2.1 Data Network

Data networks developed as a result of business applications that were written for microcomputers. The microcomputers were not connected so there was no efficient way to share data among them. It was not efficient or cost-effective for businesses to use floppy disks to share data. Sneakernet created multiple copies of the data. Each time a file was modified it would have to be shared again with all other people who needed that file. If two people modified the file and then tried to share it, one of the sets of changes would be lost. Businesses needed a solution that would successfully address the following three problems:

- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network.

Businesses realized that computer networking could increase productivity and save money. Networks were added and expanded almost as rapidly as new network technologies and products were introduced. The early development of networking was disorganized. However, a tremendous expansion occurred in the early 1980s. In the mid-1980s, the network technologies that emerged were created with a variety of hardware and software implementations. Each company that created network hardware and software used its own company standards. These individual standards were developed because of competition with other companies. As a result, many of the network technologies were incompatible with each other. It became increasingly difficult for networks that used different specifications to communicate with each other. Network equipment often had to be replaced to implement new technologies.

Table. (1) summarizes the relative sizes of LANs and WANs.

Distance Between CPUs	Location of CPUs	Name
0.1m	Printed circuit board Personal data asst.	Motherboard Personal area network (PAN)
1.0m	Millimeter Mainframe	Computer system network
10m	Room	Local area network (LAN) Your classroom
100m	Building	Local area network (LAN) Your school
1000m=1km	Campus	Local area network (LAN) Stanford University
100,000m=100km	Country	Wide area network (WAN) Cisco Systems, Inc.

1,000,000m=1,000km	Continent	Wide area network (WAN) Africa
10,000,000m=10,000km	Planet	Wide area network (WAN) The Internet
100,000,000m=100,000km	Earth-moon system	Wide area network (WAN) Earth and artificial satellites

2.2 Network Devices

Equipment that connects directly to a network segment is referred to as a device. These devices are broken up into two classifications. The first classification is **End-user devices**. End-user devices include **computers**, **printers**, **scanners**, and other devices that provide services directly to the user. The second classification is **Network devices**. Network devices include all the devices that connect the end-user devices together to allow them to communicate. End-user devices that provide users with a connection to the network are also referred to as Hosts. These devices allow users to share, create, and obtain information. The host devices can exist without a network, but without the network the host capabilities are greatly reduced Figure. (1).

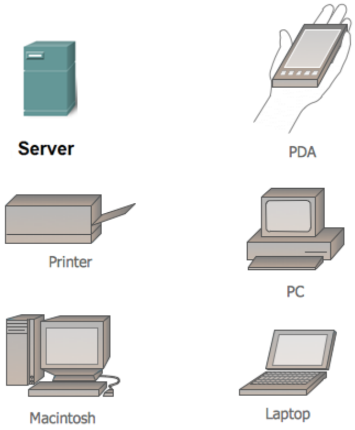


Figure 1 End user Devise

Network Interface Card (NIC) are used to physically connect host devices to the network media. They use this connection to send e-mails, print reports, scan pictures, or access databases Figure. (2). A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard. It can also be a peripheral device. NICs are sometimes called network adapters. Each NIC is identified by a unique code called a Media Access Control (MAC) address. This address is used to control data communication for the host on the network. More about the MAC address will be covered later. As the name implies, the NIC controls host access to the network.

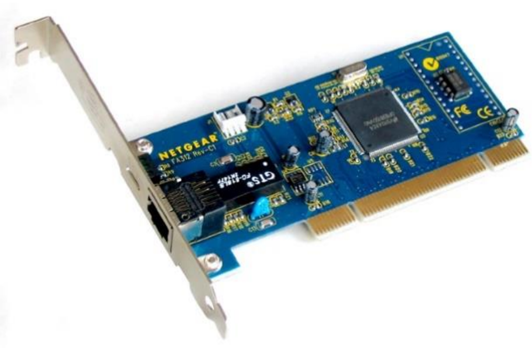


Figure 2 Network Interface Card (NIC)

Network devices are used to extend cable connections, concentrate connections, convert data formats, and manage data transfers. Examples of devices that perform these functions are repeaters, hubs, bridges, switches, routers, and Network cloud Figure (3). All of the network devices mentioned here are covered in depth later in the course. For now, a brief overview of networking devices will be provided.

