**SECTION 4 Computer Networks**

### 4.a. Modem

The word, **modem**, is derived from the combination of the words, **modulate**, to change into an analogue signal, and **demodulate**, to convert an analogue signal into a digital signal.

Both the sending and receiving ends of a standard telephone line must have a dial-up modem for data transmission to occur. The modem therefore is used to connect computers using phone lines.

### 4.b. Analogue and Digital Data

**Analogue Signal**

An analogue signal consists of a continuous electrical wave. In an analogue system data is transmitted in continuous wave form. It is called analogue because the mode of transmission is analogous to our perception of events. So, for example, we perceive sound as a continuous, modulating pattern of pitch and volume. Therefore, in an analogue system, sound is represented as an unbroken waveform. Analogous systems can therefore represent an infinite range of values.

**Digital Signal**

A digital signal consists of individual electrical pulses that represent bits grouped together into bytes. Computers store and manipulate data in a digital format. Specifically, they use a binary number system whereby all data is reduced to a series of two digits: 0 and 1.

![Digital signal vs Analogue signal](image)

### 4.c. Conversion of Analogue and Digital Data

A modem is needed because the computer processes data as digital signals while most telephone lines use analogue signals. Without this conversion, it is not possible for the computer to transmit data over telephone lines.

### 4.d. Advantages/Disadvantages of Network Environments

**Advantages**

- **Facilitating communications** – people can communicate via email, instant messaging, chat rooms, blogs, video telephone calls, video conferencing, Internet telephony, wireless messaging services and groupware.
- **Sharing hardware** – in a networked environment, each computer on the network has access to hardware on the network. Business and home users network their hardware to save money. For example, if computers and a laser printer are connected to a network, the computer users each access the laser printer on the network, as they need it.
- **Sharing data and information** – in a networked environment, any authorized computer user can access data and information stored on other computers on the network. A large company, for example, might have a database of customer information. Any authorized person, including a mobile user with a PDA or smart phone connected to the network, has access to the database.
- **Sharing software** – users connected to a network have access to software on the network. To support multiple users’ access of software, most vendors sell network versions or site licenses of their software, which usually cost less than buying individual copies of the software.
software for each computer.

- **Transferring funds** – called electronic funds transfer (EFT), it allows users connected to a network to transfer money from one bank account to another via transmission media.
- Easier to back up data held on a file server than on many individual machines.

**Disadvantages**

- There is just **too much information available**. Example, a search for the word “Shakespeare” comes up with 60,400,000 web pages. This can hinder our search for the information that we need.
- Another problem with the Internet is that **no one controls it**. That means that anyone can create a website saying anything that they want to and they cannot be stopped. Always be careful not to believe everything that you read on the Internet.
- **Fraud and theft** are also common on networks. Be careful.
- Users become dependent on them; if for example the network file server develops a fault, then many users will be unable to run application programs.
- If the network stops operating then it may not be possible to access various hardware and software resources.
- The efficiency of a network is very dependent on the skill of the system manager. A badly managed network may operate less efficiently than stand-alone machines.
- It is difficult to make the system secure from hackers.
- As traffic increases on the network the performance degrades unless it is properly designed.

**4.e. User ID and Password**

The network administrator uses the network OS to establish permissions to resources. These permissions define who can access certain resources and when they can access those resources.

**User ID**

A user name, or user ID, is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user.

**Password**

A password is a private combination of characters associated with the user name that allows access to certain computer resources. Some operating systems allow the network administrator to assign passwords to files and commands, restricting access to only authorized users.

**4.f. Communication Methods**

**4.f.1. Fax**

A fax is a document sent or received via a fax machine. A fax machine is a device that codes and encodes documents so that they can be transmitted over telephone lines. The documents can contain text, drawings, or photographs, or can be handwritten.

Many computers include fax capability by using a fax modem. A fax modem is a modem that allows you to send electronic documents as faxes. A fax modem transmits these faxes to a fax machine or to another fax modem. When a computer receives a fax, users can view the fax on the screen, saving the time and expense of printing. If necessary, you can print the fax.

