

CSC 427 (COMPUTER NETWORK) LECTURE NOTES

COMPILED BY

ABIKOYE, OLUWAKEMI CHRISTIANA (Ph.D)

DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF COMMUNICATION AND INFORMATION SCIENCES
UNIVERSITY OF ILORIN

2015/2016 SESSION

1. DATA COMMUNICATION AND NETWORKS

1.1 Definition of Data Communication

Definition 1: Data Communication is the exchange of data (in the form of Os and 1s) between two devices via some form of transmission medium (such as a wire cable).

Definition 2: **Data communication** refers to the exchange of data between a source and a receiver. Data Communication can be local or remote. It is considered local if communicating devices are in the same building or a similarly restricted geographical area while it is remote if devices are farther apart.

The meanings of source and receiver are very simple. The device that transmits the data is known as **source** and the device that receives the transmitted data is known as **receiver**. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.

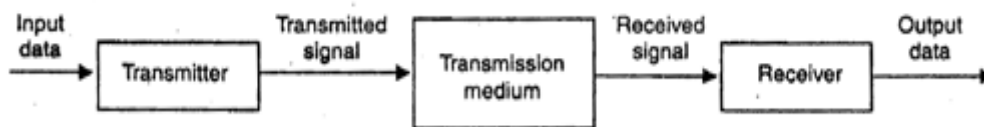


Figure 1.1: Data Communication System

A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure 1.2 provides a broader view of data communication networks. The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features.

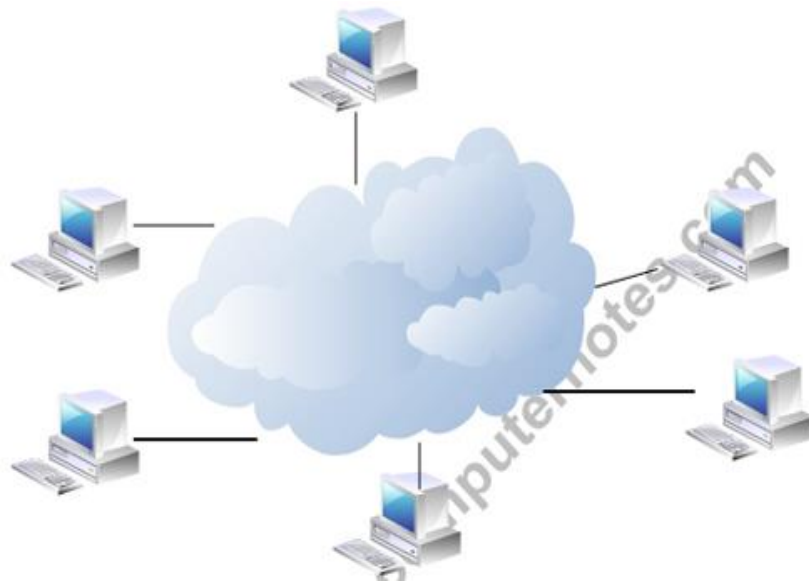


Figure 1.2: Data Communication System using Remote Locations

1.1.1 Components of data communication system

A Communication system has following components:

1. **Message:** It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.
2. **Sender:** It is the device/computer that generates and sends that message.
3. **Receiver:** It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.
4. **Medium:** It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.
5. **Protocol:** It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

A **protocol** performs the following functions:

1. **Data sequencing.** It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.
2. **Data routing.** Data routing defines the most efficient path between the source and destination.
3. **Data formatting.** Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control.** A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.
5. **Error control.** These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.
6. **Precedence and order of transmission.** These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.
7. **Connection establishment and termination.** These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.
8. **Data security.** Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.
9. **Log information.** Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

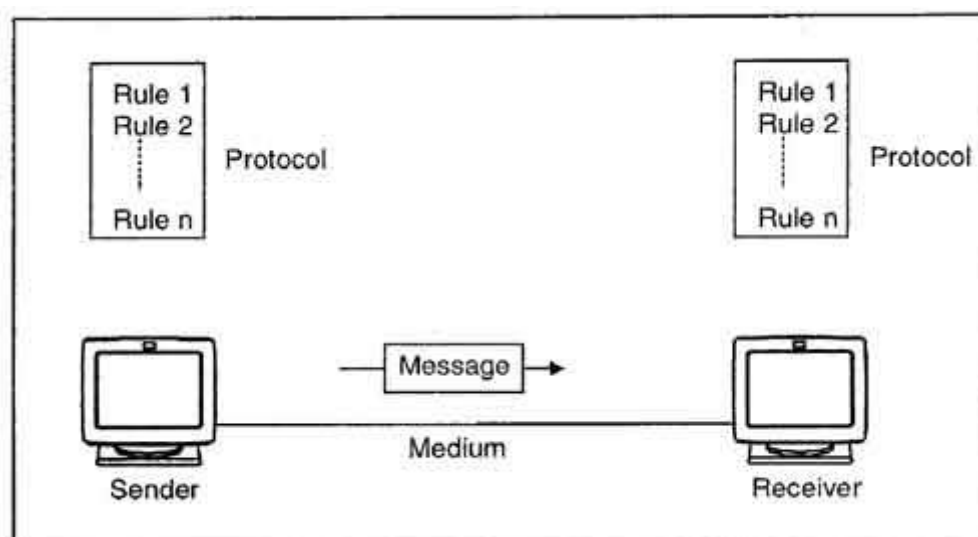


Figure 1.3: Communication process between two devices

1.2 Definition of Computer Network

Definition 1: A computer network may be defined as the coordination or interconnection of a number of individual computers. A computer network is basically established by the network layer in the Open Systems Infrastructure model, popularly known as the OSI model.

Definition 2: A computer network, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources.

Definition 3: A network can as well be define as a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

All networks must have the following:

1. A resource to share (resource)
2. A pathway to transfer data (transmission medium)
3. A set of rules governing how to communicate (protocols)

1.3 Types of Network

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage area network, or SAN
- Enterprise private network, or EPN
- Virtual private network, or VPN

1.3.1 Personal Area Network

A **personal area network**, or **PAN**, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.
- Upload the photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.

1.3.2 Local Area Network

A **Local Area Network**, or **LAN**, consists of a computer network at a single site, typically an individual office building. **Local area networks (LANs)** are used to connect networking devices that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.

The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.

LANs are typically used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same

office, but you would not want somebody just walking outside to be able to send a document to the printer from their cell phone! If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN. **Wireless Local Area Network** - a LAN based on Wi-Fi wireless network technology

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- In a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- In a "client/server" environment, in which a central computer provides network services to users.

1.3.3 Metropolitan Area Network

A **Metropolitan Area Network**, or **MAN**, consists of a computer network across an entire city, college campus or small region. A **metropolitan area network (MAN)** is a hybrid between a LAN and a WAN.

A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

1.3.4 Wide Area Network

A **Wide Area Network**, or **WAN**, occupies a very large area, such as an entire country or the entire world. **Wide Area Networks (WANs)** are used to connect LANs together. Typically, WANs are used when the LANs that must be connected are separated by a large distance.

A WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is the best-known example of a public WAN.

1.3.5 Other Types of Network

Enterprise Private Network: One approach to a private network is to build an **Enterprise Private Network**, or **EPN**. An EPN is a computer network that is entirely controlled by one organization, and it is used to connect multiple locations. Historically, telecommunications companies, like AT&T, operated their own network, separate from the public Internet. EPNs are still fairly common in certain sectors where security is of the highest concern. For example,

a number of health facilities may establish their own network between multiple sites to have full control over the confidentiality of patient records.

Virtual Private Network: With the growth of the Internet, private networks have gone virtual. A **Virtual Private Network (VPN)** is a special type of secured network. A VPN is used to provide a secure connection across a public network, such as an internet. Extranets typically use a VPN to provide a secure connection between a company and its known external users or offices. A VPN is a network in which some parts of the network use the Internet, but data is encrypted before it is sent over the Internet to indicate that it is a private network. It provides a high level of security for traffic over the Internet.

Authentication is provided to validate the identities of the two peers.

Confidentiality provides encryption of the data to keep it private from prying eyes.

Integrity is used to ensure that the data sent between the two devices or sites has not been tampered with.

A **Storage Area Network**, or **SAN**, is a network dedicated to data storage. A large organization may have different types of centralized storage, not all of which should be accessible to all users of the local area network within the organization. A dedicated SAN gives network and database administrators more control over data storage. Regular LAN users only get access to the elements of this storage system that are relevant to them. SANs provide a high-speed infrastructure to move data between storage devices and file servers .

Advantage

- Performance is fast.
- Availability is high because of the redundancy features available.
- Distances can span up to 10 kilometers.
- Management is easy because of the centralization of data resources.
- Overhead is low (uses a thin protocol).

Disadvantage of SANs is their cost.

A **Home Area Network**, or **HAN**, is a type of PAN specifically designed for home use. A home network may include things like digital televisions, home security and other types of systems that are unique to the home environment and not typically found in an office.

A **Body Area Network**, or **BAN**, is a network of wearable computing devices. This can include things like a watch, special glasses, tracking devices and heart-rate monitors. For example, an Alzheimer's patient could be outfitted with a location tracking device and a cellular

communication device. If they leave a certain area, family members can be alerted with a text or e-mail message to the location of their loved one.

Campus Area Network - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.

System Area Network (also known as Cluster Area Network).- links high-performance computers with high-speed connections in a cluster configuration.

Content networks (CNs) were developed to ease users' access to Internet resources. Companies deploy basically two types of CNs:

- caching downloaded Internet information
- Distributing Internet traffic loads across multiple servers

An **intranet** is basically a network that is local to a company. In other words, users from within this company can find all of their resources without having to go outside of the company. An intranet can include LANs, private WANs and MANs,

An **extranet** is an extended intranet, where certain internal services are made available to known external users or external business partners at remote locations.

An **internet** is used when unknown external users need to access internal resources in your network. In other words, your company might have a web site that sells various products, and you want any external user to be able to access this service.

1.4 Data Transmission Modes

Network devices use three transmission modes (methods) to exchange data, or "talk" to each other, as follows: simplex, half duplex, and full duplex.

- **Simplex transmission** is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission, which means that data can flow only in one direction from the sending device to the receiving device. Figure 1.4 illustrates simplex transmission.
- **Half-duplex transmission** is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time. Figure 1.4 illustrates half-duplex transmission.

- **Full-duplex transmission** is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time. Figure 1.4 illustrates full-duplex transmission.

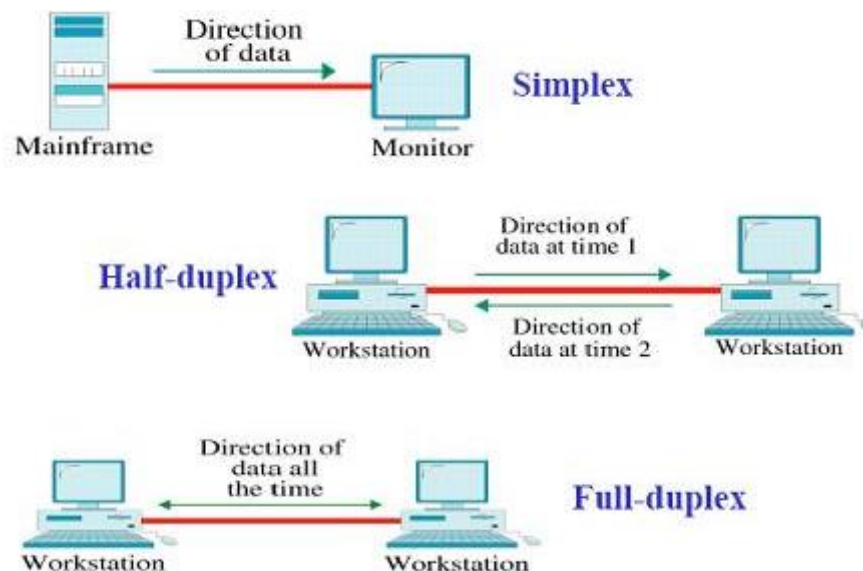


Figure 1.4: Transmission Modes

1.5 Benefits of Networks

Assuming you have six people in your family. Each has their own computer and wants to be able to print and have internet access. You don't want to pay for six modems (for internet connections) and six printers. Why not have one internet connection and one printer connected to one computer. This computer has all other computers attached to it. They all share its internet and printer. They can also each have some shared folders that everyone on the network can access (upon providing a password). Properly planned, an efficient network brings a wide range of benefits to a company such as:

Software, Hardware, File, data and information Sharing: Networks offer a quick and easy way to share files, application programs, hardware, data and information directly. Instead of using a disk or USB key to carry files from one computer or office to another, you can share files directly using a network.

Security: Specific directories can be password protected to limit access to authorized users. Also, files and programs on a network can be designated as "copy inhibit" so you don't have to worry about the illegal copying of programs.

Resource Sharing: All computers in the network can share resources such as printers, fax machines, modems, and scanners. Communication: Even outside of the internet, those on the

network can communicate with each other via electronic mail over the network system. When connected to the internet, network users can communicate with people around the world via the network.

Flexible Access: Networks allow their users to access files from computers throughout the network. This means that a user can begin work on a project on one computer and finish up on another. Multiple users can also collaborate on the same project through the network.

Workgroup Computing: Workgroup software like Microsoft BackOffice enables many users to contribute to a document concurrently. This allows for interactive teamwork.

Error reduction and improve consistency: One can reduce errors and improve consistency by having all staff work from a single source of information, so that standard versions of manuals and directories can be made available, and data can be backed up from a single point on a scheduled basis, ensuring consistency.

Facilitating communications: Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

1.6 Network Topologies

The term topology refers to the way a network is laid out, either physically or logically.

The physical topology of a network refers to the configuration of cables, computers, and other peripherals including device location and cable installation while the logical topology is the method used to pass information between workstations i.e how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other. There are five basic topologies possible: mesh, star, tree, bus, and ring

Two relationships are possible: peer-to-peer, where the devices share the link equally, and primary-secondary, where one device controls traffic and the others must transmit through it. Ring and mesh topologies are more convenient for peer-to-peer transmission, while star and tree are more convenient for primary-secondary, bus topology is equally convenient for either.

Hybrid networks are the complex networks, which can be built of two or more above mentioned topologies. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: star ring network and star bus network.

1.6.1 Bus Topology

In Bus Topology, each node is connected to a single cable, by the help of interface connectors. Bus topology uses a common backbone to connect all the network devices in a network in a linear shape. A single cable functions as the shared communication medium for all the devices attached with this cable with an interface connector. The device, which wants to communicate send the broadcast message to all the devices attached with the shared cable but only the intended recipient actually accepts and process that message.

A linear bus topology consists of a main run of cable with a terminator at each end (See Figure 1.5). All nodes (file server, workstations, and peripherals) are connected to the linear cable. Ethernet and Local Talk networks use a linear bus topology.

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.
- It works well for small networks.
- Easy to Extend

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.
- It is slow when more devices are added into the network.
- If a main cable is damaged then network will fail or be split into two networks
- It is difficult to detect trouble at an individual station.

1.6.2 Ring Topology

A ring topology is a network topology or circuit arrangement in which each network device is attached along the same signal path to two other devices, forming a path in the shape of a ring. Each device in the network that is also referred to as node handles every message that flows through the ring. Each node in the ring has a unique address. Since in ring topology there is only one pathway between any two nodes, ring networks are generally disrupted by the failure

of a single link. A network topology is set up in a circular fashion in such a way that they make a closed loop. This way data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels.

In a ring topology, there is no server computer present; all nodes work as a server and repeat the signal. The disadvantage of this topology is that if one node stops working, the entire network is affected or stops working.