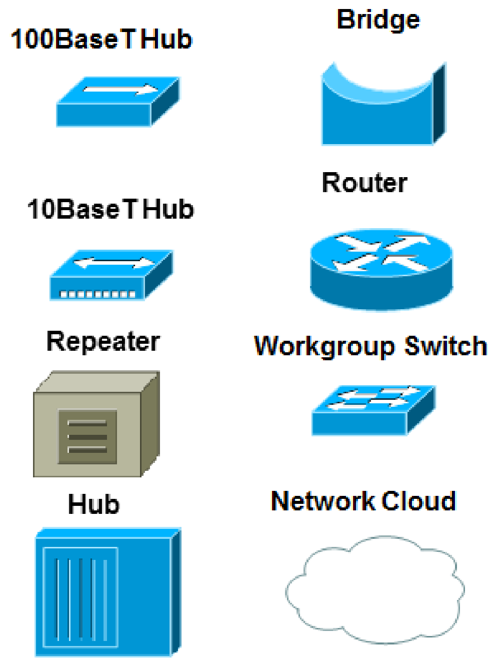


Figure 3 Network devices

A repeater is a network device used to regenerate a signal. Repeaters regenerate analog or digital signals that are distorted by transmission loss due to attenuation. A repeater does not make intelligent decision concerning forwarding packets like a router or bridge Figure (4).

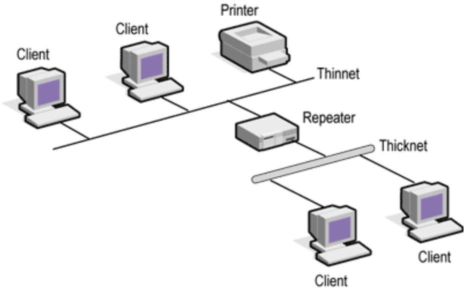


Figure 4 Repeater

Hubs concentrate connections. In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission. Active hubs concentrate hosts and also regenerate signals.

Bridges convert network data formats and perform basic data transmission management. Bridges provide connections between LANs. They also check data to determine if it should cross the bridge. This makes each part of the network more efficient Figure (5).

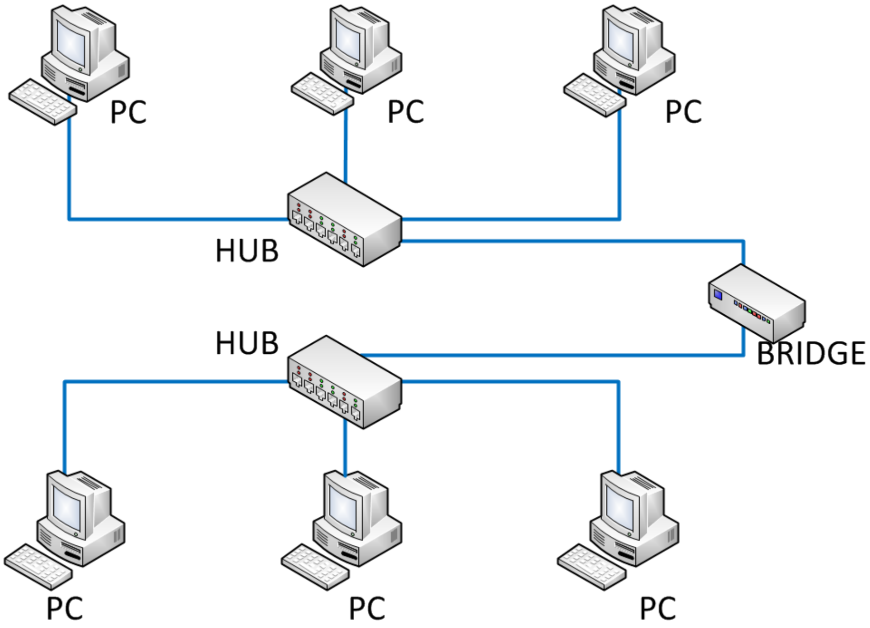


Figure 5 Hub and Bridge

Workgroup switches add more intelligence to data transfer management. They can determine if data should remain on a LAN and transfer data only to the connection that needs it. Another difference between a bridge and switch is that a switch does not convert data transmission formats Figure (6).

