3.2 COMMUNICATION AND INTERNET TECHNOLOGIES

3.2.3 LOCAL AREA NETWORKS (LAN)

NETWORK BASICS

A computer network is a collection of computing devices that are connected in various ways to communicate and share resources. Email, instant messaging, and web pages all rely on communication that occurs across and underlying computer network. We use networks to share both intangible resources, such as files, and tangibles resources, such as printers.

Usually, the connections between computers in a network are made using physical wires or cables. However, some connections are wireless, using radio waves or infrared signals to convey data. Networks are not defined only by physical connections; they are defined by the ability to communicate.

Computer networks contain devices other than computers. Printers, for instance, can be connected directly to a network so that anyone on the network can print to them. Networks also contain a variety of devices for handling network traffic. We use the general term **host** to refer to any device on the network.

A key issue related to computer networks is the speed with which data is moved from one place to another on a network. We are constantly increasing our demand on networks as we rely on them to transfer more data in general. Multimedia components such as audio and video are large contributors to this increased traffic.

WHAT IS A LAN?

A Local-Area Network (LAN) connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN.

In TCP/IP networking, a LAN is often but not always use physical connection between nodes, such as Ethernet cables.

WHY ARE LANS USED?

LAN is used depending on the application that is needed. Using LAN for an entire company that is spread worldwide is just not practical. However where LAN becomes useful is when it allows a certain number of computers to all belong to the same network and communicate within that network.

This allows LAN to become a more accessible and quicker way of communication, with very little chance of any delay. Although this is not to say a user cannot experience delay through LAN. As the number of computers increases on a certain LAN, the speed of the resulting connection begins to become diluted.

TOPOLOGIES

The shape of a network, and the relationship between the nodes in that network is known as the **Network Topology**. The network topology determines what kind of functions the network can perform, and what the quality of communication will be between nodes.

Two well known types of Topologies are:

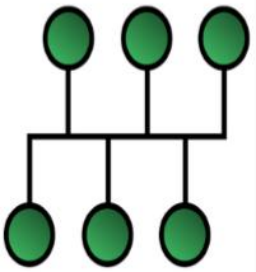
- **Bus topology**
- **Star topology**

BUS TOPOLOGY:

Bus topology is a specific kind of network topology in which all of the various devices in the network are connected to a single cable or line.

One way to think about a bus topology is that the line connected to all of the devices or nodes in the network is like an aisle along which a signal travels in order to find the node to which it is to be delivered. Typically, the cable in the bus topology has two end terminals that dampen the signal so that it does not keep moving from one end of the network to the other. In a bus network, every station receives all network traffic, and the traffic generated by each station has equal transmission priority.

Bus topologies are often valued for their simplicity and lower cost of implementation. However, one drawback is that if the central line is damaged, the entire network will go down. Also, it can be difficult to troubleshoot these kind of systems, and problems like data signal loss can occur with a longer backbone cable.



STAR TOPOLOGY:

Star topology is a network topology where each individual piece of a network is attached to a central node (often called a hub or switch). The attachment of these networks pieces to the central component is visually represented in the form similar to a star.

In Star topology, all the components of network are connected to the central device called "**Hub**" which may be a **Router** or a **Switch**. Unlike Bus topology, where nodes were connected to central cable, here all the workstations are connected to central device with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node by the help of "Hub".

All the data on the star topology passes through the central device before reaching the intended destination. Hub acts as a junction to connect different nodes present in Star Network, and at the same time it manages and controls whole of the network. Depending on which central device is

used, "Hub" can act as a repeater or signal booster. Central device can also communicate with other hubs of different network. Ethernet cable is often used to connect workstations to the central node.

An example of star topology is a radio station, where a single antenna transmits data directly to many radios. If there are 'n' number of nodes in a star topology connection, the connecting lines between the nodes should be 'n-1'.

Advantages:

As compared to Bus topology, it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of the central hub.

Easy to add and remove network components.

Failure of one node or link doesn't affect the rest of the network. At the same time it is easy to detect the fault and troubleshoot it.

Disadvantages:

Too much dependency on central device has its own drawbacks. If it fails, then whole network goes down.

The inclusion of a hub, router, or a switch increases the overall cost of the network.

Performance as well as capacity of the network is dependent on the central device.

WORKING BEHIND A WIRELESS NETWORK:

A wireless network servers the same purpose as a wired one – to link a group of computers. Because "wireless" doesn't require costly wiring, the main benefit is that it's generally easier, faster and cheaper to setup.