The redundant topologies are used to eliminate network downtime caused by a single point of failure. All networks need redundancy for enhanced reliability. Network reliability is achieved through reliable equipment and network designs that are tolerant to failures and faults. The Fiber Distributed Data Interface (FDDI) networks overcome the disruption in the network by sending data on a clockwise and a counterclockwise ring. In case there is a break in data flow, the data is wrapped back onto the complementary ring before it reaches the end of the cable thereby maintaining a path to every node within the complementary ring. The most well known example of a ring topology is Token Ring.

Advantages

- An orderly network where every device has access to the token and the opportunity to transmit
- Under heavy network load performs better than a star topology.
- To manage the connectivity between the computers it doesn't need network server.
- Due to the point to point line configuration of devices with a device on either side (each device is connected to its immediate neighbor), it is quite easy to install and reconfigure since adding or removing a device requires moving just two connections.
- Point to point line configuration makes it easy to identify and isolate faults.
- Reconfiguration for line faults of bidirectional rings can be very fast, as switching happens at a high level, and thus the traffic does not require individual rerouting

Disadvantages

- One malfunctioning workstation can throw away the entire network.
- Moves, adds and changes of devices can affect the entire network .
- Communication delay is directly proportional to number of nodes in the network
- Bandwidth is shared on all links between devices
- More difficult to configure than a Star: node adjunction = Ring shutdown and reconfiguration

1.6.3 Star Topology

In the computer networking world the most commonly used topology in LAN is the star topology. Star topologies can be implemented in home, offices or even in a building. In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node with the help of the hub. All the computers in the star topologies are connected to central devices like hub, switch or router. The functionality of all these devices is different. As compared to the bus topology, a star network requires more devices & cables to complete a network. The failure of each node or cable in a star network, won't take down the entire network as compared to the Bus topology. However if the central connecting devices such as hub, switch or router fails due to any reason, then ultimately all the network can come down or collapse.

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator (See figure 1.5). Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted-pair cable; however, it can also be used with coaxial cable or fiber-optic cable.

Advantages

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices (reliable).
- Easy to detect faults and to remove parts.

Disadvantages

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

The protocols used with star configurations are usually Ethernet or Local Talk.

1.6.4 Tree Topology

A tree topology is essentially a combination of bus topology and star topology. The nodes of bus topology are replaced with standalone star topology networks. This results in both disadvantages of bus topology and advantages of star topology.

Tree topologies are comprised of the multiple star topologies on a bus. Tree topologies integrate multiple star topologies together onto a bus. Only the hub devices can connect directly with the tree bus and each Hub functions as a root of a tree of the network devices. This bus/star/hybrid combination supports future expandability of the computer networks, much better than a bus or star (See figure 1.5).

Advantages

- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.

Disadvantages

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

1.6.5 Mesh topology

In mesh topology, there is only one possible path from one node to another node. If any cable in that path is broken, the nodes cannot communicate. Mesh topology uses lots of cables to connect every node with every other node. It is very expensive to wire up, but if any cable fails, there are many other ways for two nodes to communicate. Some WANs, like the Internet, employ mesh routing. In fact the Internet was deliberately designed like this to allow sites to communicate even during a nuclear war.

Mesh topology work on the concept of routes. In Mesh topology, message sent to the destination can take any possible shortest, easiest route to reach its destination. In the previous topologies star and bus, messages are usually broadcasted to every computer, especially in bus topology. Similarly in the Ring topology message can travel in only one direction i.e clockwise or anticlockwise. Internet employs the Mesh topology and the message finds its route for its destination. Router works in finding the routes for the messages and in reaching them to their destinations. The topology in which every devices connects to every other device is called a full Mesh topology unlike in the partial mesh in which every device is indirectly connected to the other devices.

1.6.6 Fully Connected Network Topology

A fully connected network, complete topology, or full mesh topology is a network topology in which there is a direct link between all pairs of nodes. In a fully connected network with n nodes, there are $n(n-1)/2$ direct links. Networks designed with this topology are usually very expensive to set up, but provide a high degree of reliability due to the multiple paths for data

that are provided by the large number of redundant links between nodes. This topology is mostly seen in military applications. A two-node network is technically a fully connected network.

A **fully connected network** is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching or broadcasting.

Advantage

- provide a high degree of reliability

Disadvantage

- number of connections grows quadratically with the number of nodes, as per the formula

$$c = \frac{n(n-1)}{2}$$

and so it is extremely impractical for large networks

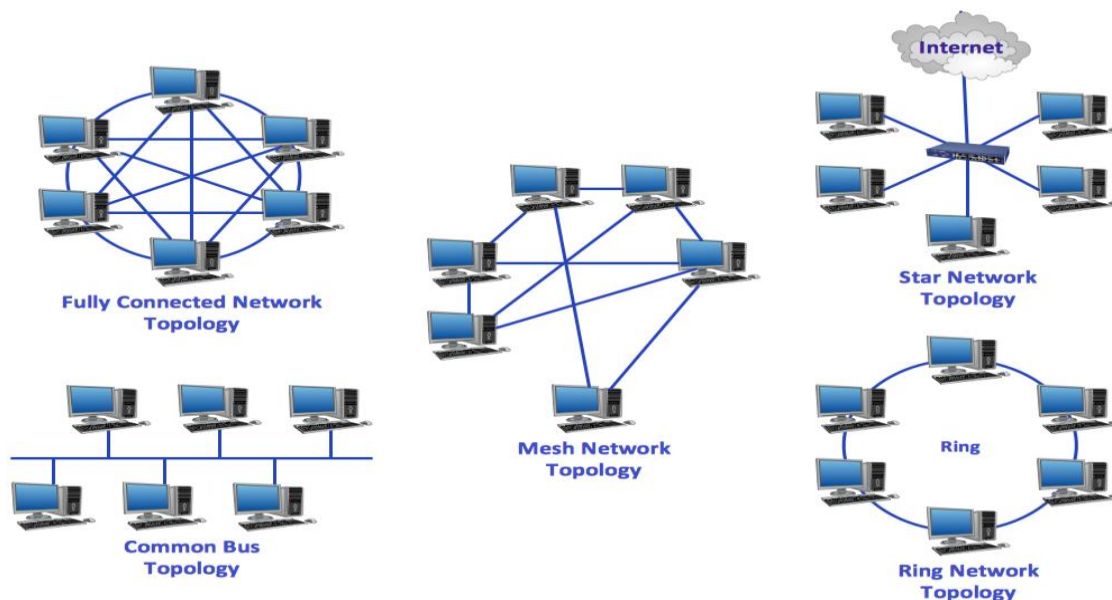


Figure 1.5: Network Topologies

1.7 Factors to consider when choosing Network Topology


Each topology has its own characteristic. To choose the right topology we must see the factors that influenced it. The factors are:

- **Length of cable needed.** The linear bus network uses shorter lengths of cable.
- **Future growth.** With a star topology, expanding a network is easily done by adding another concentrator.
- **Cable type.** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

2. Open Systems Interconnection (OSI/ISO) Reference Model

The Open Systems Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers. The following list details the seven layers of the Open Systems Interconnection (OSI) reference model: Figure 2.1 & Figure , illustrates the seven-layer OSI reference model.

- Layer 7-Application
- Layer 6-Presentation
- Layer 5-Session
- Layer 4-Transport
- Layer 3-Network
- Layer 2-Data link
- Layer 1-Physical

 **Note:** A handy way to remember the seven layers is the sentence "All people seem to need data processing." The beginning letter of each word corresponds to a layer.

- All-Application layer
- People-Presentation layer
- Seem-Session layer
- To-Transport layer
- Need-Network layer
- Data-Data link layer
- Processing-Physical layer

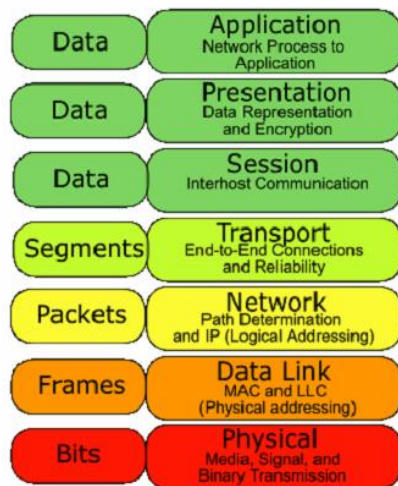


Figure 2.1: The OSI Reference Model Contains Seven Independent Layers

2.1 Characteristics of the OSI Layers

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

Figure 2.2, illustrates the division between the upper and lower OSI layers.

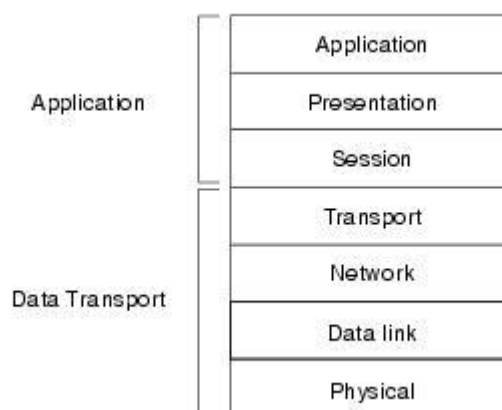


Figure 2.2: Two Sets of Layers Make Up the OSI Layers

2.2 Protocols

The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. In the context of data networking, a protocol is a formal set of rules and conventions that governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.

A wide variety of communication protocols exist. Some of these protocols include LAN protocols, WAN protocols, network protocols, and routing protocols. LAN protocols operate at the physical and data link layers of the OSI model and define communication over the various LAN media. WAN protocols operate at the lowest three layers of the OSI model and define communication over the various wide-area media. Routing protocols are network layer protocols that are responsible for exchanging information between routers so that the routers can select the proper path for network traffic.

Finally, network protocols are the various upper-layer protocols that exist in a given protocol suite. Many protocols rely on others for operation. For example, many routing protocols use network protocols to exchange information between routers. This concept of building upon the layers already in existence is the foundation of the OSI model.

2.3 OSI Model and Communication Between Systems

Information being transferred from a software application in one computer system to a software application in another must pass through the OSI layers. For example, if a software application in System A has information to transmit to a software application in System B, the application program in System A will pass its information to the application layer (Layer 7) of System A. The application layer then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

2.4 Interaction Between OSI Model Layers

A given layer in the OSI model generally communicates with three other OSI layers: the layer directly above it, the layer directly below it, and its peer layer in other networked computer

systems. The data link layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B. Figure 2.3 illustrates this example.

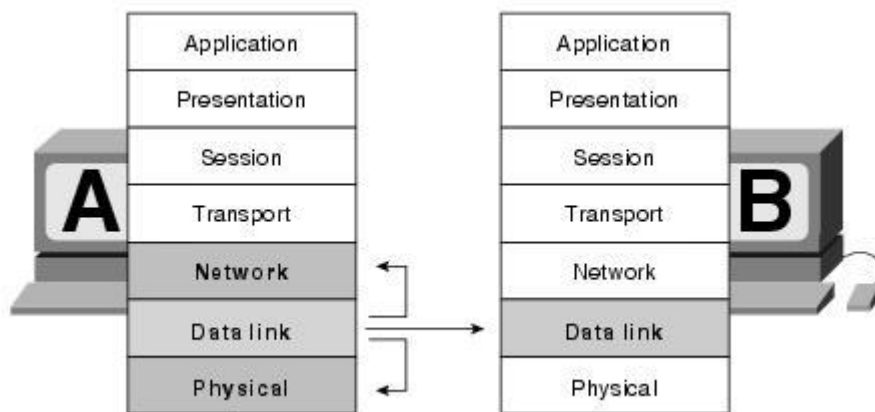


Figure 2.3: OSI Model Layers Communicate with Other Layers

2.5 OSI Layer Services

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems. Three basic elements are involved in layer services: the service user, the service provider, and the service access point (SAP).

In this context, the service user is the OSI layer that requests services from an adjacent OSI layer. The service provider is the OSI layer that provides services to service users. OSI layers can provide services to multiple service users. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer. Figure 2.4 illustrates how these three elements interact at the network and data link layers.

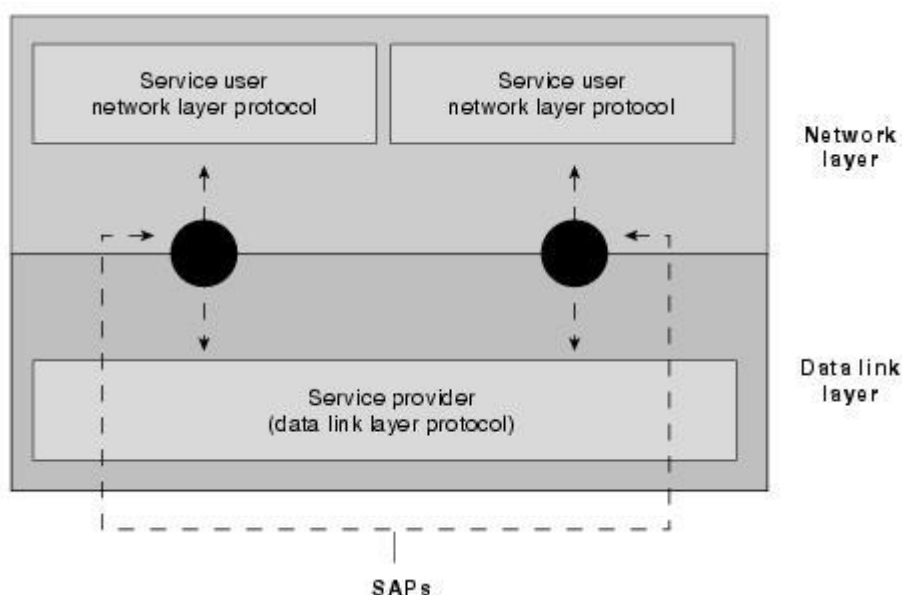


Figure 2.4: Figure: Service Users, Providers, and SAPs Interact at the Network and Data Link Layers

2.6 OSI Model Layers and Information Exchange

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer OSI layers.

Control information typically takes one of two forms: headers and trailers. Headers are prepended to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers. An OSI layer is not required to attach a header or a trailer to data from upper layers.

Headers, trailers, and data are relative concepts, depending on the layer that analyzes the information unit. At the network layer, for example, an information unit consists of a Layer 3 header and data. At the data link layer, however, all the information passed down by the network layer (the Layer 3 header and the data) is treated as data.

In other words, the data portion of an information unit at a given OSI layer potentially can contain headers, trailers, and data from all the higher layers. This is known as encapsulation.

Figure 2.5 shows how the header and data from one layer are encapsulated into the data of the next lowest layer.

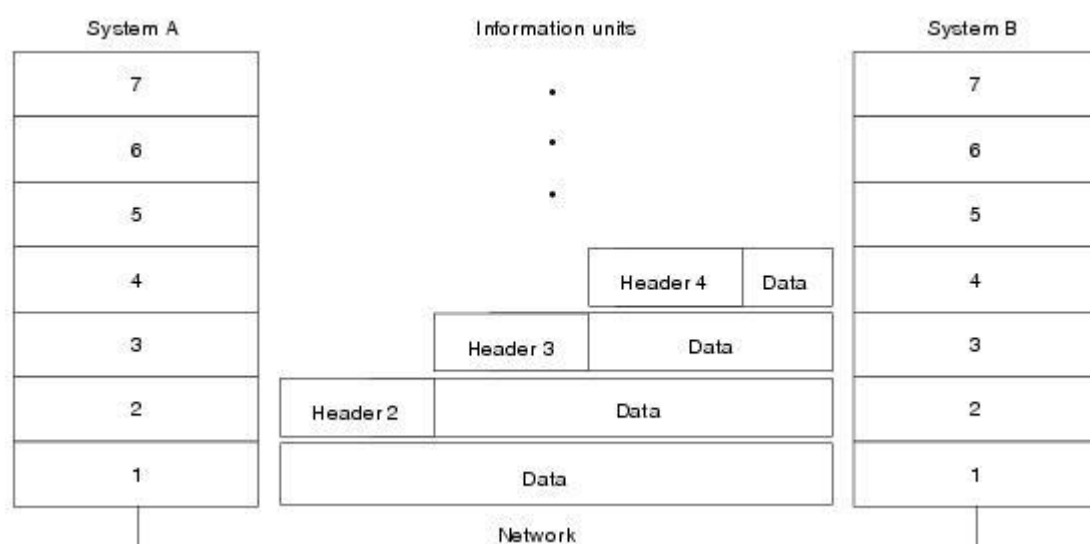


Figure 2.5: Headers and Data Can Be Encapsulated During Information Exchange

Information Exchange Process

The information exchange process occurs between peer OSI layers. Each layer in the source system adds control information to data, and each layer in the destination system analyzes and removes the control information from that data.