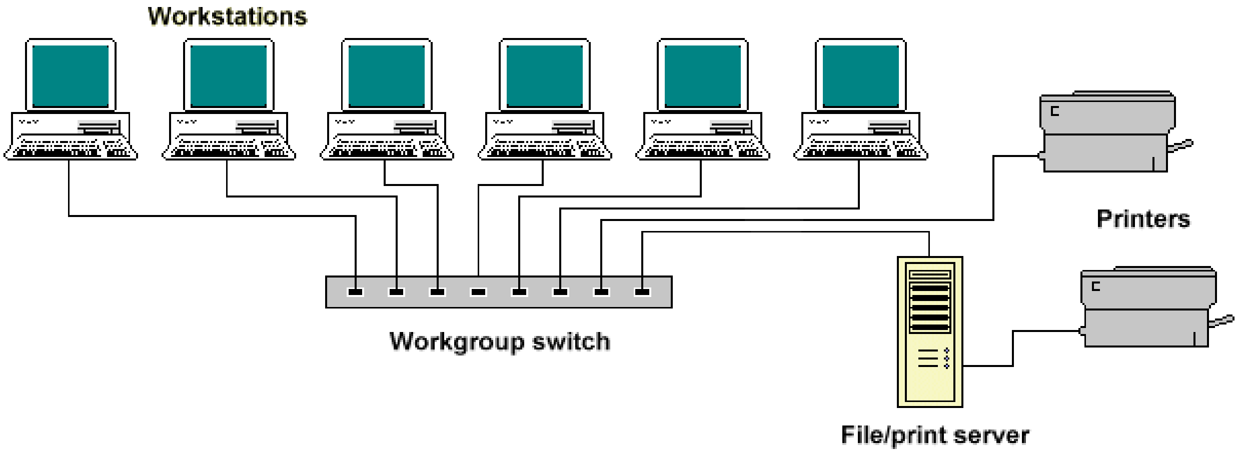


Figure 6 Workgroup switches

Routers have all the capabilities listed above. Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers. They can also connect to a WAN, which allows them to connect LANs that are separated by great distances. None of the other devices can provide this type of connection Figure (7).

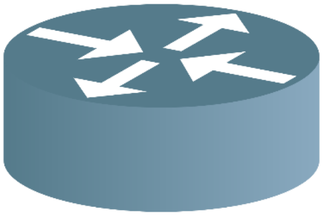


Figure 7 Router

2.3 Network Topology

Network topology defines the structure of the network. One part of the topology definition is the physical topology, which is the actual layout of the wire or media. The other part is the logical topology, which defines how the hosts access the media to send data. The physical topologies that are commonly used are as follows Figure (8):

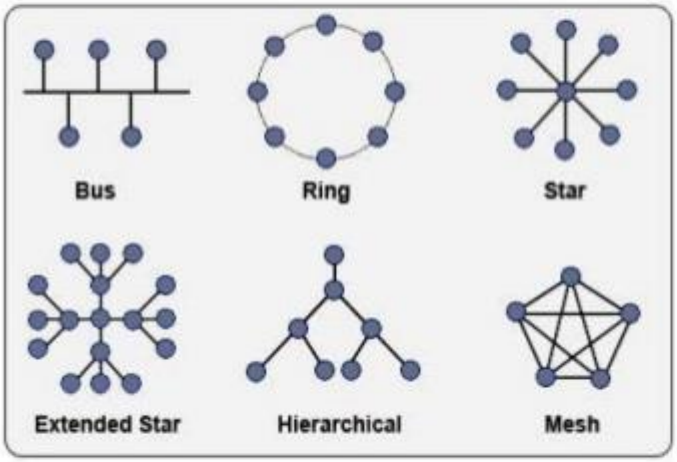


Figure 8 Physical topology

2.3.1 Bus topology uses a single backbone cable that is terminated at both ends. All the hosts connect directly to this backbone.

Advantages:

1. There is no central controller.

2. Control resides in each station
3. Less interconnecting wire is required.
4. Ease of installation.
5. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths.

Disadvantages:

1. It is possible that more than one station may attempt transmission simultaneously (collision or contention).
2. Difficult reconfiguration and fault isolation.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
4. The damaged area reflects signals back in the direction of origin, creating noise in both directions

2.3.2 Ring topology connects one host to the next and the last host to the first. This creates a physical ring of cable.

Advantages:

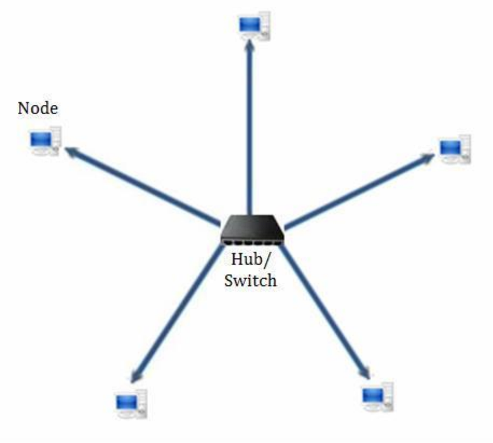
1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Each device incorporates a repeater.
5. Relatively easy to install and reconfigure.
6. Fault isolation is simplified.

Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.
2. Unidirectional traffic.

2.3.3 A star topology connects all cables to a central point.

Advantages:



1. Easy to install and reconfigure.
2. Robustness, if one link fails; only that link is affected. All other links remain active.
3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

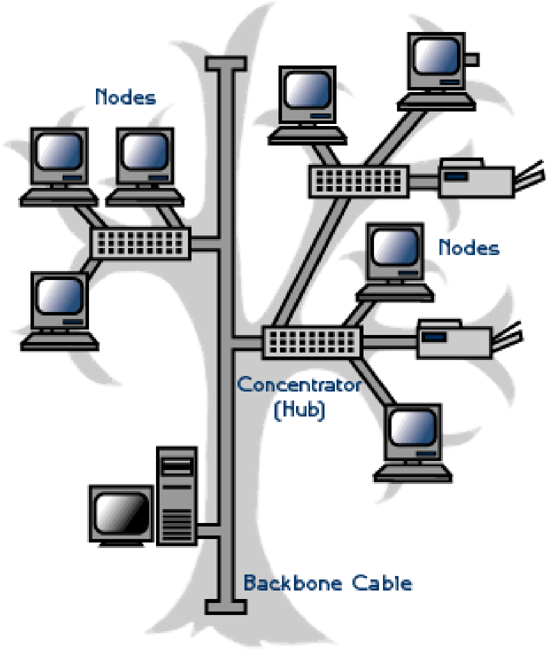
Disadvantages:

1. The devices are not linked to each other.

2. If one device wants to send data to another, it sends to the controller, which then relays the data to the other connected device.

2.3.4 An extended star topology links individual stars together by connecting the hubs or switches.

2.3.5 A hierarchical (tree) topology is similar to an extended star. However, instead of linking the hubs or switches together, the system is linked to a computer that controls the traffic on the topology.



Advantages:

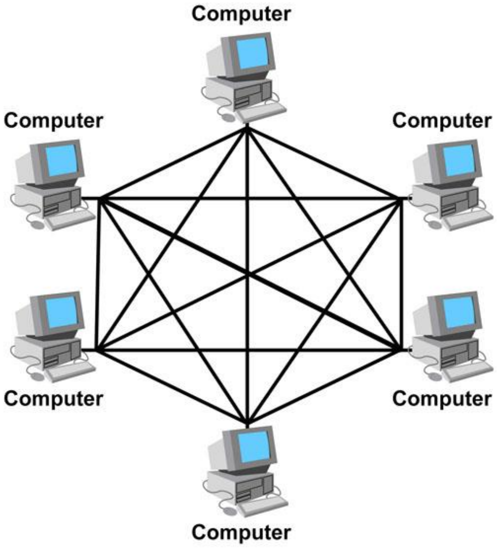
1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and priorities communications from different computers.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.

2.3.6 Mesh topology is implemented to provide as much protection as possible from interruption of service. For example, a nuclear power plant might use a mesh topology in the networked control systems. As seen in the graphic, each host has its own connections to all other hosts. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.

Advantages:



1. The use of dedicated (link carries traffic only between the two device it connects) links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. It is robust, if one link becomes unusable, it does not incapacitate (affect) the entire system.
3. Privacy and Security (every message sent travels along a dedicated line; only the intended recipient sees it).
4. Point-to-point links makes fault identification and fault isolation easy.

Disadvantages:

1. Large amount of cabling required.
2. Large amount of I/O ports required.
3. Installation and reconfiguration are difficult.
4. The sheer bulk of the wiring can be greater than the available space (in the walls, ceiling, or floors) can accommodate.
5. The hardware required to connect each link (I/O ports and cables) can be prohibitively expensive.

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast** and **token passing**.

The use of a **Broadcast topology** indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

The second logical topology is **Token passing**. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI). The diagram in Figure (9) shows many different topologies connected by network devices (**Hybrid topologies**). It shows a network of moderate complexity that is typical of a school or a small business. The diagram includes many symbols and networking concepts that will take time to learn.

