Local and Wide Area Networks

4.1 Introduction

Understanding networking technologies begins by understanding the terminology used. Modern computer networks can be classified into one of three broad categories centering on the connection and geographic configuration strategy used with the physical devices:

- Local area network (LAN)
- Wide area network (WAN)
- Metropolitan area network (MAN)

Each of these network configurations has similarities but also has its own unique characteristics and deployment strategies.

4.2 Local Area Networks (LANs)

A local area network (LAN) is best identified using the following characteristics:

- Equipment is located geographically close together.
- Equipment is wholly owned and managed by the company (no leased services).
- Equipment is connected at high speed.

Each characteristic provides a wide range of possibilities, so it's necessary to look at each one more closely. What does it mean to have all equipment located geographically close together? Is it all in a single wiring closet? Is it located on a single floor of a building, in the entire building, or can it be in two buildings next to each other? The answer is that all of those descriptions could describe equipment that is part of the same LAN.

The second characteristic—that equipment is wholly owned and managed by the company—means that all of the switches, routers, hubs, physical wiring, servers, and workstations belong to the company and are under common administrative control. The same people implement, manage, and maintain all of the equipment in a LAN. This would not be true in a WAN in which equipment may be leased and people outside the company help maintain connectivity. (We cover WANs in the following section, "Wide Area Networks.")

The third characteristic is that equipment is connected at high speed. What is high speed? ARCnet was a LAN technology that connected computers at 2.5 megabits per second (Mbps). Early Token Ring connected systems at 4Mbps. Ethernet systems today can be connected at 1 Gigabit per second (1000 Mbps).

Clearly, the definition of fast may change with time or even with the people you talk to. In fact, any one of these characteristics viewed without the others is not enough to qualify a system as being a LAN—you need to consider all three. Exceptions to the rules will always exist, and individual characteristics will be subject to interpretation, but all three characteristics can be found in all LANs.

Let's look at this from the perspective of a fictitious company named CMP Ltd. CMP Ltd is a company currently located on a single floor of a building in Kampala, Uganda. CMP Ltd has all of its computers, printers, and servers connected using 100-Mbps switches and twisted-pair copper cabling. This configuration meets our three criteria for a LAN. Even if CMP Ltd grew to occupy every floor in the building, it would still be considered a LAN as long as all of the networking devices were connected at high speed, with equipment owned and managed by the company. LANs can even span buildings as long as the three basic characteristics are met. So when is a network not a LAN? We answer that question in the following sections, which cover WANs and MANs.

4.3 Wide Area Networks (WANs)

A network is considered a wide area network (WAN) based on characteristics that are opposite those for a LAN:

- Equipment is geographically dispersed.
- Connection services, and possibly equipment, are leased from telecommunications providers such as phone companies or Internet service providers (ISPs).
- Equipment runs at much slower speeds compared to LANs.

A WAN is the opposite of a LAN in many ways. Our company, CMP Ltd, continues to grow and opens a manufacturing plant in Jinja, Uganda. Both the Kampala and Jinja locations have deployed LANs, and we need to connect these two separated networks so that data can be shared between all networking devices

companywide. At this point, we meet the first characteristic: The equipment is geographically dispersed.

We have a few choices available to us to connect our two networks—we could run our own wires from Kampala to Jinja. Without going into financial detail and the technology required, running our own wires would be a very expensive and time-consuming proposition. Instead, we investigate the option of borrowing or leasing equipment and wires that are already in place. This would meet the second characteristic of a WAN: connection services, and possibly equipment, are leased. Telecommunications companies that have equipment and wires in place to provide telephone service generally provide the option of leased lines. CMP Ltd can pay a fee and lease time on the wires for data communications.