If System A has data from a software application to send to System B, the data is passed to the application layer. The application layer in System A then communicates any control information required by the application layer in System B by prepending a header to the data. The resulting information unit (a header and the data) is passed to the presentation layer, which prepends its own header containing control information intended for the presentation layer in System B. The information unit grows in size as each layer prepends its own header (and, in some cases, a trailer) that contains control information to be used by its peer layer in System B. At the physical layer, the entire information unit is placed onto the network medium.

The physical layer in System B receives the information unit and passes it to the data link layer. The data link layer in System B then reads the control information contained in the header prepended by the data link layer in System A. The header is then removed, and the remainder of the information unit is passed to the network layer. Each layer performs the same actions: The layer reads the header from its peer layer, strips it off, and passes the remaining information unit to the next highest layer. After the application layer performs these actions, the data is passed to the recipient software application in System B, in exactly the form in which it was transmitted by the application in System A.

2.7 The Seven OSI/ISO Layers

2.7.1 OSI Model Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors. Physical layer implementations can be categorized as either LAN or WAN specifications. Figure 2.6 illustrates some common LAN and WAN physical layer implementations.

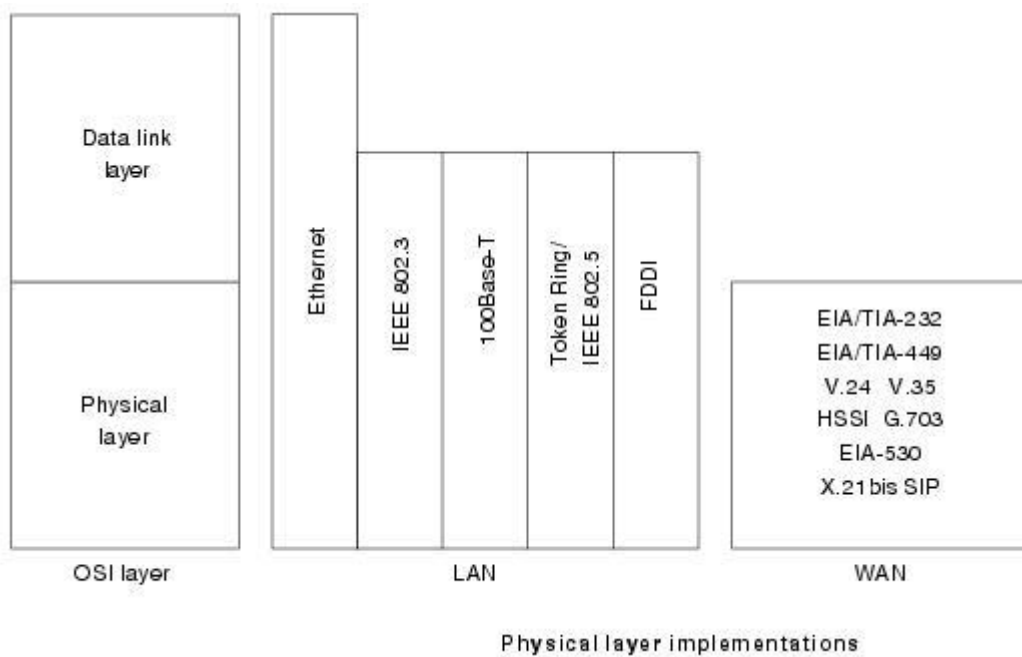


Figure 2.6: Physical Layer Implementations Can Be LAN or WAN Specifications

2.7.2 OSI Model Data Link Layer

The data link layer provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Network topology consists of the data link layer specifications that often define how devices are to be physically connected, such as in a bus or a ring topology. Error notification alerts upper-layer protocols that a transmission error has occurred, and the sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data link layer into two sub layers: Logical Link Control (LLC) and Media Access Control (MAC). Figure 2.7 illustrates the IEEE sub layers of the data link layer.

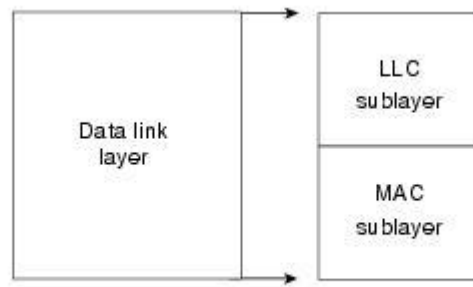


Figure 2.7: The Data Link Layer Contains Two Sub layers

The Logical Link Control (LLC) sub layer of the data link layer manages communications between devices over a single link of a network. LLC is defined in the IEEE 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols. IEEE 802.2 defines a number of fields in data link layer frames that enable multiple higher-layer protocols to share a single physical data link.

The Media Access Control (MAC) sub layer of the data link layer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer.

2.7.3 OSI Model Network Layer

The network layer defines the network address, which differs from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Because this layer defines the logical network layout, routers can use this layer to determine how to forward packets. Because of this, much of the design and configuration work for internetworks happens at Layer 3, the network layer.

2.7.4 OSI Model Transport Layer

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer.

Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link. Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating

various mechanisms for detecting transmission errors, while error recovery involves acting, such as requesting that data be retransmitted, to resolve any errors that occur.

The transport protocols used on the Internet are TCP and UDP.

2.7.5 OSI Model Session Layer

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer. Some examples of session-layer implementations include Zone Information Protocol (ZIP), the AppleTalk protocol that coordinates the name binding process; and Session Control Protocol (SCP), the DECnet Phase IV session layer protocol.

2.7.6 OSI Model Presentation Layer

The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system would be readable by the application layer of another system. Some examples of presentation layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.

Common data representation formats, or the use of standard image, sound, and video formats, enable the interchange of application data between different types of computer systems.

Conversion schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII. Standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination. Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

Presentation layer implementations are not typically associated with a particular protocol stack. Some well-known standards for video include QuickTime and Motion Picture Experts Group (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.

Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF is a standard for compressing and coding graphic images. JPEG is another compression and coding standard for graphic images, and TIFF is a standard coding format for graphic images.

2.7.8 OSI Model 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.

This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

Some examples of application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

2.8 Information Formats

The data and control information that is transmitted through internetworks takes a variety of forms. The terms used to refer to these information formats are not used consistently in the internetworking industry but sometimes are used interchangeably. Common information formats include frames, packets, datagrams, segments, messages, cells, and data units.

A **frame** is an information unit whose source and destination are data link layer entities. A frame is composed of the data link layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the data link layer entity in the destination system. Data from upper-layer entities is encapsulated in the data link layer header and trailer. Figure 2.8 illustrates the basic components of a data link layer frame.

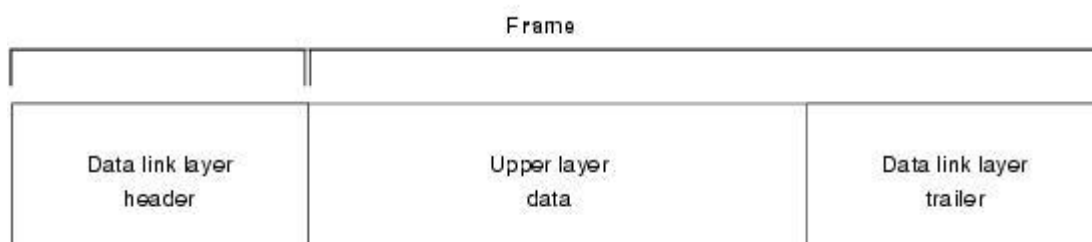


Figure 2.8: Data from Upper-Layer Entities Makes Up the Data Link Layer Frame

A **packet** is an information unit whose source and destination are network layer entities. A packet is composed of the network layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network layer entity in the destination system. Data from upper-layer entities is encapsulated in the network layer header and trailer. Figure 2.9 illustrates the basic components of a network layer packet.

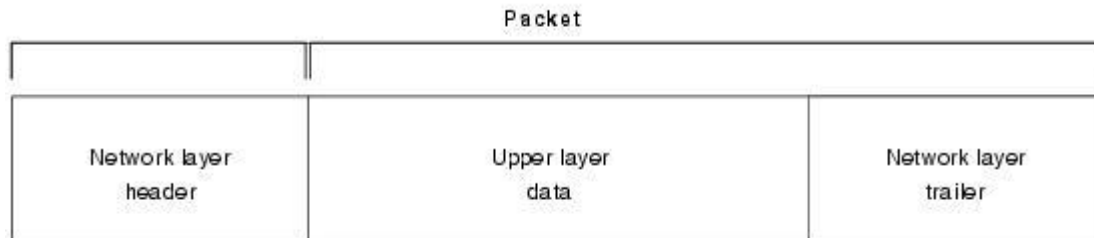


Figure 2.9: Three Basic Components Make Up a Network Layer Packet

The term **datagram** usually refers to an information unit whose source and destination are network layer entities that use connectionless network service.

The term **segment** usually refers to an information unit whose source and destination are transport layer entities.

A **message** is an information unit whose source and destination entities exist above the network layer (often at the application layer).

A **cell** is an information unit of a fixed size whose source and destination are data link layer entities. Cells are used in switched environments, such as Asynchronous Transfer Mode (ATM) and Switched Multimegabit Data Service (SMDS) networks. A cell is composed of the header and payload. The header contains control information intended for the destination data link layer entity and is typically 5 bytes long. The payload contains upper-layer data that is encapsulated in the cell header and is typically 48 bytes long.

The length of the header and the payload fields always are the same for each cell. Figure 2.10 depicts the components of a typical cell.

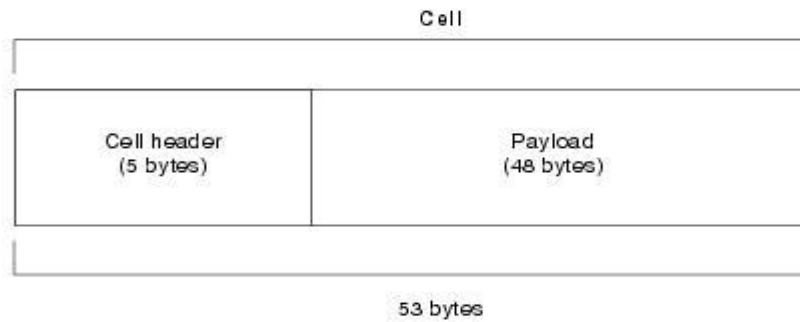


Figure 2.10: Two Components Make Up a Typical Cell

Data unit is a generic term that refers to a variety of information units. Some common data units are service data units (SDUs), protocol data units, and bridge protocol data units (BPDUs). SDUs are information units from upper-layer protocols that define a service request to a lower-layer protocol. PDU is OSI terminology for a packet. BPDUs are used by the spanning-tree algorithm as hello messages.

2.9 Connection-Oriented and Connectionless Network Services

In general, transport protocols can be characterized as being either connection-oriented or connectionless. Connection-oriented services must first establish a connection with the desired service before passing any data. A connectionless service can send the data without any need to establish a connection first. In general, connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not.

Connection-oriented service involves three phases: connection establishment, data transfer, and connection termination.

Connection-oriented network services have more overhead than connectionless ones. Connection-oriented services must negotiate a connection, transfer data, and tear down the connection, whereas a connectionless transfer can simply send the data without the added overhead of creating and tearing down a connection. Each has its place in internetworks.

3. LOCAL AREA NETWORK

A LAN is a high-speed, fault-tolerant data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications

3.1 LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

In a **unicast transmission**, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A **multicast transmission** consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A **broadcast transmission** consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

3.2 LAN Topologies

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

A **bus topology** is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks—including 100BaseT—implement a bus topology, which is illustrated in Figure 3.1



Figure 3.1 Networks Implement a Local Bus Topology

A **ring topology** is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology. Figure 3.2 depicts a logical ring topology.

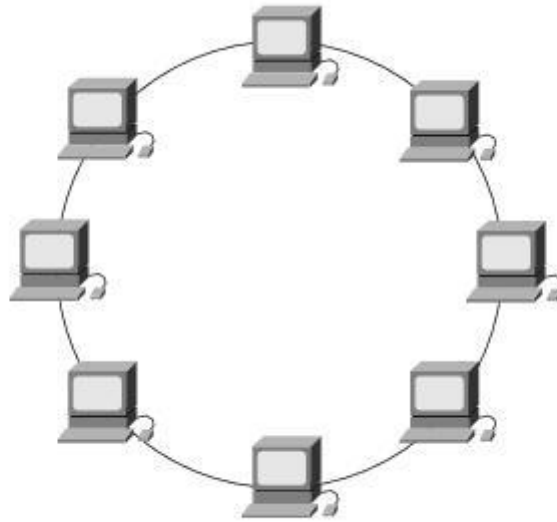


Figure 3.2: Networks Implement a Logical Ring Topology

A **star topology** is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology, which is illustrated in the following figure.

A **tree topology** is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case. Figure 3.3 illustrates a logical tree topology.

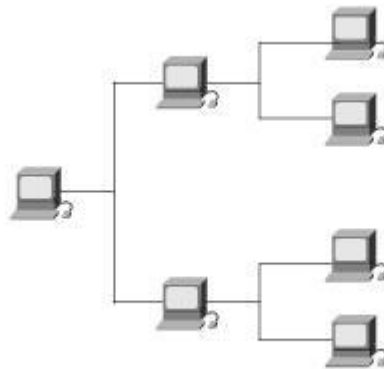


Figure 3.3: A Logical Tree Topology

3.3 LAN Transmission Media

The transmission medium is the physical path between transmitter and receiver in a data transmission system. The characteristics and quality of data transmission are determined both the nature of signal and nature of the medium. Transmission media may be classified as:

1. Guided transmission media
2. Unguided transmission media
3. In both cases, communication is in the form of electromagnetic waves.

With guided media, the waves are guided along a physical path. Examples of guided media are **twisted pair, coaxial cable, and optical fiber (Fiber Optic)**. Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum and seawater. A guided media is contained within physical boundaries, while an unguided medium is boundless.

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network. The different types of cables used in networks are as follows:

- Unshielded Twisted Pair (UTP) cable
- Shielded Twisted Pair (STP) cable
- Coaxial Cable
- Fiber Optic Cable

3.3.1 Twisted Pair Wire (Cable)

Twisted pair wire is the most widely used medium for telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer networking cabling consist of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 100 million bits per second. Twisted pair cabling comes in two forms which are Unshielded Twisted Pair (UTP) and Shielded twisted-pair (STP) which are rated in categories which are manufactured in different increments for various scenarios. Twisted pair - wire twisted to avoid crosstalk interference.

- UTP-Unshielded Twisted Pair. Normally UTP contains 8 wires or 4 pair; 100 meter maximum length; 4-100 Mbps speed.
- STP-Shielded Twisted Pair. 100 meter maximum length; 16-155 Mbps speed; lower electrical interference than UTP.

3.3.1.1 Unshielded Twisted Pair (UTP) Cable

Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks. (See figure 3.4) The quality of UTP may vary from telephone-grade wire to extremely

high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Table 3.1: Categories of Unshielded Twisted Pair

Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

10BaseT refers to the specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals. Category 6 is relatively new and is used for gigabit connections.