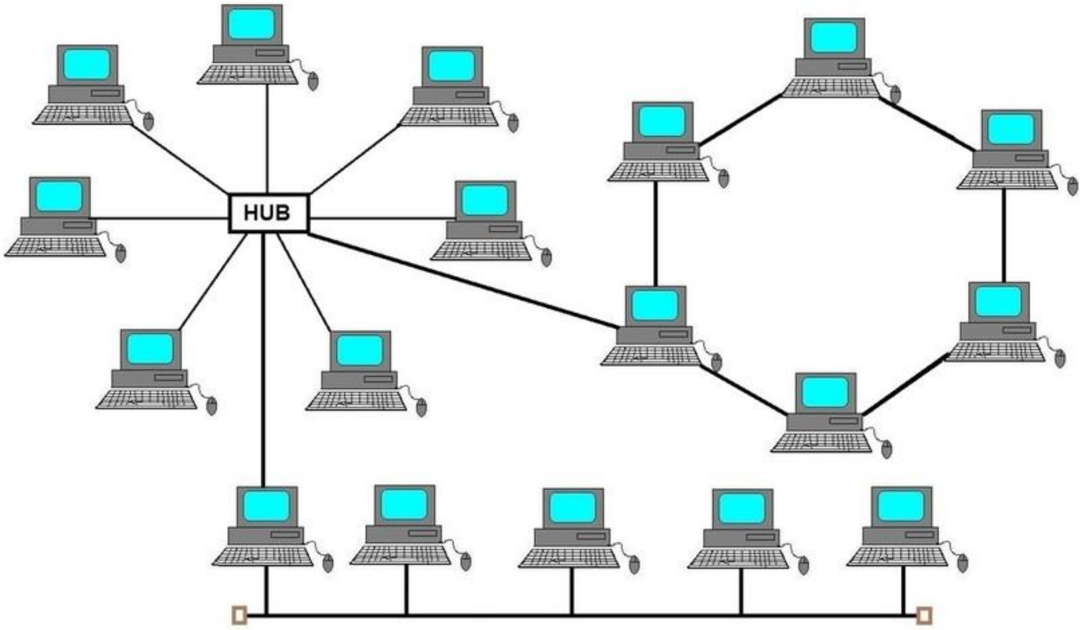


Figure 9 Different Topologies Connected by Network Devices

2.4 Local Area Network (LAN)

A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or campus. A LAN tends to use only one type of transmission medium—cabling. LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. A good example of this technology is email. LANs manage data, local communications, and computing equipment. LANs are characterized by the following:

- They transfer data at high speeds.
- They exist in a limited geographical area.

- Their technology is generally less expensive.

LANs consist of the following components:

- Computers
- Network interface cards
- Peripheral devices
- Networking media
- Network devices

Some common LAN technologies include the following:

- Ethernet
- Token Ring
- FDDI

2.5 Wide Area Network (WAN)

A wide area network (WAN) interconnects LANs. A WAN may be located entirely within a state or country, or it may be interconnected around the world, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They are more sophisticated and complex than LANs.
- Provide e-mail, Internet, file transfer, and e-commerce services.
- Their technology is expensive.

Some common WAN technologies include the following:

- Modems.
- Integrated Services Digital Network (ISDN).
- Digital subscriber line (DSL).
- Frame Relay.
- T1, E1, T3, and E3

- Synchronous Optical Network (SONET).

2.6 Metropolitan-area networks (MAN)

Metropolitan-area networks (MAN) usually consists of two or more LANs in a common geographic area. For example, a bank with multiple branches may utilize a MAN. Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas Figure (10).

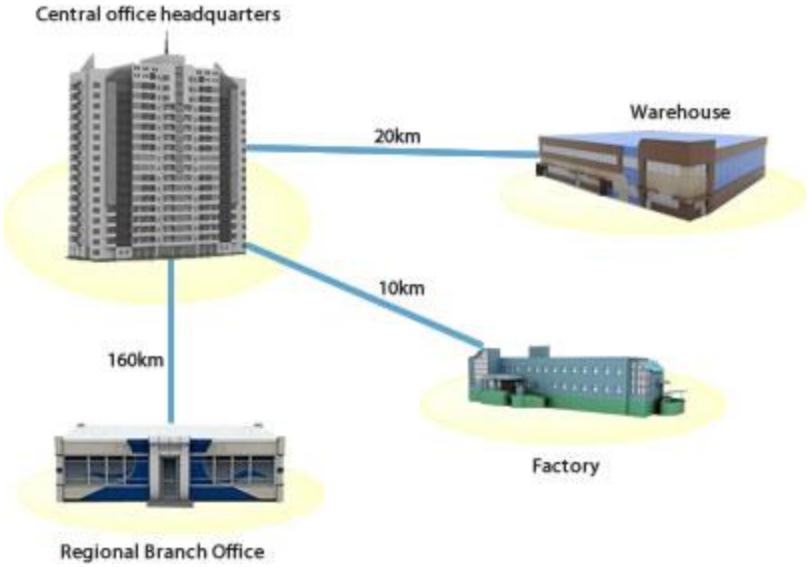


Figure 10 Metropolitan-area networks (MAN)