These links are typically much slower than LAN networking (128 kilobits per second [Kbps], up to 1.544 Mbps are typical). This too can be a trap, so don't just consider the speed of a link to qualify a network as a WAN. Some WAN infrastructures run over links that provide speeds in excess of 1.55 Mbps. This is certainly not a slow link, but because we don't own the equipment, the connection between the two offices is considered a WAN connection. If CMP Ltd continues to grow into a multinational firm with hundreds of offices worldwide, we could inter-connect them all using the same basic techniques and technology. The best known WAN in the world is the Internet.

4.4 Metropolitan Area Networks (MANs)

A metropolitan area network (MAN) combines characteristics of both LANs and WANs. A MAN is limited by geography to a single metropolitan area. Because of the growth of cities, a metropolitan area may now cross over multiple areas, so that alone is not enough to define a MAN. Let's return to our CMP Ltd Company. CMP Ltd is now a multinational firm with locations worldwide, and all of the company's LANs are connected with a large WAN.

We have expanded in Kampala to encompass buildings in the downtown area, but these buildings are too far apart to be connected with only LAN equipment. At this point we can use WAN technologies to interconnect our buildings, creating a MAN architecture for all of the LANs in the Kampala area. Multiple companies in the city may get together to connect their respective LANs together for

redundancy and higher-speed access to the Internet or other common WANs. This configuration would also be considered a MAN. Several colleges and universities also use MANs to interconnect all of their buildings and classrooms. Another possible description for a university or college is a campus area network (CAN), although the distinction is purely one of distance and not well standardized. Table 3.1 offers a brief review of each technology and shows us the key differences between each.

Table 4-1: Network Definitions

Network	Characteristics	Boundary
LAN	High-speed connectivity between all clients. Company owns all equipment.	Usually limited to a single building, unless the buildings are very close together.
WAN	Lower connectivity speeds than a LAN segment. Company leases lines and possibly equipment from a Telecomm provider.	Connections extend beyond city boundaries.
MAN	A mixture of both LAN and WAN connectivity. Used to connect numerous LANs within a metropolitan area.	Connections are confined to a single

4.5 Local Area Network Technologies

With a clear understanding of the concepts of LANs, WANs and MANs, we can now go into more detail about each of the technologies. LANs can use different types of hardware and software to connect equipment. As we discussed before, the OSI reference model was developed to provide a standard method of communication between different vendor's equipment. The OSI protocol, as developed, was too complex for wide acceptance.

Over the years, it has been used as a guideline or model for building a communications process between network devices. Because the OSI model tells us what to do but does not tell us how to do it, numerous methods have been developed that allow us to establish communications between network devices. These methods are called protocols.

As previously discussed, a protocol is most easily thought of as a set of rules for doing something. Many kinds of protocols exist—diplomatic protocols, classroom protocols, and protocols for driving a car. Each protocol defines a set of behaviors that are both acceptable and unacceptable.

The most common protocols used (in OSI Data Link layer communications) on a LAN are:

- Ethernet
- Token Ring
- Fibre Channel

Each of these protocols has different rules and standards. Some even support a wide variety of speeds for communications. They all have similarities and differences, but all define a strict set of rules for networked devices to send and receive data communications. Ethernet is arguably the most popular of the three, so we'll look at that protocol first.

4.5.1 Ethernet

Digital, Intel, and Xerox (the DIX consortium) are credited with developing the first version of the Ethernet protocol at the Palo Alto Research Center (PARC) in California. The term is now loosely applied to many different forms and speeds of that original standard. To make it easier to understand this data-link technology, we will first examine the features common to all of the different versions of Ethernet, and then we will look at the different versions and speeds along with their unique characteristics.

Ethernet is a family of frame-based computer networking technologies for local area networks (LAN). The name was inspired by the physical concept of the ether - A medium that was once supposed to fill all space and to support the propagation of electromagnetic waves. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.

Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN

technology. It has been used from around 1980 to the present, largely replacing competing LAN standards such as token ring, FDDI, and ARCNET.