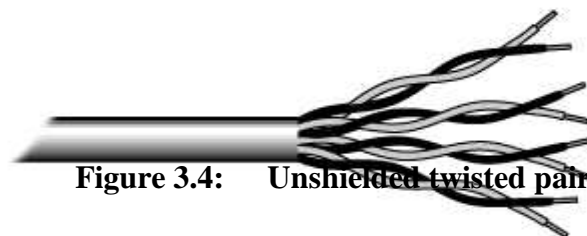


Figure 3.4: Unshielded twisted pair

Unshielded Twisted Pair Connector

The most common type of connector used with UTP is the **RJ-45 connector**.



Figure 3.5: RJ-45 connector

3.3.1.2 Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical

interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

3.3.2 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See figure 3.6). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers. Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable.

Coaxial - two conductors separated by insulation such as TV 75 ohm cable; maximum length of 185 to 500 meters; It is of two types, namely:

- Thin Coaxial
- Thick Coaxial

Figure 3.6: Coaxial Cable



3.3.2.1 Thin Coaxial Cable

Thin Coaxial cable uses a British Naval Connector (BNC) on each end. It is part of the RG-58 family of cable. Maximum cable length is 185 meters. Transmission speed is 10Mbps. Thin Coaxial cable should have 50 ohms impedance; and its terminator has 50 ohms impedance; barrel connector will have no impedance. Maximum thin coaxial nodes are 30 on a segment. One end of each cable is grounded. Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

3.3.3.2 Thick Coaxial Cable

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thicknet is a half inch rigid cable with maximum cable length of 500 meters. Transmission speed is 10Mbps; it is expensive and is not commonly used- (RG-11 or RG-8). A vampire tap or piercing tap is used with a transceiver attached to connect computers to the

cable. 100 connections may be made. The computer has an Attachment Unit Interface (AUI) on its network card which is a 15 pin DB-15 connector. The computer is connected to the transceiver at the cable from its AUI on its network card using a drop cable. Maximum thicknet nodes are 100 on a segment. One end of each cable is grounded.

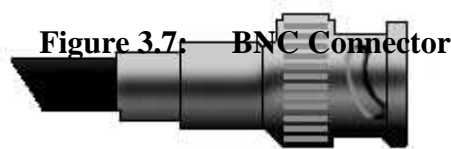
Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

The RG value for cable types refers to its size. Coax cable types are listed below.

- RG-58 /U - 50 ohm, with a solid copper wire core for thin ethernet.
- RG-58 A/U - 50 ohm, with a stranded wire core.
- RG-58 C/U - Military version of RG-58 A/U.
- RG-59 - 75 ohm, for broadband transmission such as cable TV.
- RG-62 - 93 ohm, primarily used for ArcNet.
- RG-6 - used for satellite cable (if you want to run a cable to a satellite).
- RG-8 - 50 ohm thick ethernet.
- RG-11 - 75 ohm thick ethernet.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See figure 3.7). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.



3.3.3 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See figure 3.8). Data is transmitted using light rather than electronic signals (electrons) eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also been made the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting. Usually there are two fibers, one for each direction. Cable length of 2 Kilometers; speed from 100Mbps to 2Gbps. This is the most expensive and most difficult to install, but is not subject to interference. There are two types of cables:

- single mode cables use with lasers have greater bandwidth and cost more. Injection Laser diodes (ILD) work with single mode cable.
- multimode cables use with Light Emitting Diode (LED) drivers; all signals appear to arrive at the same time. P intrinsic N diodes or photodiodes are used to convert light to electric signals when using multimode.



Figure 3.8: Fiber Optic Cable

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

Facts about fiber optic cables:

- Outer insulating jacket is made of Teflon or PVC.
- Kevlar fiber helps to strengthen the cable and prevent breakage.
- A plastic coating is used to cushion the fiber center.
- Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

3.3.4 Ethernet Cabling

The types of Ethernet cables available are

1. Straight-through cable
2. Crossover cable
3. Rolled cable

3.3.4.1 Straight-through cable

Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to / create this type. Only pins 1, 2, 3 and 6 are used. Just connect 1 to 1, 2 to 2, 3 to 3 and 6 to 6 and you will be up and networking in no time while practically we connect all 4 pairs straighten of CAT-5. However, this would be an Ethernet only cable and would not work with Voice, Token Ring, ISDN, etc. This type of cable is used to connect

1. Host to switch or hub
2. Router to switch or hub

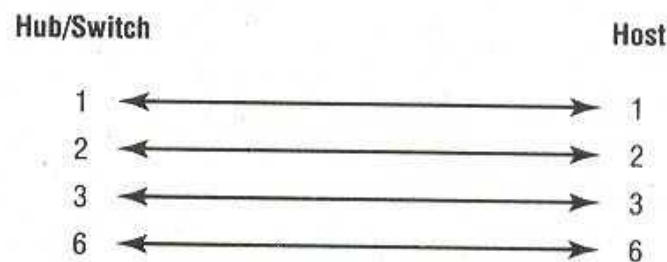


Figure 3.9: Straight-through cable

3.3.4.2 Crossover Cable

Four wires are used in straight-through cable to connect Ethernet devices. Only four pins are used in this type of cabling. In crossover cable we connect 1 to 3 and 2 to 6 on each side of cable. This type of cable is used to connect

1. Switch to switch
2. Hub to hub
3. Host to host
4. Hub to switch
5. Router direct to host

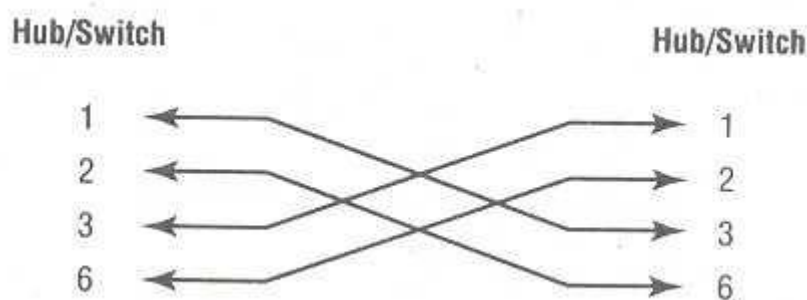


Figure 3.10: Crossover Cable

3.3.4.3 Rolled Cable

Although rolled cable is not used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port. If you have a Cisco router or switch, you would use this cable to connect your PC running Hyper Terminal to the Cisco hardware. Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networking

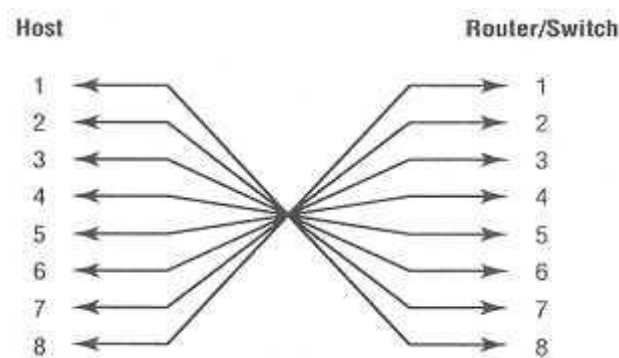


Figure 3.11: Rolled Cable

Table 3.2: Cable Summary

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100meters
10Base2	Thin Coaxial	185Meters
10Base5	Thick Coaxial	500Meters
10BaseF	Fiber Optic	2000Meters
100BaseT	Unshielded Twisted pair	100Meters
100BaseTX	Unshielded Twisted Pair	220Meters

3.4 LAN devices

Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches, and routers.

- A **repeater** is a physical layer device used to interconnect the media segments of an extended network, which amplifies or regenerates digital signals received while sending them from one part of a network into another. It works on OSI layer 1. Repeater is a hardware device used to strengthen signals being transmitted on networks. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment. These

actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified. The total number of repeaters and network segments that can be connected is limited due to timing and other issues.

- A **hub** is a physical-layer device that connects multiple user stations, each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network while maintaining the logical bus or ring configuration of the LAN. A hub connects multiple Ethernet segments, making them act as a single segment. When using a hub, every attached device shares the same broadcast domain and the same collision domain. Therefore, only one computer connected to the hub is able to transmit at a time. Depending on the network topology, the hub provides a basic level 1 OSI model connection among the network objects (workstations, servers, etc.). It provides bandwidth which is shared among all the objects, in contrast to switches, which provide a connection between individual nodes. It works on OSI layer 1. In some respects, a hub functions as a multiport repeater. Types of hub include Passive hub, Active hub & Intelligent hub.
- A **LAN extender** is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network-layer protocols (such as IP, IPX, and AppleTalk), and filter traffic based on the MAC address or network-layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts. LAN extenders, however, are not capable of segmenting traffic or creating security firewalls.
- **Bridges** is a hardware networking device used to connect two LANs. A bridge operates at data link layer of the OSI reference model. Bridges analyze incoming frames, make forwarding decisions based on information contained in the frames, and forward the frames toward the destination. In some cases, such as source-route bridging, the entire path to the destination is contained in each frame. In other cases, such as transparent bridging, frames are forwarded one hop at a time toward the destination.
- **Switches** a device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment. Unlike a hub, a switch splits the network traffic and sends it to different destinations rather than to all systems on the network. It works on OSI layer 2. They are data link layer devices that, like bridges, enable multiple physical LAN segments to be interconnected into a single larger network. Similar to bridges, switches forward and flood traffic based on MAC addresses. Because switching is performed in hardware instead of in software, however, it is significantly faster. Switches use either store-and-forward switching or cut-through switching when forwarding traffic. Many

types of switches exist, including ATM switches, LAN switches, and various types of WAN switches.

- **A Router is** a specialized network device that determines the next network point to which it can forward a data packet towards the ultimate destination of the packet. A network layer device that connects networks with different physical media and translates between network architectures. Unlike a gateway, it cannot interface different protocols. It works on OSI layer 3. Routers perform two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as switching. Although switching is relatively straightforward, path determination can be very complex. Routers can:
 - Direct signal traffic efficiently
 - Route messages between any two protocols
 - Route messages between linear bus, star, star-wired ring topologies
 - Route messages across fiber optic, coaxial and twisted-pair cabling



Hub



A Switch



A bridge



A router

Figure 3.12: LAN devices

3.5 LAN Media-Access Methods

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time. This is done in two main ways: Carrier Sense Multiple Access Collision Detect (CSMA/CD) and token passing.

3.5.1 CSMA/CD

In the **CSMA/CD** media-access scheme, network devices contend for use of the physical network medium. In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases. CSMA/CD is therefore sometimes called contention access. Examples of LANs that use the CSMA/CD media-access scheme are Ethernet/IEEE 802.3 networks, including 100BaseT.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

Normally CSMA/CD networks are half-duplex, meaning that while a device sends information, it cannot receive at the time. While that device is talking, it is incapable of also listening for other traffic. This is much like a walkie-talkie. When one person wants to talk, he presses the transmit button and begins speaking. While he is talking, no one else on the same frequency can talk. When the sending person is finished, he releases the transmit button and the frequency is available to others. When switches are introduced, full-duplex operation is possible. Full-duplex works much like a telephone-you can listen as well as talk at the same time. When a network device is attached directly to the port of a network switch, the two devices may be capable of operating in full-duplex mode. In full-duplex mode, performance can be increased, but not quite as much as some like to claim. A 100-Mbps Ethernet segment is capable of transmitting 200 Mbps of data, but only 100 Mbps can travel in one direction at a time. Because

most data connections are asymmetric (with more data traveling in one direction than the other), the gain is not as great as many claim. However, full-duplex operation does increase the throughput of most applications because the network media is no longer shared. Two devices on a full-duplex connection can send data as soon as it is ready.

3.5.2 Token-passing

In the **token-passing** media-access scheme, network devices access the physical medium based on possession of a token. In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval. Examples of LANs that use the token-passing media-access scheme are Token Ring/IEEE 802.5 and FDDI.

Token-passing networks such as Token Ring can also benefit from network switches. In large networks, the delay between turns to transmit may be significant because the token is passed around the network.

3.6 LAN Technologies

3.6.1 Ethernet

The term Ethernet refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps-10Base-T Ethernet
- 100 Mbps-Fast Ethernet
- 1000 Mbps-Gigabit Ethernet (1000BaseT)

It is a widely used LAN technology which is invented by Bob Metcalfe and D.R. Boggs at Xerox PARC (Palo Alto Research Center) in 1970s. Defined in a standard by Xerox, Intel and Digital - *DIX* standard, standard now managed by IEEE - defines formats, voltages, cable lengths. It was standardized in IEEE 802.3 in 1980. One Ethernet cable is sometimes called a *segment* which is limited to 500 meters in length. The Minimum separation between connections is 3 meters. Ethernet originally speed is 3Mbps but the current standard is 10Mbps.

Traditional Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector. Ethernet follows star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.

Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data. This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other nodes have already transmitted on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. A collision occurs when this happens. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

- Is easy to understand, implement, manage, and maintain
- Allows low-cost network implementations
- Provides extensive topological flexibility for network installation
- Guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer

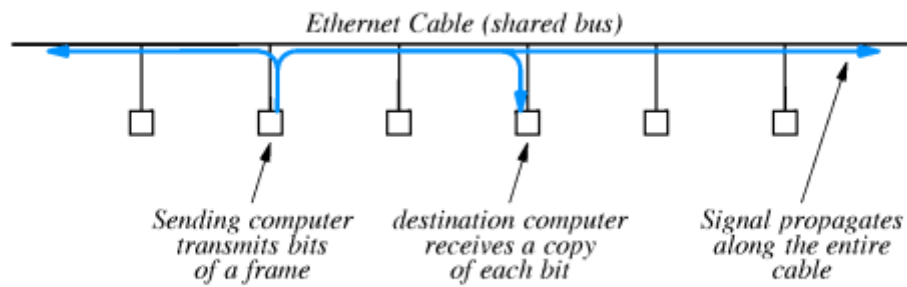


Figure 3.13: Transmission of bits along Ethernet

Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100 MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance) technique for wireless Ethernet LAN.

Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100 MBPS on fiber. Ethernet over fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

Giga-Ethernet

After being introduced in 1995, Fast-Ethernet could enjoy its high speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber(1000BaseX).

3.6.2 Token Ring/ IEEE 802.5

The Token Ring network was originally developed by IBM in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and it continues to shadow IBM's Token Ring development. The term Token Ring generally is used to refer to both IBM's Token Ring network and IEEE 802.5 networks.

Token Ring and IEEE 802.5 networks are basically compatible, although the specifications differ in minor ways. IBM's Token Ring network specifies a star, with all end stations attached to a device called a Multistation Access Unit (MSAU). In contrast, IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on a star. Other differences exist, including media type (IEEE 802.5 does not specify a media type, although IBM Token Ring networks use twisted-pair wire) and routing information field size.