2.7 Storage-area networks (SAN)

A storage-area network (SAN) is a dedicated, high-performance network used to move data between servers and storage resources. Because it is a separate, dedicated network, it avoids any traffic conflict between clients and servers. SAN technology allows high-speed server-to-storage, storage-to-storage, or server-to-server connectivity. This method uses a separate network infrastructure that relieves any problems associated with existing network connectivity Figure (11). SANs offer the following features:

- **Performance**: SANs allow concurrent access of disk or tape arrays by two or more servers at high speeds. This provides enhanced system performance.

- **Availability**: SANs Data can be duplicated on a SAN up to 10 km (6.2 miles) away. **Scalability**: A SAN can use a variety of technologies.

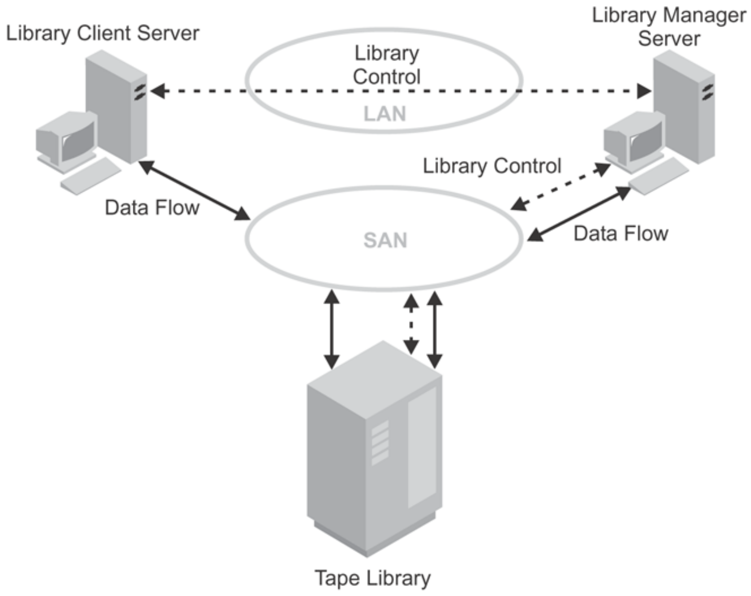


Figure 11 Storage-area networks (SAN)

2.8 Virtual Private Network (VPN)

A virtual private network (VPN) is a private network that is constructed within a public network infrastructure such as the global Internet. Using VPN, a telecommuter can remotely access the network of the company headquarters. Through the Internet, a secure tunnel can be built between the PC of the telecommuter and a VPN router at the company headquarters Figure (12).

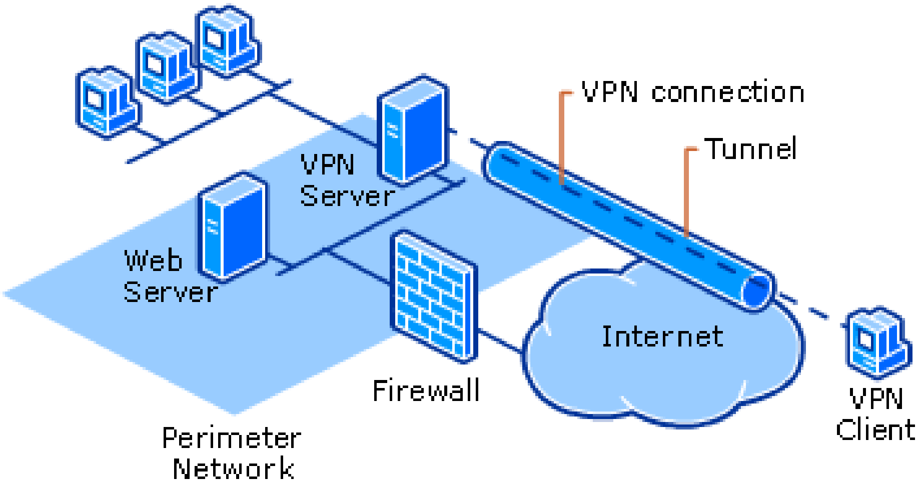


Figure 12 Virtual Private Network (VPN)