**Advantages**

- Faxed signed document is legally acceptable
- Faxes cannot be hacked into
- Faxes cannot be affected by virus

**Disadvantages**

- Fax can be seen by anyone in the company / not confidential
- Paper can jam in the fax machine
- May not be readable when it arrives
- Receiver's fax line may be continually engaged
- Receiver's fax may be out of paper
- Receiver's fax may not be switched on
4.f.2. Email

Short for electronic mail, the transmission of messages and files via a computer network. You use an e-mail program to create, send, receive, forward, store, print and delete e-mail messages. The message can be simple text or can include an attachment such as a word processing document, a graphic, an audio clip or a video clip.

Facilities of Email

- send a message anywhere in the world for the price of a local call
- attach files such as documents, photographs, maps, executable programs
- keep an address book of people you regularly email.
- Send the same letter to a group of people simultaneously
- reply to an email simply by clicking on the reply button, inserting text from the original message as required
- forward a received message with comments on to an individual or group
- with the right software or a web-based email address such as Hotmail, pick up your mail from anywhere in the world, useful for example while traveling
- join a mailing list and get free information sent to you on a regular basis.

Advantages of Email

- It is cheaper than fax or telephone for messages sent over long distances
- You can email someone in America, for example, without having to worry about time zones – the messages will be picked up at a convenient time.
- You receive an answer much more quickly than by mail, and it is preferable to leaving a message on a telephone answering machine, as you know when it has been received.
- It is easy to use and encourages friendly conversation and directness – you don't have to be formal in a business email, and rules about the correct way to set out a letter simply don't apply. It breaks down barriers and cuts across hierarchies, which helps effective communication.

Disadvantages of Email

- Perhaps because it is so direct, it can be easy to offend people without meaning to.
- Busy people may be overloaded with email; it can be a bit depressing to get your mail at 9 am and find you have 53 emails waiting to be answered. Junk mail can also be a problem.
- Viruses can be spread in email attachments. You should always virus-check attached files before opening them, even if they are sent by a friend, as viruses can be passed on unwittingly.

4.f.3. Bulletin Boards

A Bulletin Board System, or BBS, is a computer system running software that allows users to connect and login to the system using a terminal program. Originally BBSes were accessed only over a phone line using a modem, but by the early 1990s some BBSes allowed access via a Telnet or packet radio connection.

Once a user logged in, they could perform functions such as downloading or uploading software and data, reading news, and exchanging messages with other users. Many BBSes also offered on-line games, in which users could compete with each other, and BBSes with multiple phone lines often offered IRC-like chat rooms, allowing users to meet each other.

4.f.4. Tele/Video Conferencing

Video conferencing is a real-time meeting between two or more geographically separated people who use a network to transmit audio and video data. Each participant has a video camera (webcam), microphone and speaker attached to their computer. As the participants speak, their voices are carried over the network and played back to the other participants' speakers. The images captured by the cameras are displayed on the other participants' computer monitors.
Hardware required
- Webcam/small video camera
- Microphones
- Speakers
- Modem

How it works
- Employees must be connected on-line (they need to access the Internet) in order to work.
- Images of the employees appear on the screen in real time.
- Software is needed in each computer to operate the conference.
- Employees can be heard by all the other employees in the conference.

Advantages
- Saves traveling time
- Do not have to pay for conference room
- Do not have to hire transport
- Conferences can be called at short notice
- Don't have to carry bulky documents to conference
- Disabled participants do not have to travel

Disadvantages
- Different time zones make it difficult to have a video conference between people in different countries
- Start up costs can be high/equipment can be expensive to buy
- Communication link can go down/reception can be poor
- Equipment can fail
- Can seem impersonal
- Pictures and sound can be out of synchronization

4.g. LANs, WLANs and WANs

LAN
A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network, called a node, often shares resources such as printers, large hard disks, and programs. Often, the nodes are connected via wires.

Wireless Local Area Network
Local area network that uses no physical wires. Computers and devices that access a wireless LAN must have built-in wireless capability or the appropriate wireless network card, PC Card, or flash card. Very often, a WLAN communicates with a wired LAN for access to its resources, such as software, hardware, and the Internet.

WAN
A wide area network (WAN) is a network that covers a large geographic area (such as a city, country, or the world) using a communications channel that combines many types of media such as telephone lines, cables, and radio waves. A WAN can be one large network or can consist of two or more LANs connected together.

WANs are very common and are not necessarily Internet based.