Token Ring and IEEE 802.5 are two principal examples of token-passing networks (FDDI is the other) i.e the access method used involves token-passing. Token-passing networks move a small frame, called a token, around the network. Token is short, reserved frame that cannot appear in data. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time

In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. Because there is only one token, only one computer will transmit at a time, hardware must regenerate token if lost. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

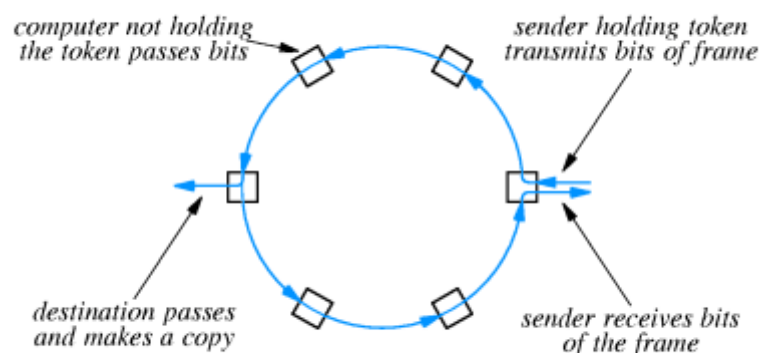


Figure 3.14: Operation of Token ring

3.6.3 FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. *Fiber Distributed Data Interconnect* (FDDI) is another ring technology, FDDI uses a dual ring physical topology. The access method used by FDDI involves token-passing. It uses fiber optics between stations and transmits data at 100Mbps. FDDI uses pairs of fibers to form two concentric rings. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. It uses *counter-rotating* rings in which data flows in opposite directions. In case of fiber or station failure, remaining stations *loop back* and reroute data through spare ring. All stations automatically configure loop back by monitoring data ring. A major advantage of FDDI is high speed. It operates over fiber optic cable at 100 Mbps.

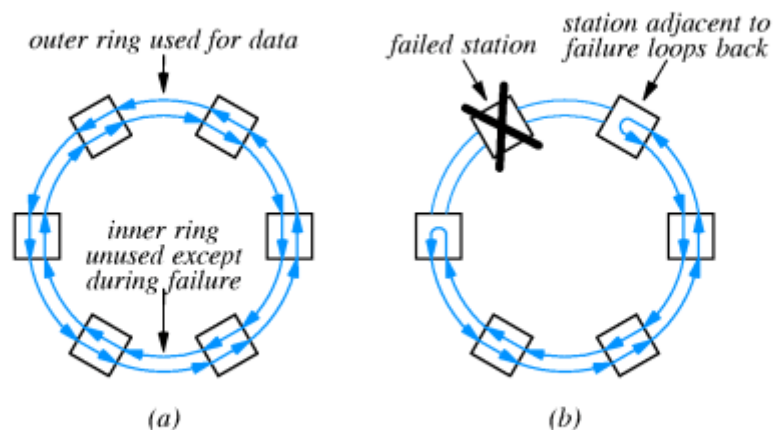


Figure 3.15: Operation of FDDI

3.6.4 Local Talk

This is a LAN technology that uses bus topology. Local Talk was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is low speed. Its speed of transmission is only 230.4 Kbps. It has low cost ("free" with a Macintosh); easy to install and connect.

3.6.5 Wireless LAN (WLAN)

WLAN use radio signals at 900MHz and transmit data at the rate of 2Mbps. Its shared medium is radio instead of coax. In contrast with wired LAN, not all participants may be able to reach each other. WLAN has low signal strength, propagation blocked by walls, etc.

Wireless uses *collision avoidance* rather than collision detection. Transmitting computer sends very short message to receiver while receiver responds with short message reserving slot for transmitter. Response from receiver is *broadcast* so all potential transmitters receive reservation. During collisions, receiver may receive simultaneous requests which results in collision at receiver. **Both** requests are lost, neither transmitter receives reservation; both use backoff and retry. Receiver may receive closely spaced requests, it selects one and the selected transmitter sends message while transmitter not selected uses backoff and retries

3.6.6 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) technology consists of electronic packet switches to which computers can connect. ATM switches form *hub* into which computers connect in a *star* topology. Computers get point-to-point connections - data from transmitter is routed directly through hub switches to destination. ATM transmits data at over 100Mbps at a speed of 155 Mbps and higher and uses fiber optics to connect computer to switch. Each connection includes two fibers. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients. As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

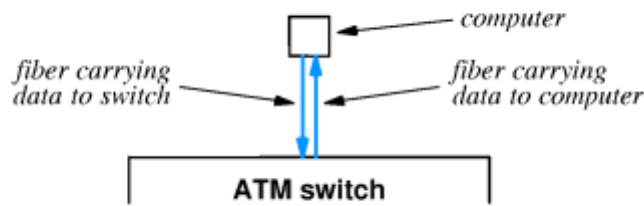


Figure 3.16: ATM Switch

Table 3.3: Comparing LAN Technologies

Protocol	Cable	Speed	Topology	Media Access Method
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree	CSMA/CD
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star	CSMA/CD
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star	CSMA/CA
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring	Token Passing
FDDI	Fiber	100 Mbps	Dual ring	Token Passing
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree	

3.6 LAN Application and Security

3.6.1 LAN Applications

1. Personal Computer LANs

- A common LAN configuration is one that supports personal computers. With the relatively low cost of such systems, individual managers within organizations often independently procure personal computers for departmental applications, such as spreadsheet and project management tools, and for Internet access.
- Some programs, such as econometric forecasting models, are too big to run on a small computer. Corporate-wide data files, such as accounting and payroll, require a centralized facility but should be accessible to a number of users. In addition, there are other kinds of files that, although specialized, must be shared by a number of users. Further, there are sound reasons for connecting individual intelligent workstations not

only to a central facility but to each other as well. Members of a project or organization team need to share work and information. By far the most efficient way to do so is digitally.

- Certain expensive resources, such as a disk or a laser printer, can be shared by all users of the departmental LAN. In addition, the network can tie into larger corporate network facilities. For example, the corporation may have a building-wide LAN and a wide area private network. A communications server can provide controlled access to these resources.

2. Back-End Networks and Storage Area Networks

Back-end networks are used to interconnect large systems such as mainframes, supercomputers, and mass storage devices. The key requirement here is for bulk data transfer among a limited number of devices in a small area. Back-end networks are commonly found at sites of large companies or research installations with large data-processing budgets. Because of the scale involved, a small difference in productivity can mean millions of dollars.

A concept related to that of the back-end network is the storage area network (SAN). A SAN is a separate network to handle storage needs. The SAN unties storage tasks from specific servers and creates a shared storage facility across a high-speed network. The collection of networked storage devices can include hard disks, tape libraries, and CD arrays. Most SANs use Fibre Channel

3. High-Speed Office Networks

Traditionally, the office environment has included a variety of devices with low- to medium-speed data transfer requirements. However, new applications in the office environment have been developed for which the limited speeds (up to 10 Mbps) of the traditional LAN are inadequate. Desktop image processors have increased network data flow by an unprecedented amount.

Examples of these applications include fax machines, document image processors, and graphics programs on personal computers and workstations. Consider that a typical page with 200 picture elements, or *pixels* (black or white points), per inch resolution (which is adequate but not high resolution) generates 3,740,000 bits (8.5 inches x 11 inches x 40,000 pixels per square inch). Even with compression techniques, this generates a tremendous load. In addition, disk technology and price/performance have evolved so that desktop storage capacities in the gigabyte range are typical. These new demands require LANs with high speed that can support the larger numbers and greater geographic extent of office systems as compared to back-end systems.

4. Backbone LANs

The increasing use of distributed processing applications and personal computers has led to a need for a flexible strategy for local networking. Support of premises-wide data communications requires a networking service that's capable of spanning the distances involved and that interconnects equipment in a single (perhaps large) building or a cluster of buildings.

5. Factory LANs

The factory environment is increasingly being dominated by automated equipment: programmable controllers, automated materials-handling devices, time and attendance stations, machine vision devices, and various forms of robots. To manage the production or manufacturing process, it's essential to tie this equipment together. And, indeed, the very nature of the equipment facilitates this. Microprocessor devices have the potential to collect information from the shop floor and accept commands. With the proper use of the information and commands, it's possible to improve the manufacturing process and to provide detailed machine control.

The more a factory is automated, the greater the need for communications. Only by interconnecting all the devices and by providing mechanisms for their cooperation can the automated factory be made to work. The means for interconnection is the factory LAN.

Factory LANs are a niche market requiring, in general, more flexible and reliable LANs than are found in the typical office environment.

6. Library LANs

Application of LANs in Libraries:

- Housekeeping applications - acquisition, cataloguing, circulation control.
- Educational programmes - user education from distance and other study programmes.
- Office administration - connection to administration offices for easy access of necessary files.
- Connection with other libraries - inter library loans and electronic journals.

3.6.2 LAN security

LAN can be secured through the use of the following, Private VLANs, VLAN Membership Policy Server (VMPS), VLAN Access Lists (VACLs), port security, port filtering, IPSEC (IP Security), Intrusion Detection System (IDS), Firewalls and other LAN security features

There are many resources available to help secure your LAN. They fall into four main categories:

- Security scan programs that you run from a web page
- Port monitors and Trojan cleaners
- "Firewalls" that you run on your computer(s)
- Security related Web sites.
- Security applications

4. WIDE AREA NETWORK (WAN)

WAN operates beyond the geographic scope of a LAN. As shown in Figure 4-1, WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.

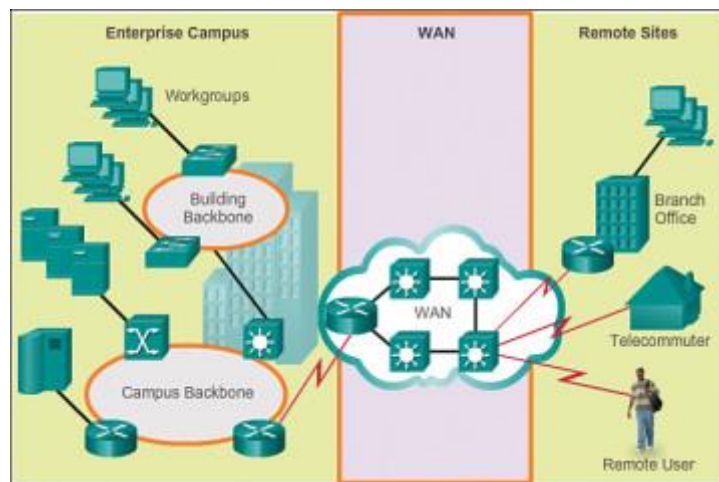


Figure 4.1: WANs Interconnect Users and LANs

A WAN is owned by a *service provider*. An organization must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide links to interconnect remote sites for the purpose of transporting data, voice, and video. In contrast, LANs are typically owned by the organization and used to connect local computers, peripherals, and other devices within a single building or other small geographic area.

4.1 WANs in the OSI Model

As shown in Figure 4.2, WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).

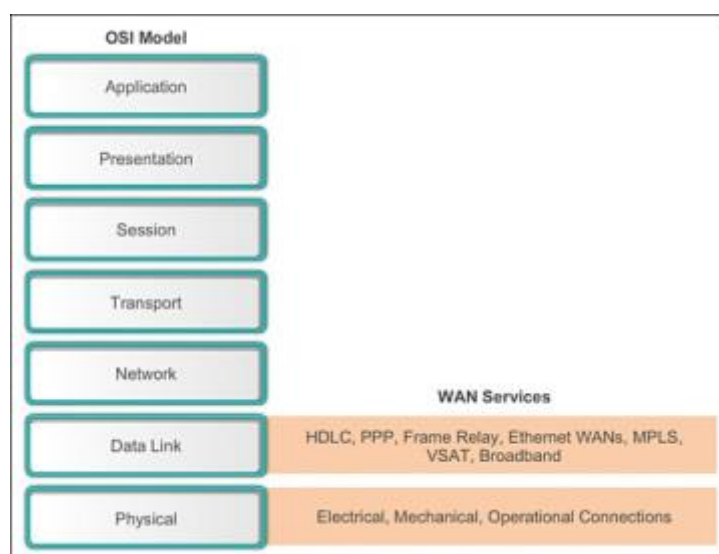


Figure 4.2: WANs Operate in Layer 1 and Layer 2

WAN access standards typically describe both physical layer delivery methods and data link layer requirements, including physical addressing, flow control, and encapsulation.

WAN access standards are defined and managed by a number of recognized authorities, including the

- Telecommunication Industry Association and the Electronic Industries Alliance (TIA/EIA)
- International Organization for Standardization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)

Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider. Layer 2 protocols define how data is encapsulated for transmission toward a remote location, and the mechanisms for transferring the resulting frames. A variety of different technologies are used, such as the ***Point-to-Point Protocol (PPP)***, ***Frame Relay***, and ***Asynchronous Transfer Mode (ATM)***. Some of these protocols use the same basic framing or a subset of the ***High-Level Data Link Control (HDLC)*** mechanism. Most WAN links are point to point. For this reason, the address field in the Layer 2 frame is usually not used.

WAN networks use different types of media to transmit data. Some media used for WAN data transmissions are similar to those used for LAN data transmissions but implementation differs. Examples include Copper wires, fiber-optic cables, radio frequency (RF) signals

4.2 Common WAN Terminology

One primary difference between a WAN and a LAN is that an organization must subscribe to an outside WAN service provider and use the WAN carrier network services to interconnect its sites and users. A WAN uses data links provided by carrier services to access the Internet and connect different locations of an organization to each other, to locations of other organizations, to external services, and to remote users.

The physical layer of a WAN describes the physical connections between the company network and the service provider network. As illustrated in [Figure 4.3](#), common terminology is used to describe WAN components and reference points.

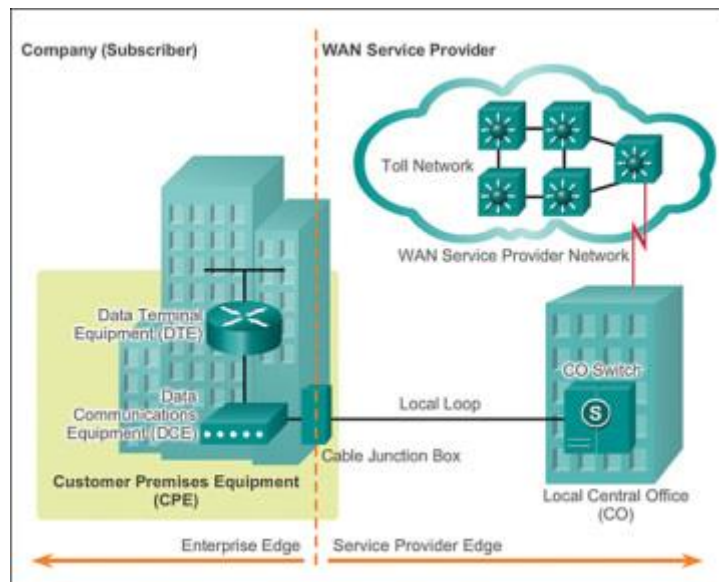


Figure 4.3: Common WAN Terminology

Specifically, these terms include

- **Customer Premises Equipment (CPE):** The devices and inside wiring located on the enterprise edge connecting to a carrier link. The subscriber either owns the CPE or leases the CPE from the service provider. A subscriber, in this context, is a company that arranges for WAN services from a service provider.
- **Data Communications Equipment (DCE):** Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.
- **Data Terminal Equipment (DTE):** The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.
- **Demarcation point:** A point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.
- **Local loop:** The actual copper or fiber cable that connects the CPE to the CO of the service provider. The local loop is also sometimes called the “last mile.”
- **Central office (CO):** The CO is the local service provider facility or building that connects the CPE to the provider network.

- **Toll network:** This consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

4.3 WAN switching methods

Switching of any type involves moving something through a series of intermediate steps, or segments, rather than moving it directly from start point to end point. Switching in networks works in somewhat the same way: Instead of relying on a permanent connection between source and destination, network switching relies on series of temporary connections that relay messages from station to station. Switching serves the same purpose as the direct connection, but it uses transmission resources more efficiently.

WANs (and LANs, including Ethernet and Token Ring) rely primarily on packet switching, but they also make use of circuit switching, message switching, and the relatively recent, high-speed packet-switching technology known as *cell relay*.