Wireless networks operate using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave association. When a RF current is supplied to an antenna, an electromagnetic field is created which is able to propagate through space.

The cornerstone of a wireless network is a device known as an **access point**. The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. Since wireless networks are usually connected to wired ones, an access point also often serves as a link to resources available on the wired network, such as an Internet connection.

In order to connect to an access point and join a wireless network, computers must be equipped with **wireless network adapters**.

Since the networks are wireless speed and range of the network may vary according to the technology being used. And in order to prevent unwanted users from connecting to the network, different encryption schemes are used to block out unwanted users. Examples are WEP, WPA, and WPA2.

HARDWARE USED TO SUPPORT A LAN:

1. Switch

A **network switch** is a device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports. Ethernet switches are the most common type. Mainstream Ethernet switches like those inside broadband routers support speeds up to 1 Gigabit per second. A switch uses hardware addresses to process and forward data to the target computer on the network.

2. Servers

A server is a computer or a device on a network that provides data to other computers on the same network. They also manage network resources. Many types of servers exist. Each type runs software specific to the purpose of the server.

There are many different types of servers. For example:

- **File Server:** a computer and storage device dedicated to storing files. Any user on the network can store files on the server.
- **Print server:** a computer that manages one or more printers.
- **Network server:** a computer that manages network traffic.
- **Database server:** a computer system that processes database queries.

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

While server software is specific to the type of server, the hardware is not as important. In fact, a regular desktop computer can be turned into a server by adding the appropriate software. For example, a computer connected to a home network can be designated as a file server, print server, or both.

While any computer can be configured as a server, most large businesses use rack-mountable hardware designed specifically for server functionality. These systems, often take up minimal space and often have useful features such as LED status lights and hot-swappable hard drive bays. Multiple rack-mountable servers can be placed in a single rack and often share the same monitor and input devices. Most servers are accessed remotely using remote access software, so input devices are often not even necessary.

While servers can run on different types of computers, it is important that the hardware is sufficient to support the demands of the server. For instance, a web server that runs lots of web scripts in real-time should have a fast processor and enough RAM to handle the "load" without slowing down. A file server should have one or more fast hard drives or SSDs that can read and write data quickly. Regardless of the type of server, a fast network connection is critical, since all data flows through that connection.

3. Network Interface Cards (NICs)

A NIC is a card that physically makes the connection between the computer and the network cable. It enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable.

Due to the popularity and low cost of the Ethernet standard, most new computers have a network interface built directly into the motherboard.

This is a picture of a wireless network card; usually plugged into laptop computers that do not have onboard wireless capabilities.

UNDERSTANDING ETHERNET AND CSMA/CD:

Ethernet is a local area technology, with networks traditionally operating within a single building, connecting devices in a close proximity. At most, Ethernet devices could have only a few hundred meters of cable between them, making it impractical to connect geographically apart locations.

In order for successful communication to take place between 2 computers on the same network, they must both understand the same protocols. A protocol refers to a set of rules that governs communication.

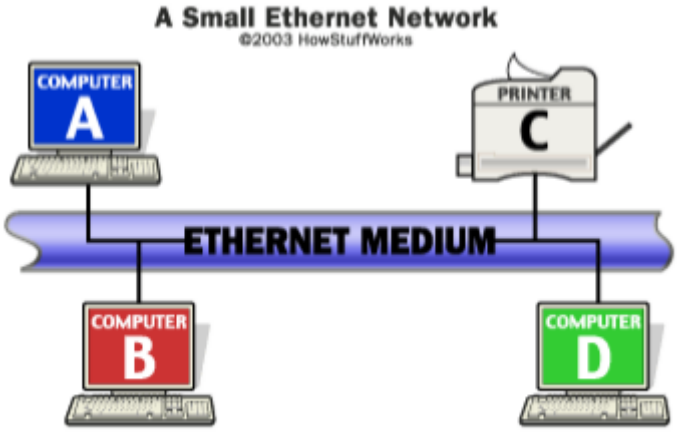
Ethernet follows a simple set of rules that govern its basic operation. To better understand these rules, it is important to understand the basics of Ethernet terminology.

- **Medium** – Ethernet devices attach to a common medium that provides a path along which the electronic signals will travel. Historically, this medium has been coaxial copper cable, but today it is more commonly a twisted pair or fiber optic cabling.
- **Segment** – We refer to a single shared medium as an Ethernet segment.
- **Node** – Devices that attach to that segment are stations or nodes.
- **Frame** – The nodes communicate in short messages called frames, which are variably sized chunks of information.

