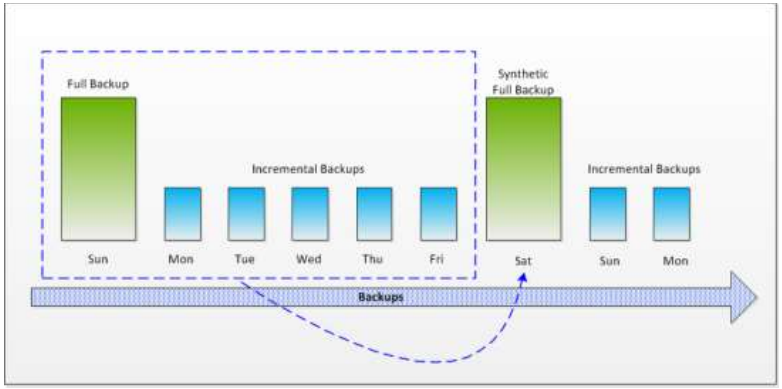
Incremental backup

- Pros
  - Keeps a revision history of actively changing files
  - Fastest backup type
  - Uses the least amount of media to complete a single backup
- Cons
  - Much more difficult to manage

Backup schedule-example1



Backup schedule-exampl2



Schedule Example-3

- Full backup twice per year
- Differential each first Saturday morning of each month that is not scheduled for a full backup
- Incremental each Saturday morning that is not scheduled for a Full or Differential

Backup Devices

- Tape Backup Devices
  - Cartridge Tape Drive
  - 8-mm Tape Drive
  - Digital Audio Tape Drive
  - Linear Tape Open
  - Digital Linear Tape
  - Jukebox/Stacker Systems
- Optical Backup Devices
- Magneto-optical Backup Devices
- Disk Systems As Backup Devices
  - RAID Disk Arrays
  - Problems with Disks As Backup Devices
- High-Density Removable Media Backups

Tape Backup

- Tape historically has been the preferred backup media for very large data storage environments.
- Tape has a useful life span.
- Tape can be very robust for storage
- Easy to transport
- Some tape formats are more reliable than others.

Backup Inventory

- The media label information:
  - Date
  - System identifier
  - Partition name(s)
  - Backup category: full, differential, incremental

Restore

- Common reasons for restores
  - Accidental file deletion
  - Disk failure
  - Disaster recovery
    - Fire, flood, earthquake, hacker attack, sabotage, terrorist attack, etc.

Replication

- Remote data replication is sometimes assumed to be equivalent to backup, but this is not the case.
- Replication solutions can be either synchronous or asynchronous, meaning transfer of data to a remote copy is achieved either immediately or with a short time delay. Both methods create a secondary copy of data identical to the primary copy, with synchronous solutions achieving this in real time.
- This means that any data corruption or user file deletion is immediately (or very quickly) replicated to the secondary copy, therefore making it ineffective as a backup method.
- Another point to remember with replication is that only one copy of the data is kept at the secondary location. This means that the replicated copy doesn't include historical versions of data from preceding days, weeks and months, unlike a backup.

Archiving

- Archiving, on the other hand, is the retention of data for lengthy periods, usually years, sometimes decades, and moves the data from its primary location.
- "Backup is for restoring a file, object, database, volume or system based on some recovery time objective and recovery point objective, whereas the archive is a picture of the data and its state at a point in time."
- key characteristics of archiving systems. These include: "Indexing and metadata management for search, replication, cloning, secure shred, Worm (write-once read-many), along with compliance or regulatory items."
- In addition, archiving includes movement of data off production storage systems onto the archive medium, driven by retention policies. "Data mover tools may be tightly or loosely integrated with the destination or target devices and in some cases even have overlapping features.
- The third component which does not attract as much awareness is the most important, however – how the data mover tools integrate with different applications, which need to be configured to use rules or policies to archive the data, or present it to the data mover.
- Another element of the distinction can also be the medium. Media used for backup need to be able to ingest vast quantities of data quickly during a limited time window. As a result, disk rather than tape has increasingly been used for the added performance it provides, as well as providing faster access times to recently backed-up data.
- Archives, on the other hand, have increasingly become tape-based, which offers the advantage of being cheap and robust over long periods of time, while the fairly slow speed of recovery is rarely a problem as occurrences are rare.

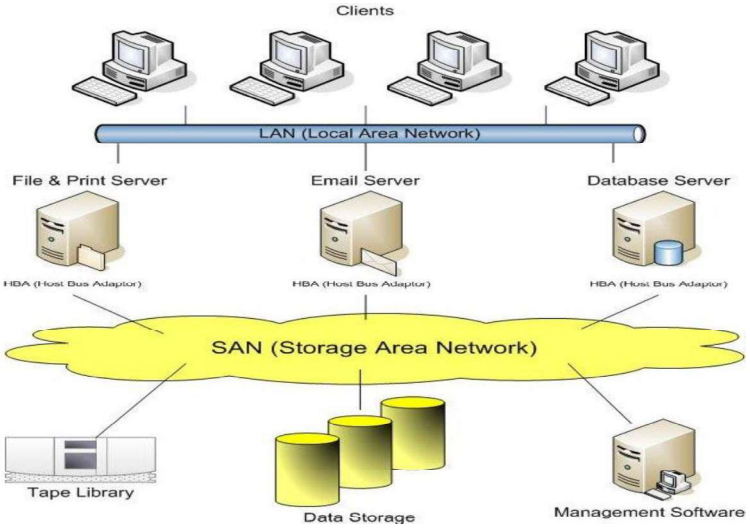
Storage Networking and Virtualization

SAN

- A storage area network (SAN) is a secure high-speed data transfer network that provides access to consolidated block-level storage. SAN makes a network of storage devices accessible to multiple servers. SAN devices appear to servers as attached drives, eliminating traditional network bottlenecks.
- SANs are sometimes also referred to as SAN storage, SAN network, network SAN, etc.