4.3.1 Circuit Switching

A type of communications that establishes a dedicated communications channel for the duration of a given transmission. The oldest means by which communications channels were established. Circuit switching involves creating a direct physical connection between sender and receiver, a connection that lasts as long as the two parties need to communicate. In order for this to happen, of course, the connection must be set up before any communication can occur. Once the connection is made, however, the sender and receiver can count on "owning" the bandwidth allotted to them for as long as they remain connected. Although both the sender and receiver must abide by the same data transfer speed, circuit switching does allow for a fixed (and rapid) rate of transmission. The primary drawback to circuit switching is the fact that any unused bandwidth remains exactly that: unused. Because the connection is reserved only for the two communicating parties, that unused bandwidth cannot be "borrowed" for any other transmission.

The most common form of circuit switching happens in that most familiar of networks, the telephone system, but circuit switching is also used in some networks. Currently available ISDN lines, also known as *narrowband ISDN*, and the form of T1 known as *switched T1* are both examples of circuit-switched communications technologies. [Figure 4.4](#) illustrates an example of this type of circuit.

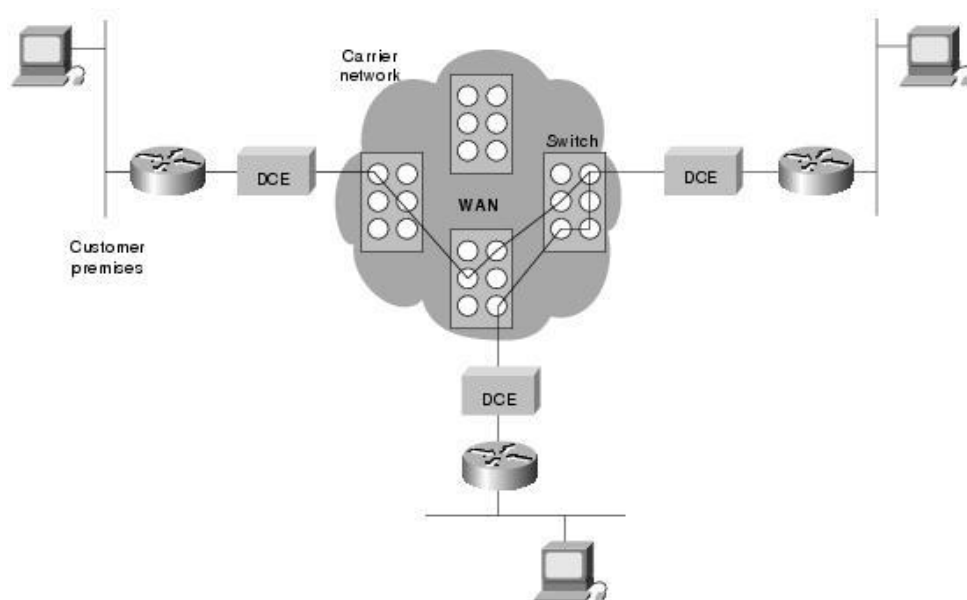


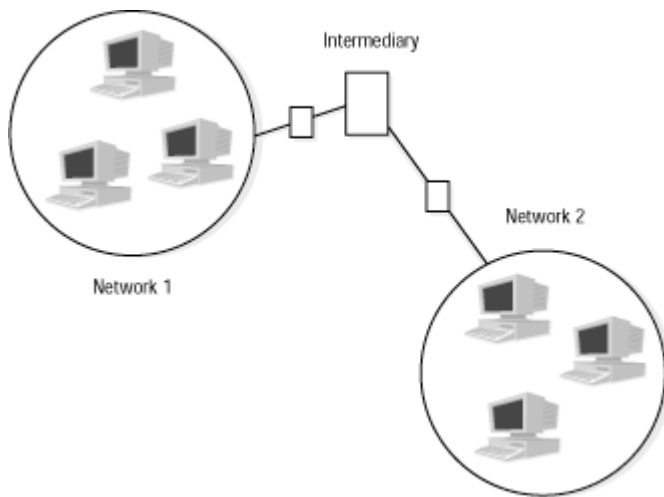
Figure 4.4: A Circuit-Switched WAN Undergoes a Process Similar to That Used for a Telephone Call

4.3.2 Message Switching

A data communications technology that routes whole messages to their destination one hop at a time. It is developed in 1961, evolved into packet switching. Unlike circuit switching, message switching does not involve a direct physical connection between sender and receiver. When a network relies on message switching, the sender can fire off a transmission—after addressing it appropriately—whenever it wants. That message is then routed through intermediate stations or, possibly, to a central network computer. Along the way, each intermediary accepts the entire message, scrutinizes the address, and then forwards the message to the next party, which can be another intermediary or the destination node.

What is notable about message-switching networks, and indeed happens to be one of their defining features, is that the intermediaries aren't required to forward messages immediately. Instead, they can hold messages before sending them on to their next destination. This is one of the advantages of message switching. Because the intermediate stations can wait for an opportunity to transmit, the network can avoid, or at least reduce, heavy traffic periods, and it has some control over the efficient use of communication lines.

Message switching today is more likely to be known as store-and-forward. E-mail is an example of store-and-forward technology



4.3.3 Packet Switching

In Packet Switching data is broken up into small blocks of data called packets. A network communications technology that only opens up connections long enough for a small data packet to move from one network segment to another.

Packet switching, although it is also involved in routing data within and between LANs such as Ethernet and Token Ring, is also the backbone of WAN routing. It's not the highway on which the data packets travel, but it *is* the dispatching system and to some extent the cargo containers that carry the data from place to place. In a sense, packet switching is the Federal Express or United Parcel Service of a WAN.

In packet switching, all transmissions are broken into units called packets, each of which contains addressing information that identifies both the source and destination nodes. These packets are then routed through various intermediaries, known as *Packet Switching Exchanges (PSEs)*, until they reach their destination. At each stop along the way, the intermediary inspects the packet's destination address, consults a routing table, and forwards the packet at the highest possible speed to the next link in the chain leading to the recipient.

As they travel from link to link, packets are often carried on what are known as *virtual circuits*—temporary allocations of bandwidth over which the sending and receiving stations communicate after agreeing on certain "ground rules," including packet size, flow control, and error control. Thus, unlike circuit switching, packet switching typically does not tie up a line indefinitely for the benefit of sender and receiver. Transmissions require only the bandwidth needed for forwarding any given packet, and because packet switching is also based on multiplexing messages, many transmissions can be interleaved on the same networking medium at the same time. [Figure 4.5](#) shows an example packet-switched circuit.

The virtual connections between customer sites are often referred to as a virtual circuit.

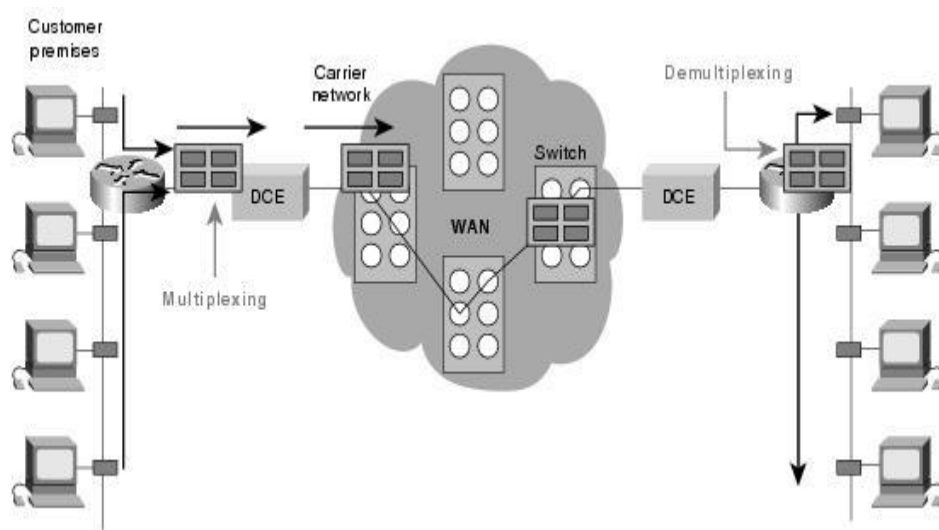


Figure 4.5: Packet Switching Transfers Packets across a Carrier Network

Packet-switched networks transfer data over variable routes in little bundles called packets. The sender can't just assume that a transmitted packet will eventually find its way to the correct destination. There has to be some kind of connection—some kind of link between the sender and the recipient. That link can be based on either *connectionless* or *connection-oriented* services, depending on the type of packet-switching network involved.

- In a (so to speak) connectionless "connection," an actual communications link isn't established between sender and recipient before packets can be transmitted. Each transmitted packet is considered an independent unit, unrelated to any other. As a result, the packets making up a complete message can be routed over different paths to reach their destination.
- In a connection-oriented service, the communications link is made before any packets are transmitted. Because the link is established before transmission begins, the packets comprising a message all follow the same route to their destination. In establishing the link between sender and recipient, a connection-oriented service can make use of either *switched virtual circuits (SVCs)* or *permanent virtual circuits (PVCs)*:

Using a **switched virtual circuit** is comparable to calling someone on the telephone. The caller connects to the called computer, they exchange information, and then they terminate the connection while using a **permanent virtual circuit**, on the other hand, is more like relying

on a leased line. The line remains available for use at all times, even when no transmissions are passing through it.

4.4 WAN Technologies

WAN technologies are widely diverse and include microwaves and WiMAX to cellular technologies to Frame Relay.

FRAME RELAY

Frame Relay is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay originally was designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well. WAN service designed to connect two points that require only intermittent communications

Frame relay is a newer, faster, and less cumbersome form of packet switching than X.25. Often referred to as a *fast packet switching* technology, frame relay transfers variable-length packets up to 4 KB in size at 56 Kbps or T1 (1.544 or 2 Mbps) speeds over permanent virtual circuits. Operating only at the data link layer, frame relay outpaces the X.25 protocol by stripping away much of the "accounting" overhead, such as error correction and network flow control, that is needed in an X.25 environment. Because frame relay, unlike X.25 with its early reliance on often unreliable telephone connections, was designed to take advantage of newer digital transmission capabilities, such as fiberoptic cable and ISDN. These offer reliability and lowered error rates and thus make the types of checking and monitoring mechanisms in X.25 unnecessary.

Devices attached to a Frame Relay WAN fall into the following two general categories:

- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches.

Like X.25, however, frame relay is based on the transmission of variable length packets, and it defines the interface between DTEs and DCEs. It is also based on multiplexing a number of (virtual) circuits on a single communications line.

Like X.25, frame relay switches rely on addressing information in each frame header to determine where packets are to be sent. The network transfers these packets at a predetermined rate that it assumes allows for free flow of information during normal operations.

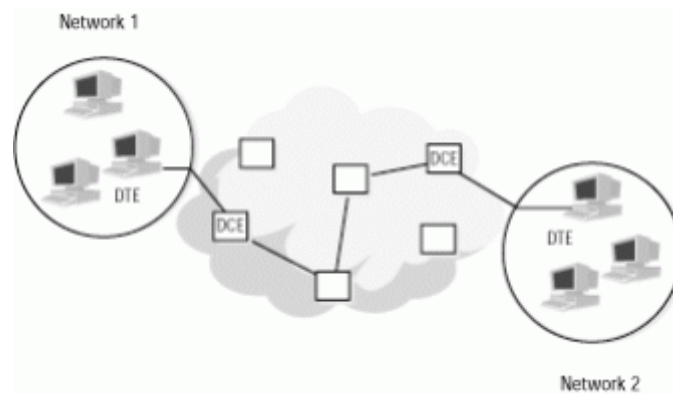
Although frame relay networks do not themselves take on the task of controlling the flow of frames through the network, they do rely on special bits in the frame headers that enable them to address congestion. The first response to congestion is to request the sending application to "cool it" a little and slow its transmission speed; the second involves discarding frames flagged as lower-priority deliveries, and thus essentially reducing congestion by throwing away some of the cargo.

Frame relay networks connecting LANs to a WAN rely, of course, on routers and switching equipment capable of providing appropriate frame-relay interfaces.

X.25

Originating in the 1970s, X.25 is a connection-oriented, packet-switching protocol, originally based on the use of ordinary analog telephone lines that has remained a standard in networking for about twenty years. Computers on an X.25 network carry on full-duplex communication, which begins when one computer contacts the other and the called computer responds by accepting the call.

Although X.25 is a packet-switching protocol, its concern is not with the way packets are routed from switch to switch between networks, but with defining the means by which sending and receiving computers (known as DTEs) interface with the communications devices (DCEs) through which the transmissions actually flow. X.25 has no control over the actual path taken by the packets making up any particular transmission, and as a result the packets exchanged between X.25 networks are often shown as entering a cloud at the beginning of the route and exiting the cloud at the end.



A recommendation of the ITU (formerly the CCITT), X.25 relates to the lowest three network layers—physical, data link, and network—in the ISO reference model:

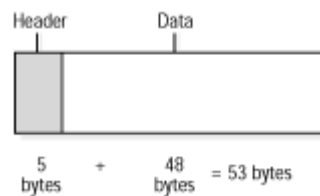
- At the lowest (physical) layer, X.25 specifies the means—electrical, mechanical, and so on—by which communication takes place over the physical media. At this level, X.25 covers standards such as RS-232, the ITU's V.24 specification for international connections, and the ITU's V.35 recommendation for high-speed modem signaling over multiple telephone circuits.
- At the next (data link) level, X.25 covers the link access protocol, known as LAPB (Link Access Protocol, Balanced), that defines how packets are framed. The LAPB ensures that two communicating devices can establish an error-free connection.
- At the highest level (in terms of X.25), the network layer, the X.25 protocol covers packet formats and the routing and multiplexing of transmissions between the communicating devices.

On an X.25 network, transmissions are typically broken into 128-byte packets. They can, however, be as small as 64 bytes or as large as 4096 bytes.

ATM

ATM is a connection-oriented networking technology, closely tied to the ITU's recommendation on *broadband ISDN (BISDN)* released in 1988. ATM is good for is high-speed LAN and WAN networking over a range of media types from the traditional coaxial cable, twisted pair, and fiberoptic to communications services of the future, including Fiber Channel, FDDI, and SONET

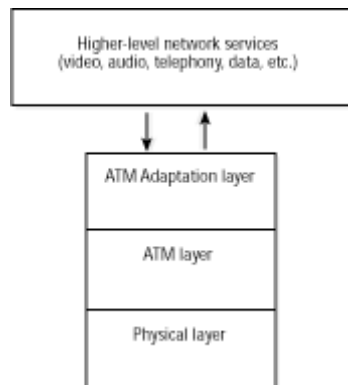
Cell relay ATM, like X.25 and frame relay, is based on packet switching. Unlike both X.25 and frame relay, however, ATM relies on cell relay, a high-speed transmission method based on fixed-size units (tiny ones only 53 bytes long) that are known as *cells* and that are multiplexed onto the carrier.



Because uniformly sized cells travel faster and can be routed faster than variable-length packets, they are one reason—though certainly not the only one—that ATM is so fast. Transmission speeds are commonly 56 Kbps to 1.544 Mbps, but the ITU has also defined ATM speeds as high as 622 Mbps (over fiberoptic cable).