2.9 Intranets and Extranets

One common configuration of a LAN is an intranet. Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data. Extranets refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application-level security. An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

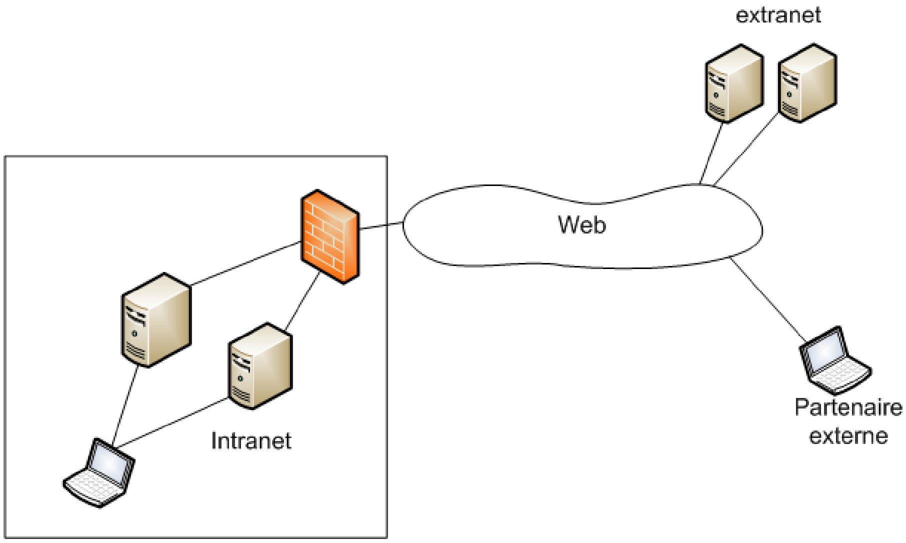


Figure 13 Intranets and Extranet

2.10 Network Interconnection

When LAN and WAN technologies are used, many computers are interconnected to provide services to their users. To accomplish this, networked computers take on different roles or functions in relation to each other. Some types of applications require computers to function as equal partners. Other types of applications distribute their work so that one computer functions to serve a number of others in an unequal relationship. Two computers generally use request and response protocols to communicate with each other. One computer issues a request for a service, and a second computer receives and responds to that request. The requestor acts like a client and the responder acts like a server.

2.10.1 Peer-to-Peer Network

In a peer-to-peer network, networked computers act as equal partners, or peers. As peers, each computer can take on the client function or the server function. Computer A may request for a file from Computer B, which then sends the file to Computer A. Computer A acts like the client and Computer B acts like the server. At a later time, Computers A and B can reverse roles. In a peer-to-peer network, individual users control their own resources. The users may decide to share certain files with other users. Peer-to-peer networks are relatively easy to install and operate. No additional equipment is necessary beyond a suitable operating system installed on each computer. Since users control their own resources, no dedicated administrators are needed. As networks grow, peer-to-peer relationships become increasingly difficult to coordinate. A peer-to peer network works well with ten or fewer computers. Since peer-to-peer networks do not scale well, their efficiency decreases rapidly as the number of computers on the network increases. Also, individual users control access to the resources on their computers, which means security may be difficult to maintain. The client/server model of networking can be used to overcome the limitations of the peer-to-peer network.