Features of SAN

- Separate network handling storage needs.
- Detaches storage tasks from specific servers.
- Shared storage facility across high-speed network.
- Hard disks, tape libraries, CD arrays.
- Improved client-server storage access
- Direct storage to storage communication for backup
- Centralized management
- Storage consolidation/shared infrastructure
- High availability and disaster recovery
- High bandwidth
- Scalabilities
- Shared data



Principle, Goal and Interest

- **Principle:** centralized storage resources and federate them with high speed network.
- **Goals:** simplified management, autonomous storage units with end host.
- **Interests:** ease of data management (store operations, backups. Restore….)

Storage Controller-The heart of SAN

- It is a software/hardware entity that manages one or more storage containing entities and provides a simple and abstract view of the managed devices.
- Storage controller-Location in the SAN: It can be found →

1. **Internal to the host/server**
   Disadvantages: Does not allow sharing of the storage system between multiple hosts/servers.
2. **In the same enclosure with the disk arrays/tape drives**
   Disadvantage: controller capacity limited by the capacity of enclosure
3. **A standalone entity, connected to the SAN and manages other disk arrays and Controllers: Advantages:**

i. Supports managing more than one enclosure
ii. Facilitates redundant controllers and makes backups simpler.
iii. Facilitates multi-vendor systems and interoperability

Benefits of SAN

- In general, there are a few basic areas where employing a SAN can reduce overall storage costs significantly:
- **Availability:** SAN storage is in general more reliable than DAS attached disk. This can save your company money by avoiding application outages. The cost of an hour of application downtime varies from company to company but can exceed millions in some cases.
- **Disk utilization:** When buying server-attached storage most people buy more than they currently need so they can "grow into" the storage. The space that is unutilized is wasted until it is needed. In SANs, that space can be "assigned" to any server that needs more storage, thus deferring new storage purchases.
- **Management:** Using DAS you need to manually install new disks to add storage. In a SAN you can remotely assign it to a server. No downtime and perhaps not even a reboot is required if the OS can handle it. You can manage ALL your storage GLOBALLY from a single console.
- **Backup:** Using snapshots and data replication can save your backside when disasters happen and using a SAN for centralizing data backup can improve recovery time dramatically while reducing overall costs by sharing tape resources and eliminating backup windows.

Virtualization

- Desktop Virtualization
- Server Virtualization
- Network Virtualization
- Storage Virtualization
- Application Virtualization

Vendors of Virtualization

- Vmware
- ORACIE VM
- CITRIX
- MICROSOFT

Benefits from Virtualization

- Save money and energy
- Simplify management

Desktop Virtualization

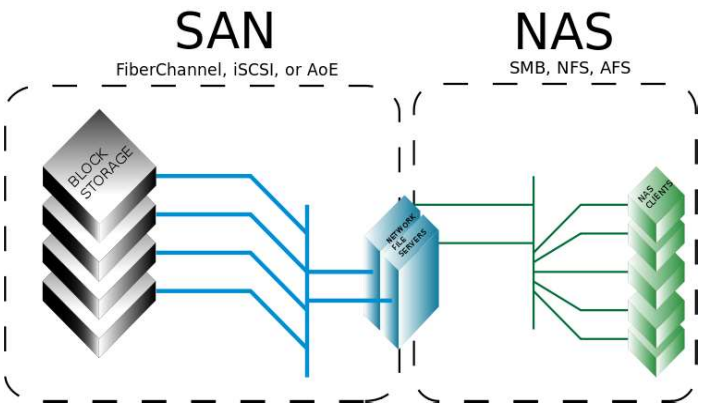
- VMware Workstation (Local)
- Microsoft Virtual PC (Local)
- Citrix XenDesktop (Centralized)

Components of Virtual Machines?

- Configuration file
- Hard disk file(s)
- Virtual machine state file
- In-memory file

NAS

- A ***n**etwork-**a**ttached **s**torage* (NAS) device is a server that is dedicated to nothing more than file sharing. Network-attached storage does not provide any of the activities that a server in a server-centric system typically provides, such as email, authentication or file management.
- **Description:** A NAS unit is a computer connected to a network that provides only file-based data storage services to other devices on the network. Although it may technically be possible to run other software on a NAS unit, it is usually not designed to be a general-purpose server. For example, NAS units usually do not have a keyboard or display, and are controlled and configured over the network, often using a browser. A full-featured operating system is not needed on a NAS device, so often a stripped-down operating system is used.



Benefits of NAS

1. Improve performance
2. Reduced storage capacity requirement
3. Increase reliability
4. Reduce management cost
5. Improve scalability
6. Improve security
7. Increase data availability
8. Eliminate backup issues