ATM defines three layers

1. ATM adaptation layer (AAL)
2. ATM layer, roughly corresponding to the OSI data link layer
3. physical layer, equivalent to the OSI physical layer

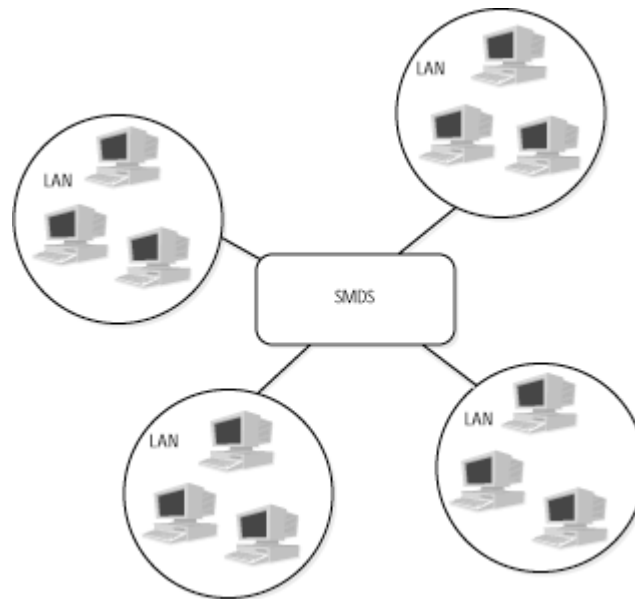


SMDS

SMDS, known as *Switched Multimegabit Data Service*. Switched Multimegabit Data Service (SMDS) is a high-speed, packet-switched, datagram-based WAN networking technology used for communication over public data networks (PDNs). SMDS can use fiber- or copper-based media; it supports speeds of 1.544 Mbps over Digital Signal level 1 (DS-1) transmission facilities, or 44.736 Mbps over Digital Signal level 3 (DS-3) transmission facilities. In addition, SMDS data units are large enough to encapsulate entire IEEE 802.3, IEEE 802.5, and Fiber Distributed Data Interface (FDDI) frames.

SMDS is a broadband public networking service offered by communications carriers as a means for businesses to connect LANs in separate locations. It is a connectionless, packet-switched technology designed to provide business with a less expensive means of linking networks than through the use of dedicated leased lines. Besides reducing cost, SMDS is notable for being well-suited to the type of "bursty" traffic characteristic of LAN (or LAN-to-

LAN) communications. In other words, it does the job when it's needed. Because SMDS is connectionless, it is available when and as needed, rather than being "on" at all times. It is also a fast technology, transmitting at speeds of 1 Mbps to (in the United States) 45 Mbps. The basis of an SMDS connection is a network address designed as a telephone number that includes country code and area code, as well as the local number. This address is assigned by the carrier and is used to connect LAN with LAN. A group address can also be used to broadcast information to a number of different LANs at the same time.



Users who need to transfer information to one or more LANs simply select the appropriate addresses in order to indicate where the information is to be delivered. SMDS takes it from there and makes a "best effort" to deliver the packets to their destinations. It does not check for errors in transmission, nor does it make an attempt at flow control. Those tasks are left to the communicating LANs.

The packets transferred through SMDS are simple, variable-length affairs containing the source and destination addresses and up to 9188 bytes of data. These packets are routed individually and can contain data in whatever form the sending LAN works with—Ethernet packet, Token Ring packet, and so on. SMDS essentially just passes the information from one place to the other and doesn't deal with the form or format of the data. In other words, SMDS acts somewhat like a courier service—it picks up and delivers but does not concern itself with the contents of its packages.

SMDS networks consist of several underlying devices to provide high-speed data service. These include CPE, carrier equipment, and the Subscriber Network Interface (SNI). CPE is terminal equipment typically owned and maintained by the customer. CPE includes end

devices, such as terminals and personal computers, and intermediate nodes, such as routers, modems, and multiplexers. Intermediate nodes, however, sometimes are provided by the SMDS carrier. Carrier equipment generally consists of high-speed WAN switches that must conform to certain network equipment specifications, these specifications define network operations, the interface between a local carrier network and a long-distance carrier network, and the interface between two switches inside a single carrier network. The SNI is the interface between CPE and carrier equipment. This interface is the point at which the customer network ends and the carrier network begins. The function of the SNI is to render the technology and operation of the carrier SMDS network transparent to the customer.

The SMDS Interface Protocol (SIP) is used for communications between CPE and SMDS carrier equipment.

SONET

SONET technology is a type of protocol which can transmit data at the speed of 150 Gbps by making the use of fiber links but has to be controlled by atomic clocks. The SONET here stands for Synchronous Optical Networking and is very beneficial for the networks which spans to many geographical regions because of the mechanism of atomic clock used in it. This is generally used only by mega corporations for data trafficking. *ONET*, or *Synchronous Optical Network*, is an ANSI standard for the transmission of different types of information—data, voice, video—over the optical (fiberoptic) cables widely used by long-distance carriers.

Designed to provide communications carriers with a standard interface for connecting optical networks, SONET was formulated by an organization known as the Exchange Carriers Standards Association (ECSA) and later incorporated into an ITU recommendation known as *Synchronous Digital Hierarchy*, or *SDH*.

Originally designed in the mid-1980s, SONET works at the physical layer and is concerned with the details related to framing, multiplexing, managing, and transmitting information synchronously over optical media. In essence, SONET specifies a standard means for multiplexing a number of slower signals onto a larger, faster one for transmission. In relation to this multiplexing capability, two signal definitions lie at the heart of the SONET standard:

- Optical carrier (OC) levels, which are used by fiberoptic media and which translate roughly to speed and carrying capacity
- Synchronous transfer signals (STS), which are the electrical equivalents of OC levels and are used by non-fiber media

SDH

SDH is one of the standards which are similar to the SONET technology. SDH transfers data making use of optical fibers along with LED or laser light. The capabilities and speed of the SDH technology are quite in comparison to SONET and is also controlled by atomic clocks. It was originally introduced by European Telecommunications and Standards Institute and SONET was defined by American National and Standards Institute. SDH also provides 50 Mbps bandwidth at STM - 0.

SONET and **SDH** are Multiplexing protocols used to transfer multiple digital bit streams, also called channels, over fiber-optic cables using either lasers or LED (light emitting diodes). Both can send multiple digital bit streams over copper wires at data rates slower than those possible with fiber optic. SONET and SDH are essentially the same; SONET used in the United States and Canada, rest of world uses SDH

T-LINES

Group of technologies that use digital multiplexing in telecommunications. They are distinctive from other telecommunications technologies because they are made up of a number of smaller channels, created by multiplexing. Multiplexing creates smaller channels; one media cable can carry multiple channels. Smaller channels, or sub-channels, are 64 kbps in bandwidth. T-Lines come in several different levels: –Fractional T-Lines, T1, T1C, T2, T3, T4, and T5. The most commonly used levels are T1, T3, and T5

DIAL- UP

Dial up is one of the oldest WAN network communication technologies available. Dial-up works by using a modem to connect a computer to a plain old telephone service (POTS). Methods to work around speed limitations:

- V.44 compression
- Server-side compression

ISDN

ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. It is a set of standards designed to carry voice, video, data, and other services in a digital format over the Packet Switched Telephone Networks(PSTN). It uses circuit switching to establish, maintain, and release connections. It also allows access to packet switched networks

The advantage of ISDN over dial-up is that it is able to integrate voice and data over the same lines. ISDN devices include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN is very unlikely for real life and there is almost no possibility that you will encounter it in use these days. ISDN has two important aspects i.e. ISDN BRI and ISDN PRI.

ISDN BRI has protocol of layer 2 which allows it to communicate between two channels and a controlling channel. The channel responsible for communication is bearer channel and for controlling is the delta channel. Each of these bearer channels can carry 64 Kbps data and delta channel can carry 16 Kbps for better data control. ISDN PRI came out way later and is very similar to a T1 line and contains 23 bearer channels and one delta channel both with speed of 64 Kbps.

ISDN BRI Service

An entry-level version of ISDN and is the most commonly used version of ISDN. The ISDN Basic Rate Interface (BRI) service offers two B channels and one D channel (2B+D). BRI B-channel service operates at 64 kbps and is meant to carry user data. It achieves upstream and downstream data rates by bonding to 64 kbps channels. B channels is known as bearer channels and one 16 kbps signaling channel is called a delta channel or a D channel.

BRI D-channel service operates at 16 kbps and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances. The D channel signaling protocol comprises Layers 1 through 3 of the OSI reference model. BRI also provides for framing control and other overhead, bringing its total bit rate to 192 kbps. The BRI physical layer specification is International Telecommunication Union-Telecommunications Standards Section (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430.

ISDN PRI Service

Similar to ISDN-BRI except it has more than two B channels bonded together. D channel for ISDN-PRI has a throughput of 64 kbps instead of 16 kbps. ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431. In the United States, ISDN-PRI commonly carried over a T-1 line of 1.544 mbps

DSL

Digital Subscriber Line (DSL) technology is a modem technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL uses the Packet Switched Telephone Networks (PSTN) and also uses a higher frequency than voice communications to carry data. The Phone systems that support DSL also need a special terminal adapter on the customer end

It is an inexpensive option for home users and small organizations which provides good bandwidth at cheaper rates. DSL stands for Digital Subscriber Line the most common form of this technique these days is Asymmetric DSL or ADSL. The line for such connection is already there in the form of telephone lines, so this connection is the cheaper way to access internet.

Asymmetric Digital Subscriber Line (ADSL)

- Provides a different data throughput for upstream communications than for downstream
- Depending on ADSL standard being used, downstream transmission rates can range from 1.5 mbps to 12.0 mbps
- Upstream transmission rates range from .5 mbps to 1.8 mbps

High-Bit-Rate Digital Subscriber Line (HDSL)

- Developed to use twisted-pair copper
- Can carry both voice and data
- Uses T-1 lines and is often used to interconnect local carriers
- When used to interconnect local carriers, repeaters are placed every 1.2 miles or so

Very-High-Bit-Rate Digital Subscriber Line (VDSL)

- Can provide very high data transfer rates
- Up to 52 mbps downstream rates and up to 16 mbps upstream
- VDSL standard first approved in 2001, updated and improved in 2006
- In the United States, AT&T, Verizon, and Qwest offer VDSL in some areas

WiMAX

It stands for Worldwide Interoperability to Microwave Access and is a telecommunication protocol which can be used for many applications like broadband connection and it can also allow you to use the network at a much greater distance than the traditional Wi-Fi. It is also cost-effective and can deliver speeds up to 40 Mbps. A wireless communications standard that uses microwaves. Most current version of WiMAX is IEEE 802.16m. It has data rates of up to 40 megabits per second on mobile platforms and –up to 1 gigabit per second on fixed platforms. Has a maximum fixed platform range of 30 miles and a maximum mobile platform range of 3 to 5 miles. LTE, Long Term Evolution, is a WiMAX alternative.

4.5 WAN devices

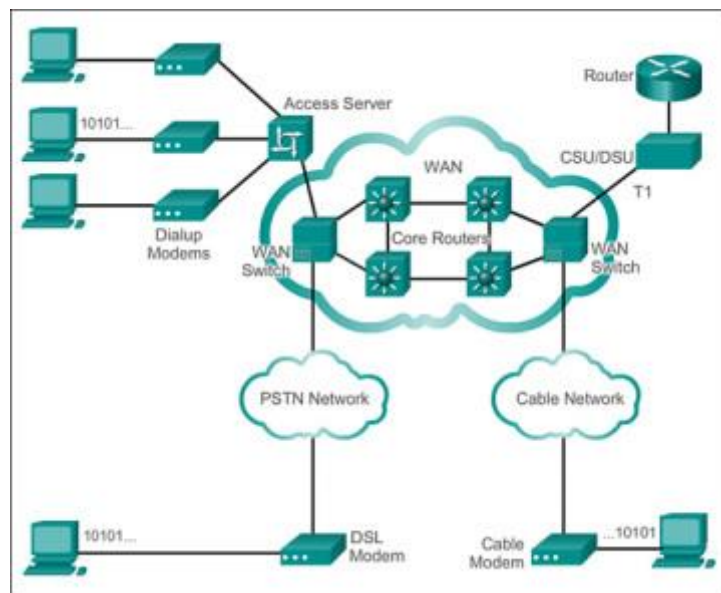


Figure 4.6: WAN devices

1. WAN Switch

A WAN switch is a multiport internetworking device used in carrier(service provider) networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS, and operate at the data link layer of the OSI reference model. Figure 4.7 illustrates two routers at remote ends of a WAN that are connected by WAN switches.

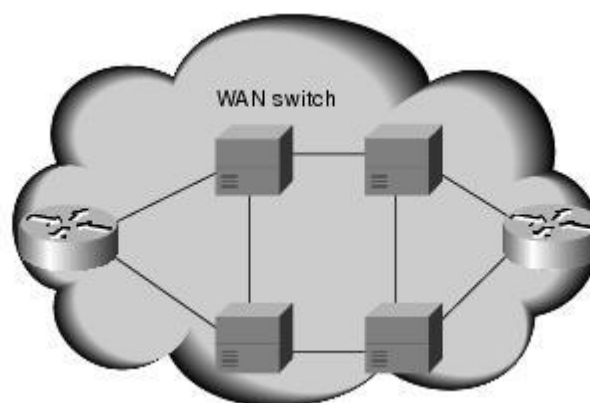


Figure 4.7: Two Routers at Remote Ends of a WAN Can Be Connected by WAN Switches

2. Access Server

Devices used to concentrate the dial-in and dial-out user communications of dialup modems. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users. It acts as a concentration point for dial-in and dial-out connections. Figure 4.8 illustrates an access server concentrating dial-out connections into a WAN.

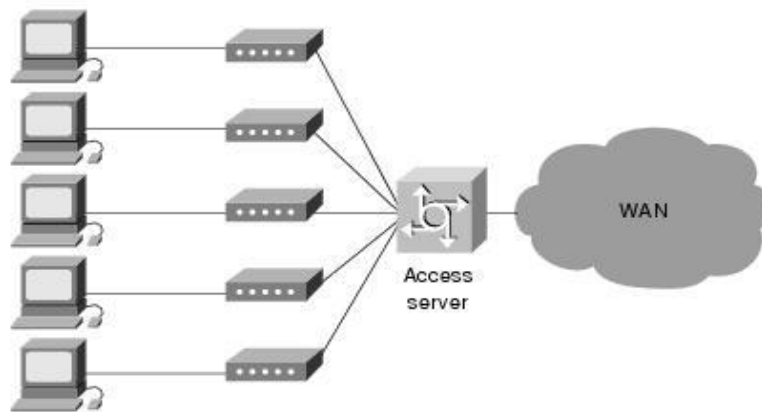


Figure 4.8: An Access Server Concentrates Dial-Out Connections into a WAN

3. Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. Figure 4.9 illustrates a simple modem-to-modem connection through a WAN.



Figure 4.9: A Modem Connection Through a WAN Handles Analog and Digital Signals

- **Dialup modem:** Considered to be a legacy WAN technology, a voiceband modem converts (i.e., modulates) the digital signals produced by a computer into voice frequencies that can be transmitted over the analog lines of the public telephone

network. On the other side of the connection, another modem converts the sounds back into a digital signal (i.e., demodulates) for input to a computer or network connection.

- **Broadband modem:** A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds.

4. CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Digital leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa. Figure 4.10 illustrates the placement of the CSU/DSU in a WAN implementation.

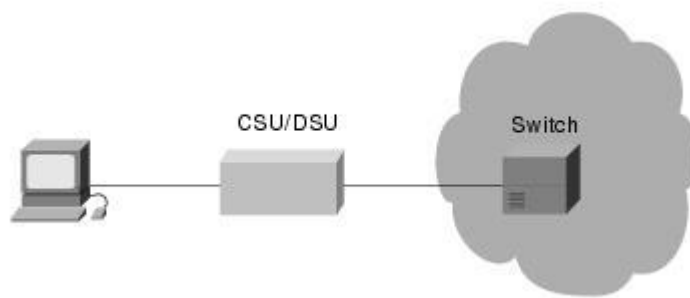


Figure 4.10: The CSU/DSU Stands Between the Switch and the Terminal

5. ISDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem, although it is called a terminal adapter because it does not actually convert analog to digital signals. Figure 4.11 illustrates the placement of the terminal adapter in an ISDN environment.