Frames are analogous to sentences in human language. In English, we have rules for constructions our sentences: We know that each sentence must contain a subject and a predicate. The **Ethernet protocol** specifies a set of rules for constructing frames. There are explicit minimum and maximum lengths for frames, and a set of required pieces of information that must appear in the frame. Each frame must include, for example, both a **destination address** and a **source address**, which identify the recipient and the sender of the message. The address uniquely identifies the node, just as a name identifies a particular person. **No two Ethernet devices should ever have the same address**.

ETHERNET MEDIUM

Since a signal on the Ethernet medium reaches every attached node, the destination address is critical to identify the intended recipient of the frame.



For example, in the figure above, when **computer B** transmits to **printer C**, **computers A** and **D** will still receive and examine the frame. However, when a station first receives a frame, it checks the destination address to see if the frame is intended for itself. If it is not, the station discards the frame without even examining its contents.

One interesting thing about Ethernet addressing is the implementation of a **broadcasting address**. A frame with a destination address equal to the broadcast address (simply called a broadcast, for short) is intended for every node on the network, and every node will both receive and process this type of frame.

CSMA/CD

The acronym **CSMA/CD** signifies **carrier-sense multiple access with collision detection** and describes how the Ethernet protocol regulates communication among nodes. While the term may seem intimidating, if we break it apart into its component concepts we will see that it describes rules very similar to those that people use in police conversation.

To help illustrate the operation of Ethernet, we will use an analogy of a dinner table conversation.

Let's represent our Ethernet segment as a dinner table, and let several people engage in polite conversation at the table (**represented as nodes**). The term **multiple access** covers what we already discussed above: When one Ethernet station transmits, all the stations on the medium hear the transmission, just as when one person at the table talks, everyone present is able to hear him or her.

Now let's imagine that you are at the table and you have something you would like to say. At the moment, however, I am talking. Since this is a polite conversation, rather than you immediately speaking up and interrupting me, you would wait until I finished talking before making your statement. This is the same concept described in the Ethernet protocol as **carrier sense**. Before a station transmits, it "listens" to the medium to determine if another station is transmitting. If the medium is quiet, the station recognizes that this is an appropriate time to transmit.

COLLISION DETECTION:

Carrier-sense multiple access gives us a good start in regulating our conversation, but there is one scenario we still need to address. Let's go back to our dinner table analogy and imagine that there is a momentary pause in the conversation. You and I both have something we would like to add, and we both "sense the carrier" based on the silence, so we begin speaking at approximately the same time. In Ethernet terminology, a **collision** occurs when we both spoke at once.

In our conversation, we can handle this situation gracefully. We both hear the other speak at the same time we are speaking, so we can stop to give the other person a chance to go on. Ethernet nodes also listen to the medium while they transmit to ensure that they are the only station transmitting at that time. If the stations hear their own transmission returning in an out of ordered form, as would happen if some other station had begun to transmit its own message at the same time, then they know that a collision occurred. A single Ethernet segment is sometimes called a **collision domain** because no two stations on the segment can transmit at the same time without causing a collision. When stations detect a collision, they cease transmission, wait a random amount of time, and attempt to transmit when they again detect silence on the medium.

The random pause and retry is an important part of the protocol. If two stations collide when transmitting at once, then both will need to transmit again. At the next appropriate chance to transmit, both stations involved with the previous collision will have data ready to transmit. If they transmitted again at the first opportunity, they would most likely collide again and again indefinitely. Instead, the random delay makes it unlikely that any two stations will collide more than a few times in a row.

LIMITATIONS OF ETHERNET:

A single shared cable can serve as the basis for a complete Ethernet network, which is what we discussed above. However, there are practical limits to the size of our Ethernet network in this case. A primary concern is the length of the shared cable.

Electrical signals propagate along a cable very quickly, but they weaken as they travel, and electrical interference from neighboring devices can scramble the signal. A network cable must be short enough that devices at opposite ends can receive each other's signals clearly and with minimal delay. This places a distance limitation on the maximum separation between two devices (called the **network diameter**) on an Ethernet network. Additionally, since in CSMA/CD only a single device can transmit at a given time, there are practical limits to the number of devices that can coexist in a single network. Attach too many devices to one shared segment and contention for the medium will increase. Every device may have to wait an inordinately long time before getting a chance to transmit.