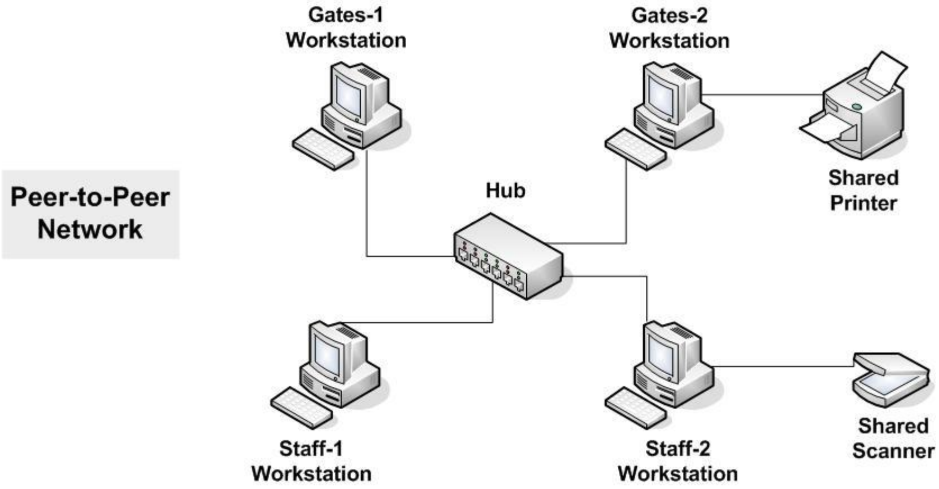


Figure 14 Peer-to-Peer Network

2.10.2 Client/Server

In a client/server arrangement, network services are located on a dedicated computer called a server. The server responds to the requests of clients. The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services. Most network operating systems adopt the form of a client/server relationship. Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers. Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Each client is assigned an account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server-based networks simplify the administration of large networks. The concentration of network resources such as files, printers, and applications on servers also makes it easier to back-up and maintain the data. Resources can be located on specialized, dedicated servers for easier access. Most client/server systems also include ways to enhance the network with new services that extend the usefulness of the network. The centralized functions in a client/server network has substantial advantages and some disadvantages. Though a centralized server enhances security, ease of access, and control, it introduces a single point of failure into the network. Without an operational server, the network cannot function at all. Servers require a trained, expert staff member to administer and maintain. Server systems also require additional hardware and specialized software that add to the cost.

Advantages of a Peer-to-Peer Network	Advantages of a Client/Server Network
Less expensive to implement.	Provides for better security.
Does not require additional specialized network administration software.	Easier to administer when the network is large because administration is centralized.
Does not require a dedicated network administrator.	All data can be backed up on one central location.

Disadvantages of a Peer-to-Peer Network	Disadvantages of a Client/Server Network
Does not scale well to large networks and administration becomes unmanageable.	Requires expensive specialized network administrative and operational software.

Each user must be trained to perform administrative tasks.	Requires expensive, more powerful hardware for the server machine.
Less secure.	Requires a professional administrator.
All machines sharing the resources negatively impact the performance.	Has a single point failure. User data is unavailable if the server is down.

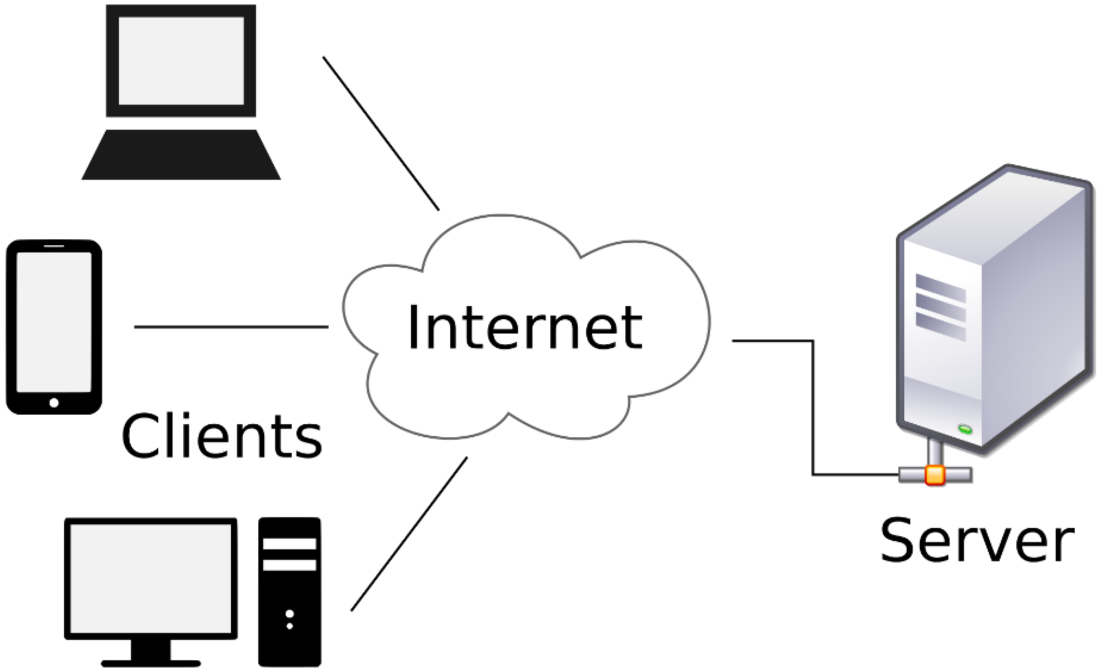


Figure 15 Client/Server Network