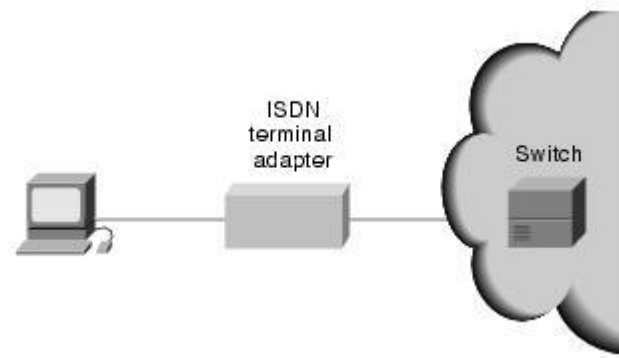


Figure 4.11: The Terminal Adapter Connects the ISDN Terminal Adapter to Other Interfaces

6. Router

This is a Customer Premises Equipment (CPE) device that provides internetworking and WAN access interface ports used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or (Digital Subscriber Line (DSL), is required to connect the router to the local service provider.

7. Core router/multilayer switch

These are the routers and multilayer switches that reside within the service provider WAN backbone. To fulfill this role, the devices must be able to support routing protocols being used in the core and multiple high speed interfaces used in the WAN core backbone. They must also be able to forward IP packets at full speed on all of those interfaces. Key core routers interconnect to other provider core routers.

5. WIRELESS LOCAL AREA NETWORK (WLAN) (IEEE 802.11)

- Wireless LAN (WLAN) - provides all the features and benefits of traditional LAN technologies such as Ethernet, but without the limitations of wires or cables.
- Provides network connectivity over wireless media
- An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network
- The AP is connected to wired network and is equipped with antennae to provide wireless connectivity
- Range (Distance between Access Point and WLAN client) depends on structural hindrances and RF gain of the antenna at the Access Point
- To service larger areas, multiple APs may be installed with a 20-30% overlap
- A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off)
- The three most commonly used are 802.11a, 802.11b and 802.11g.
 - 802.11a - Provides up to 54 Mbps transmission in the 5GHz band
 - 802.11b - Provides up to 11 Mbps transmission in the 2.4 GHz band.
 - 802.11g - Provides up to 54 Mbps transmission in the 2.4 GHz band.
- WLANs use the 2.4 GHz and 5-GHz frequency bands.
- IEEE 802.11 networks work on license free industrial, science, medicine (ISM) license-free (unlicensed) frequency bands.
- ISM (Industry, Scientific, Medical) S-Band ISM
 - 802.11b and 802.11g: 2.4- 2.5 GHz
- C-Band ISM
 - 802.11a: 5.725 – 5.875 GHz

5.1 IEEE 802.11 Operating Modes

IEEE 802.11 defines the following operating modes:

- Ad hoc mode
- Infrastructure mode

Ad Hoc Mode

In ad hoc mode, wireless clients communicate directly with each other without the use of a wireless AP or a wired network, as shown in Figure 5.1.



Figure 5.1: Ad hoc mode

Ad hoc mode is also called peer-to-peer mode. Wireless clients in ad hoc mode form an Independent Basic Service Set (IBSS), which is two or more wireless clients who communicate directly without the use of a wireless AP.

Ad hoc mode is used to connect wireless clients together when there is no wireless AP present, when the wireless AP rejects an association due to failed authentication, or when the wireless client is explicitly configured to use ad hoc mode.

Infrastructure Mode

In infrastructure mode, there is at least one wireless AP and one wireless client. The wireless client uses the wireless AP to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless AP.

A single wireless AP supporting one or multiple wireless clients is known as a Basic Service Set (BSS). A set of two or more wireless APs connected to the same wired network is known as an Extended Service Set (ESS). An ESS is a single logical network segment (also known as a subnet), and is identified by its SSID. An ESS is shown in Figure 5.2.

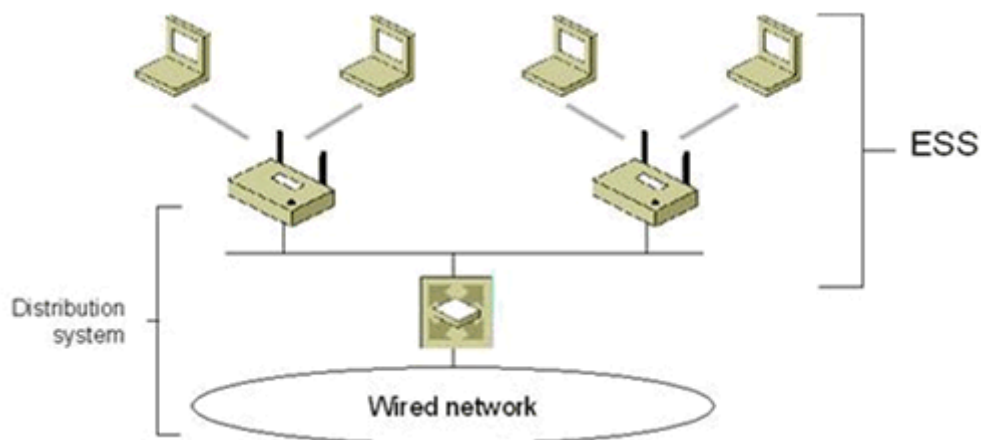


Figure 5.2: Infrastructure mode and an ESS

5.2 WLAN Technologies (Standards)

1. IEEE 802.11a

- Operates at 5 GHz band
- IEEE 802.11a operates at a data transmission rate as high as 54 Mbps and uses the C-Band ISM.
- Supports multi-rate 6 Mbps, 9 Mbps, 12Mbps, 18Mbps... up to 54 Mbps
- Use Orthogonal Frequency Division Multiplexing (OFDM) with 52 subcarriers, 4 us symbols (0.8 us guard interval). OFDM allows data to be transmitted by subfrequencies in parallel. This provides greater resistance to interference and greater throughput. This higher speed technology allows wireless LAN networking to perform better for video and conferencing applications.
- Use Inverse Discrete Fourier Transform (IFFT) to combine multi-carrier signals to single time domain symbol

2. 802.11b

- The major enhancement to IEEE 802.11 by IEEE 802.11b is the standardization of the Physical layer to support higher bit rates.
- IEEE 802.11b supports two additional speeds, 5.5 Mbps and 11 Mbps, using the S-Band ISM.
- IEEE 802.11b uses the Direct Sequence Spread Spectrum (DSSS) transmission scheme to provide the higher data rates.
- The bit rate of 11 Mbps is achievable in ideal conditions.
- In less-than-ideal conditions, 802.11b uses the slower speeds of 5.5 Mbps, 2 Mbps, and 1 Mbps.

3. 802.11g

- IEEE 802.11g, is a relatively new standard, operates at a bit rate up to 54 Mbps
- Uses the S-Band ISM and OFDM.
- 802.11g is also backward compatible with 802.11b and can operate at the 802.11b bit rates and use the DSSS transmission scheme.
- 802.11g wireless network adapters can connect to an 802.11b wireless AP, and 802.11b wireless network adapters can connect to an 802.11g wireless AP.
- 802.11g provides a migration path for 802.11b networks to a frequency-compatible standard technology with a higher bit rate.

- Existing 802.11b wireless network adapters cannot be upgraded to 802.11g by updating the firmware of the adapter and must be replaced.
- Unlike migrating from 802.11b to 802.11a (in which all the network adapters in both the wireless clients and the wireless APs must be replaced at the same time), migrating from 802.11b to 802.11g can be done incrementally.
- Like 802.11a, 802.11g uses 54 Mbps in ideal conditions and the slower speeds of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps in less-than-ideal conditions.

4. HiperLAN

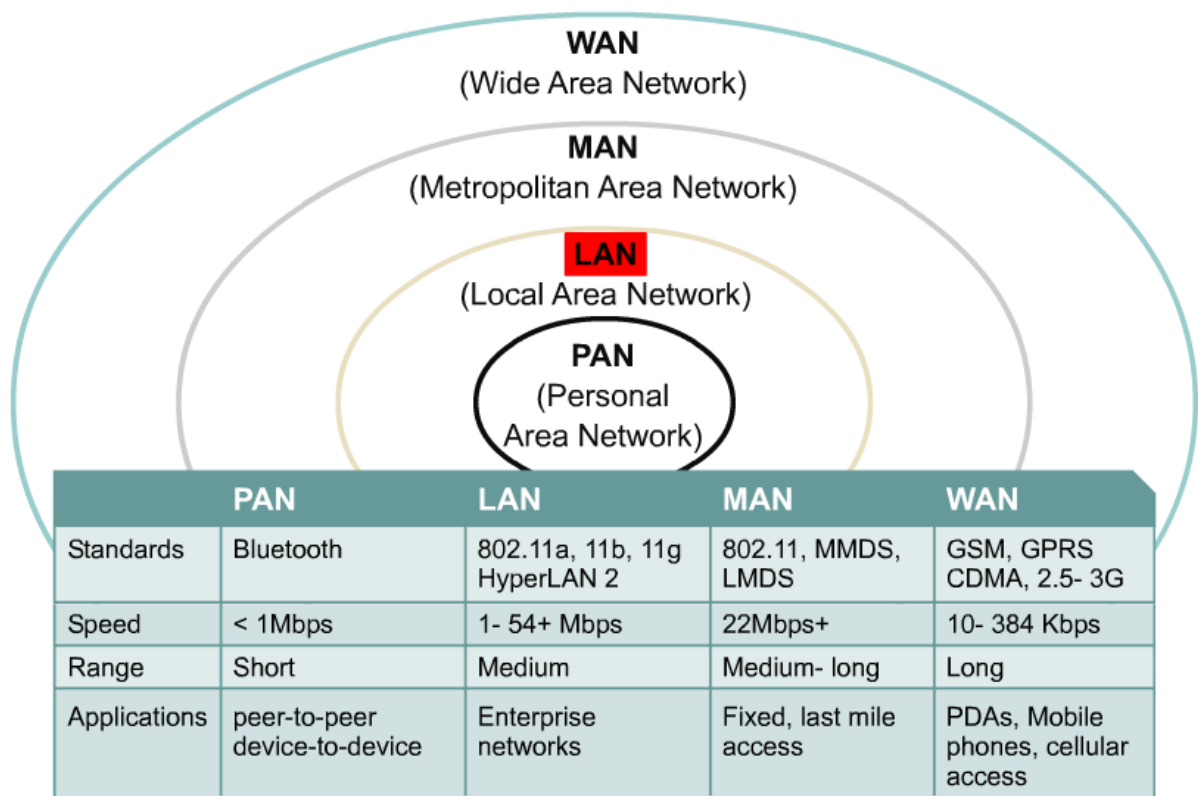
- High performance LAN or HiperLAN (ETSI-BRAN EN 300 652) in the 5 GHz ISM
 - version 1 up to 24 Mbps
 - version 2 up to 54 Mbps
- HiperLAN provides also QoS for data, video, voice and images

5. Bluetooth

- Range up to 100 meters only (*cable replacement tech.*).
- Operates at max of 740 kbps at 2.4 GHz ISM band.
- Applies fast frequency hopping 1600 hops/second.
- Can have serious interference with 802.11
- 2.4 GHz range network.

Others include

- Cellular
- 3G (3rd Generation)
- UWB (Ultra Wide Band)
- FSO (Free Space Optics)
- Radio waves off meteor trails.



5.3 WLAN Transmission Media

There are different ways by which WLANs transmit information. It includes

1. Infrared transmission
2. Spread-spectrum transmission
3. Radio waves transmission
4. Microwaves
5. Communication Satellite

1. Infrared Transmission

Infrared (IR) is a wireless transmission media that sends signals using infrared light waves. This method uses infrared light to carry information. IR transmission also require a line of sight transmission as that required by microwaves. Computer devices such as a mouse, printer and digital camera, which have an IrDA port may transfer data from one device to another using infrared light waves. IR is an alternative to short-range radio communications such as Bluetooth

- 850-950 nm, diffuse light (to allow point-to-multipoint communication).
- 10 m maximum range with no sunlight or heat interfere.

There are three types of infrared transmission: diffused, directed and directed point-to-point.

- **Diffused**

The infrared light transmitted by the sender unit fills the area (e.g. office). Therefore the receiver unit located anywhere in that area can receive the signal.

- **Directed**

The infrared light is focused before transmitting the signal. This method increases the transmission speed.

- **Directed point-to-point**

Directed point-to-point infrared transmission provides the highest transmission speed. Here the receiver is aligned with the sender unit. The infrared light is then transmitted directly to the receiver.

The light source used in infrared transmission depends on the environment. Light emitting diode (LED) is used in indoor areas, while lasers are used in outdoor areas. Infrared radiation (IR) has major biological effects. It greatly affects the eyes and skin. Microwave signals are also dangerous to health. But with proper design of systems, these effects are reduced considerably.

2. Spread Spectrum Transmission

- Widely used technology. Developed by the military.
- More bandwidth consumed than narrowband.
- Produces a louder signal.
- Reliability, integrity and security.

With this transmission technology, there are two methods used by wireless LAN products: frequency hopping and direct sequence modulation.

- **Frequency Hopping**

The signal jumps from one frequency to another within a given frequency range. The transmitter device "listens" to a channel, if it detects an idle time (i.e. no signal is transmitted), it transmits the data using the full channel bandwidth. If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner. It uses narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.

- **Direct Sequence Modulation**

This method uses a wide frequency band together with Code Division Multiple Access (CDMA). Signals from different units are transmitted at a given frequency range. The power levels of these signals are very low (just above background noise). A code is transmitted with each signal so that the receiver can identify the appropriate signal

transmitted by the sender unit. It generates redundant bit pattern for each bit to be transmitted known as a chip. The longer the chip the greater the probability original data can be recovered.

The frequency at which such signals are transmitted is called the ISM (industrial, scientific and medical) band. This frequency band is reserved for ISM devices. The ISM band has three frequency ranges: 902-928, 2400-2483.5 and 5725-5850 MHz. An exception to this is Motorola's ALTAIR which operates at 18GHz. Spread spectrum transmission technology is used by many wireless LAN manufacturers such as NCR for waveLAN product and SpectraLink for the 2000 PCS.

3. Radio waves

Radio waves frequency are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors. Radio waves also are Omni-directional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically. Typically using the license free ISM band at 2.4 GHz

- **Advantages**
 - experience from wireless WAN and mobile phones can be used
 - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- **Disadvantages**
 - very limited license free frequency bands
 - shielding more difficult, interference with other electrical devices

Examples: WaveLAN, HIPERLAN, Bluetooth

4. Microwaves

These are radio waves that provide a high-speed signal transmission; from one microwave station to another; which are normally located on the top of buildings, towers or mountain to avoid possible obstructions. Microwaves transmission is fast (up to 4,500 times faster than a dial-up modem but is limited to line-of-sight transmission, which means that the microwaves must transmit in a straight line with no obstructions between microwave antennas. This transmission is used where installing physical transmission media is difficult or impossible (e.g. deserts, lakes or to communicate with a satellite) but light –of- sight transmission is available.

Motorola's WLAN product (ALTAIR) transmits data by using low powered microwave radio signals. It operates at the 18GHz frequency band.

5. Communication Satellite

This is a space station that receives microwave signals from an earth-based station, amplifies the signals, and broadcasts the signal back over a wide area to any number of earth-based station. A transmission from the earth to a satellite is called an **uplink**; a transmission from a satellite to an earth station is called a **downlink**. Communication satellites are used in application such as air navigation, television and radio broadcast, videoconferencing and paging. Communication satellites are usually placed about 22,300 miles above the earth's equator and moves at the same rate as the earth.

Applications of communication satellite include television and radio broadcasts, videoconferencing, paging and global positioning systems.

Advantages of satellites

- Lots of data can be sent simultaneously.
- Allow high quality broadband communication across continents.

Disadvantages of satellites

- The fee to launch a satellite is extremely expensively.
- The infrastructure needed to access satellite communications is also expensive.