The architecture of Ethernet defines how network clients gain access to the, medium, or network wire, at the beginning of the communications process. The procedure used to gain media access is referred to as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). It sets up the basic rules for:

- Sending data
- Receiving data
- Error identification

Carrier sense requires that a network device wishing to communicate must first listen for a carrier signal. The presence of a carrier signal means that another device on the network is already communicating. The process of listening first ensures that one station does not attempt communications before another station is done. Ethernet defines the listening time as 9.6 microseconds. If the wire is free from signals for 9.6 ms, then a network station wishing to communicate can begin the next step in the process. Why 9.6 ms? This time is referred to as the Inter-Frame Gap (IFG).

In the original specifications of Ethernet, network devices shared the network wire (not so in today's switched networks). When one station was done transmitting, it took a small amount of time for the network interface card (NIC) to transition from transmit mode to receive mode. To allow for the transition time, all stations must wait a minimum of 9.6 ms from the last received signal before attempting to send data on the wire.

If network devices were not forced to wait, a station that had just finished transmitting might miss the start of a new data stream because it would still be transitioning between transmit and receive. On the networks of today, systems often run on full-duplex switched Ethernet. In this configuration, the network interface can send and receive data at the same time, so no inter-frame gap is necessary.

Multiple Access can have two meanings. For one, it refers to the fact that any station can attempt wire access at any time—it's basically a free-for-all. The other meaning derives from the fact that even if a client machine has just finished

sending data; it can attempt to access the wire again as long as it waits the correct amount of time.

Collision detection is used by the network interface to determine whether two stations have attempted to communicate at the same time. Note that this behavior is not only probable, but also expected, as part of the original design. Given at least two network devices on a common network wire, the stations are likely to listen and find the wire free of traffic. Both will then attempt to communicate, and the resulting signals will interfere with each other to cause a collision. This probability increases as the number of network devices increases. All devices with the potential to send signals that will collide are said to be in the same ***collision domain***.

4.5.2 Token Ring

A Token Ring network is a LAN in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Figure 4-1 shows how it works:

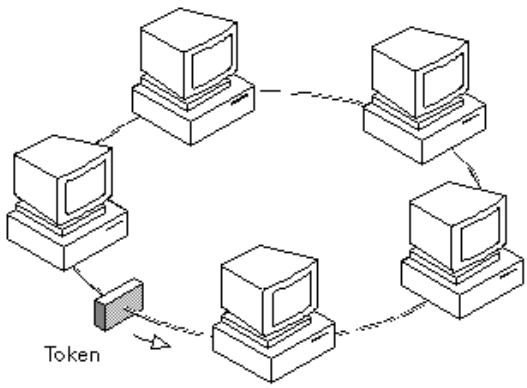

Figure 4-1: Token Ring

1. Empty information frames are continuously circulated on the ring.
2. When a computer has a message to send, it inserts a token in an empty frame (this may consist of simply changing a 0 to a 1 in the token bit part of the frame) and inserts a message and a destination identifier in the frame.
3. The frame is then examined by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and changes the token back to 0.
4. When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.
5. The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

The token scheme can also be used with bus topology LANs.

4.5.3 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) is another token-passing environment that relies on a dual-ring configuration for fault tolerance. In addition to its ability to recover from a primary ring failure, FDDI also functions at 100 Mbps. Although this might not sound impressive today, it was remarkably faster and more reliable than any other technology available when it was released in the mid-1980s.

FDDI is frequently used as high-speed Backbone technology because of its support for high Bandwidth and greater distances than copper. It should be noted that relatively recently, a related Copper specification, called Copper Distributed Data Interface (CDDI), has emerged to provide 100-Mbps service over copper. CDDI is the implementation of FDDI protocols over twisted-pair copper wire. FDDI uses dual-ring architecture shown in Figure 4-2 with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle.