4.h. Difference between LAN, WLAN and WAN (and main characteristics of each)

<table>
<thead>
<tr>
<th></th>
<th>LAN</th>
<th>WLAN</th>
<th>WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>Usually in one building</td>
<td>Usually in one building</td>
<td>Covers a much larger area</td>
</tr>
</tbody>
</table>
4.i. Network Topologies

A network topology refers to the layout of the computers and devices in a communications network. Three commonly used network topologies are bus, ring and star. Networks usually use combinations of these topologies.

Bus Network
A bus network consists of a single central cable, to which all computers and other devices connect. The bus is the physical cable that connects the computers and other devices. The bus in a bus network transmits data, instructions and information in both directions. When a sending device transmits data, the address of the receiving device is included with the transmission so the data is routed to the appropriate receiving device.

**Advantages** – inexpensive and easy to install. Computers and other devices can be attached and detached at any point on the bus without disturbing the rest of the network. Failure of one device usually does not affect the rest of the bus network.

**Disadvantage** – If the bus is inoperative, the network remains inoperative until the bus is back in working order.
- Cable failure is difficult to isolate
- Network performance degrades under a heavy load

Ring Network
On a ring network, a cable forms a closed loop with all computers and devices arranged along the ring. Data transmitted on a ring network travels from device to device around the entire ring, in one direction. When a computer or device sends data, the data travels to each computer on the ring until it reaches its destination. The ring topology primarily is used for LANs, but also is used in WANs.

**Advantages** – it can span a larger distance than a bus network.
- There is no dependence on a central computer or file server, and each node controls transmission to and from itself.
- Transmission of messages around the ring is relatively simple, with messages traveling in one direction only.
- Very high transmission rates are possible.

**Disadvantage** – more difficult to install. If a computer or device on a ring network fails, all devices before the failed device are unaffected, but those after the failed device cannot function.

Star Network
On a star network, all of the computers and devices on the network connect to a central device, thus forming a star. The central device that provides a common connection point for nodes on the network often is called the hub/switch. All data that transfers from one node to another passes through the hub.

**Advantages** – fairly easy to install and maintain. Nodes can be added to and removed from the network with little or no disturbance to the network. If one node fails, only that node is affected.
- Simple to isolate faults
- Consistent performance even when the network is being heavily used.
- No problems with 'collisions' of data since each station has its own cable to the server.
- The system is more secure as messages are sent directly to the central computer and cannot be intercepted by other stations.
- Different stations can transmit at different speeds.

**Disadvantage** – If the hub fails, the entire network is inoperative until the hub is repaired.
- May be costly to install because of the length of cable required. The cabling can be a substantial part of the overall cost of installing a network.
4.j. Characteristics and purpose of Common Network Environments

Intranet
An intranet, which is short for INTernal Restricted Access NETwork, is an internal network (usually a LAN) that uses Internet technologies. These networks of computers are usually available solely within a company or organization and provide good security for confidential information and therefore usually the pages are controlled by passwords. It may also provide secure email communication. Intranets generally make company information accessible to employees and facilitate working in groups.

An intranet essentially is a small version of the Internet that exists within an organization. It has a Web server, supports multimedia Web pages coded in HTML, and is accessible via a Web browser such as Microsoft Internet Explorer or Netscape Navigator. Users update information on the intranet by creating and posting a Web page, using a method similar to that used on the Internet.

Internet
The Internet, which stands for INTERnational NETwork, is the worldwide collection of networks that connects millions of businesses, government agencies, educational institutions, and individuals. Each of the networks on the Internet provides resources that add to the abundance of goods, services, and information accessible via the Internet. People can have unlimited access to the Internet from anywhere and acquire a great amount of information from it.

<table>
<thead>
<tr>
<th>Difference between Intranet and Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet – INTERnational NETwork</td>
</tr>
<tr>
<td>It is a Wide Area Network (WAN)</td>
</tr>
<tr>
<td>Can access it from anywhere</td>
</tr>
<tr>
<td>Unlimited access</td>
</tr>
</tbody>
</table>

4.k. Common Network Devices

Hubs
The central device that provides a common connection point for nodes on a network. Hubs can be used to connect networks as well as provide the central connection point in a star network. When used to connect networks, some hubs are also routers. That is, the hub receives data from many directions and then forwards it to one or more destinations.
Routers
A communications device that connects multiple computers or other routers together and transmits data to its correct destination on the network. A router can be used on any size of network. On the larger scale, routers along the Internet backbone forward data packets to their destination using the fastest available path. For smaller business and home networks, a router allows multiple computers to share a single high-speed Internet connection. These routers connect from 2 to 250 computers.
Bridges
Bridges are intelligent devices that connect networks using the same protocol.
Switches
A switch is a hardware that decides how to route Internet transmissions. Switches are similar to software routers, but faster and less flexible.
Proxy Servers
A proxy server is a server that sits between a client application, such as a Web browser, and a real server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache.