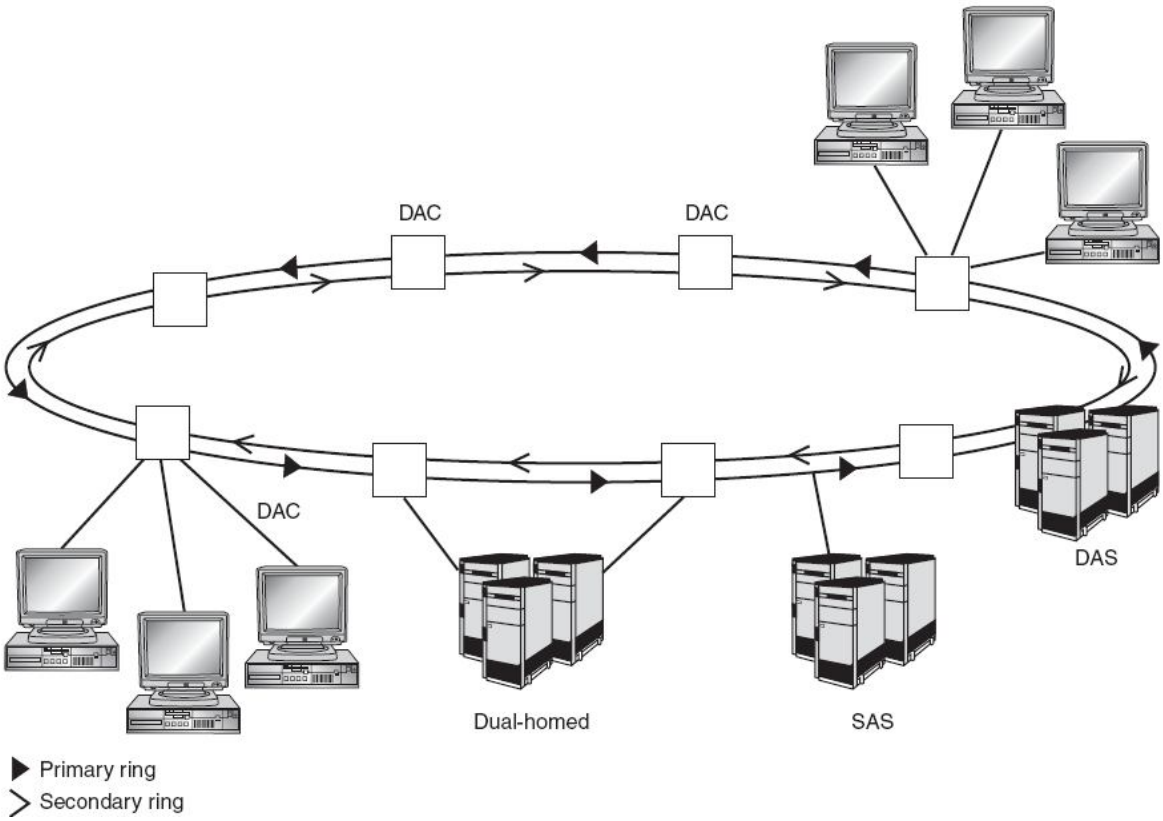

Figure 4-2: Dual-ring topology

Dual-attached station (DAS): This system is attached to both the primary and secondary ring and is capable of wrapping the ring in case of a primary ring failure (explained later).

Dual-attached concentrator (DAC): This system is attached to both the primary and secondary ring and is capable of wrapping the ring in case of a primary ring failure. Additionally, it has one or more ports that allow workstations and other devices access to both rings.

Single attached station (SAS): This system is attached to the primary ring only. In the event of a local primary ring failure, this device will be off the network.

Dual-homed: This system is attached to two individual DACs using two separate interface cards. One card is transmitting, and one card is on standby in case of failure.

4.6 Wide Area Network Technologies

Although LANs serve most communications and resource needs, WANs give companies the ability to leverage information technology across wide geographic areas. WAN connections include Integrated Services Digital Network (ISDN), Frame Relay, Switched Multimegabit Data Service (SMDS), Synchronous Optical Network (SONET), High-level Data Link Control (HDLC), and Logical Link Control (LLC).

4.6.1 Circuit Switching

This involves creating a circuit between two points when needed. The communications path is created only when data is present, and the circuit is torn down when the data delivery is complete. Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection as shown in Figure 4-3. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved.

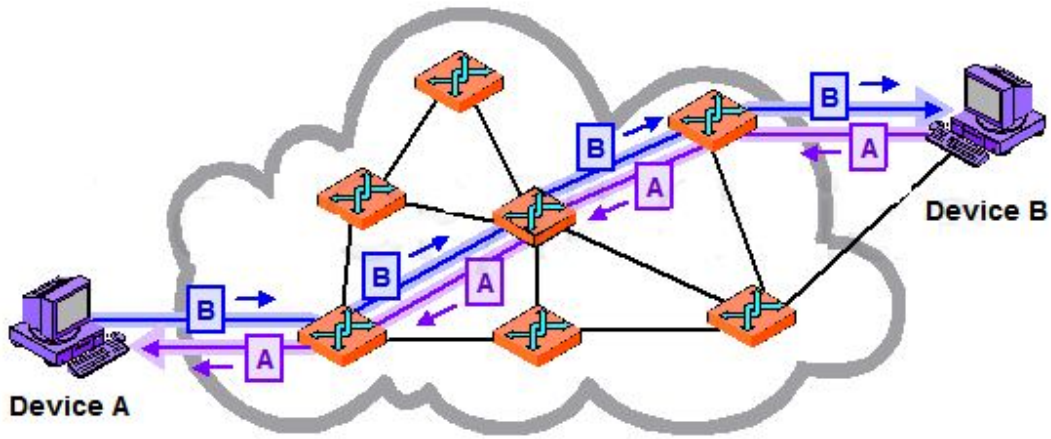

Figure 4-3: Circuit Switched Network

4.6.2 Packet Switching

Packet-switched describes the type of network in which relatively small units of data called packets are routed through a network based on the destination address

contained within each packet as shown in Figure 4-4. Breaking communication down into packets allows the same data path to be shared among many users in the network. This type of communication between sender and receiver is known as connectionless (rather than dedicated). Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.

This allows multiple companies to share the cost of WANs by sharing the network transmission path. Packet switching uses virtual circuits for data delivery. Permanent virtual circuits (PVCs) are predefined paths for data flow between two end points. The virtual circuit is up even when no data is present. Switched virtual circuits (SVCs) function the same as circuit switching. The path is built when data needs to be transferred and torn down when data transfer is complete.

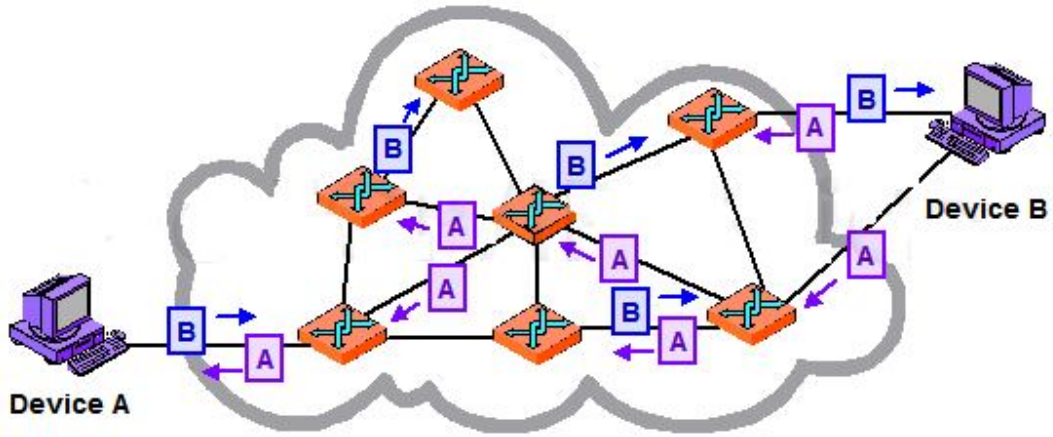

Figure 4-4: Packet Switched Network