4.1. Confidentiality and Data Security in Common Network Environments

Information transmitted over networks has a higher degree of security risk than information kept on a company's premises. In a business, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater.
Internet and network attacks that jeopardize security include computer viruses, worms and Trojan horses; denial of service attacks; and spoofing.
Another type of computer security risk is unauthorized access and use. Unauthorized access is the use of a computer or network without permission. Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities. Unauthorized use includes a variety of activities: an employee using an organization's computer to send personal e-mail messages, an employee using the organization's word processing software to track his or her child's soccer league scores, or someone gaining access to a bank computer and performing an unauthorized transfer.
Ways in which personal data might be misused
- Looking at other people's data
- Changing other people's data
- Deleting other people's data
- Spreading data around

4.m. Encryption in Common Network Environments

4.m.1. Need for encryption

Encryption - the process of encoding (changing) data and information into unreadable form (so that it seems meaningless when intercepted). Network administrators can set up a network to encrypt data as it travels over the network to prevent unauthorized users from reading the data. When an authorized user attempts to read the data, it automatically is decrypted, or converted back into a readable form. This encryption is needed because it provides security for sensitive data, especially during transmission. When a hacker succeeds in intercepting the data, the data cannot be understood by hackers because it is encrypted. Therefore the hacker cannot inflict damage through the use of the data.

4.m.2. Authentication Techniques

Identification – verifies that an individual is a valid user.
Authentication – verifies that the individual is the person he or she claims to be.
Three methods of identification and authentication include user names and passwords,
possessed objects, and biometric devices.

User names and passwords

A user name, or user ID, is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user. A password is a private combination of characters associated with the user name that allows access to certain computer resources. Most multiuser operating systems require that users correctly enter a user name and password before they can access the data, information and programs stored on a computer network. Many other systems that maintain financial, personal and other confidential information also require a user name and password as part of their login procedure.

Possessed objects

A possessed object is any item that you must carry to gain access to a computer or computer facility. Examples of possessed objects are badges, cards, smart cards and keys. The card you use in an automated teller machine (ATM) is a possessed object that allows access to your bank account. Possessed objects often are used in combination with personal identification numbers (PINs). A PIN is a numeric password, either assigned by a company or selected by a user. PINs provide an additional level of security.

Biometric devices

A biometric device authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into a digital code that is then compared with a digital code stored in the computer verifying a physical or behavioral characteristic. If the digital code in the computer does not match the personal characteristic code, the computer denies access to the individual.

Data Transmission

- Data transmission occurs between a transmitter and a receiver.
- The media may be guided or unguided:
  - guided: twisted pair, coaxial cable, and fiber.
  - unguided: trough air, water, or vacuum.
  - Either type of transmission is based on electromagnetic waves.
- A direct link is the signal transmission path between two devices with no intermediate device other than repeaters and amplifiers.
- A guided medium is point-to-point if
  - it provides a direct link between two devices;
  - the medium is shared by only those two devices.
- In a multi-point configuration, more than two devices share the transmission medium.
- We distinguish 3 forms of transmission:
  - Simplex
  - Half Duplex
  - Full Duplex
• Simplex: Transmission in only one direction; one station is the transmitter, the other the receiver. Examples:
  o One-Way Street
  o Keyboard-Computer connection
  o Computer-Monitor connection
  o TV Broadcast
  o Can you think of other simplex examples?

• Half Duplex: Transmission in both directions possible, but NOT at the same time. Here, the attached stations are both, sender and receiver. Examples:
  o One-Lane Road with access control lights. While cars go in one directions, cars going the opposite way must wait.
  o Walkie-Talkies
  o CB-Radios
  o Traditional Ethernet (Coax or 10baseT)

• Full Duplex: Transmission in both directions simultaneously. Both stations can send and receive at the same time. Examples:
  o Regular 2-way street
  o Full-Duplex repeated Ethernet (Gbit Ethernet)

• Full Duplex transmission can be accomplished in two ways:
  o Separated physical transmission media
  o Divided channel capacity and separation of signals in different directions.