

Module 6

Network Concepts

6. OBJECTIVES

Students will be able to:

- Define the concept of networking
- Describe the characteristics of Local Area Networks (LANs)
- Summarize the differences between client/server and peer-to-peer networks
- List the criteria to consider when selecting adapters
- List the three types of hubs
- Explain the differences between bus, star, and ring networking topologies
- Describe different types of cables used in setting up a network
- List the seven layers of the Open Systems Interconnection (OSI) model

6.1 OVERVIEW

In our lives, networking has become woven into almost everything we do. With a good understanding of the concepts that make up networking, we can choose networking products for what they will let you do (without becoming an engineer) and understand how they complete their task. Networking terminology equates functions with engineering and, as such, it can represent an obstacle when you set out to consider a network. Even if you are familiar with general PC terminology, you will find some network-specific terms unfamiliar. Here, we want to give you an understanding of these network components and terminology.

6.2 NETWORK CONCEPTS

Networking is the concept of sharing resources and services. A network of computers is a group of interconnected systems sharing resources, and interacting using a shared communications link (See Figure 6-1). A network, therefore, is a set of interconnected systems with something to share. The shared resource can be data, a printer, a fax modem, or a service such as a database or an e-mail system. The individual systems must be connected through a pathway (called the transmission medium) that is used to transmit the resource or service between the computers. All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called protocols.

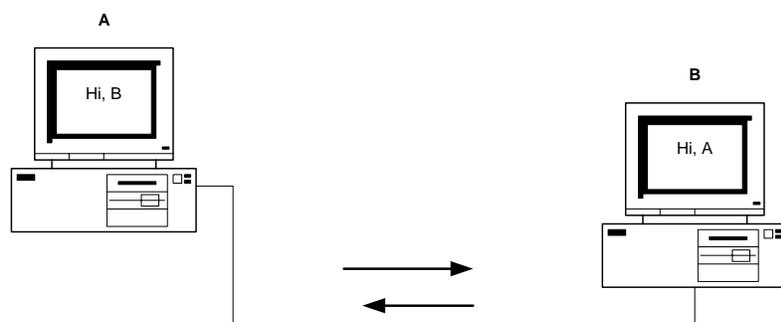


Figure 6-1. Simple Computer Network

Having a transmission pathway does not always guarantee communication. When two entities communicate, they do not merely exchange information; rather, they must understand the information

they receive from each other. The goal of computer networking therefore, is not simply to exchange data, but to understand and use data received from other entities on the network.

An analogy is people speaking. Just because two people can speak, it does not mean they automatically can understand each other. These two people might speak different languages or interpret words differently. One person might use sign language, while the other uses spoken language. As in human communication, even though you have two entities that “speak” there is not guarantee they will be able to understand each other. Just because two computers are sharing resources, it does not necessarily mean they can communicate.

Because computers can be used in different ways and can be located at different distances from each other, enabling computers to communicate often can be a daunting task that draws on a wide variety of technologies.

6.2.1 LOCAL AND WIDE AREA NETWORKS

6.2.1.1 LOCAL AREA NETWORKS (LANS)

A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or a campus. LANs are characterized by the following:

- They transfer data at high speeds (higher bandwidths).
- They exist in a limited geographical area.
- Connectivity and resources, especially the transmission media, usually are managed by the company running the LAN.

6.2.1.2 WIDE AREA NETWORKS (WANS)

A wide area network (WAN) interconnects LANs. A WAN can be located entirely within a state or country, or it can be interconnected around the world. WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They usually interconnect multiple LANs.
- They often transfer data at lower speeds (lower bandwidth).
- Connectivity and resources, especially the transmission media, usually are managed by a third-party carrier such as a telephone or cable company

WANs can be further classified into two categories: enterprise WANs and global WANs. An enterprise WAN connects the widely separated computer resources of a single organization. An organization with computer operations at several distant sites can employ an enterprise WAN to interconnect the sites. An enterprise WAN can combine private and commercial network services, but it is dedicated to the needs of a particular organization. A global WAN interconnects networks of several corporations or organizations. Other terms that describe networks include municipal area network (MAN) – a connected network that spans the geographic boundaries of a municipality – and a campus area network (CAN) – a network that spans a campus or a set of buildings. These terms often lead to confusion because people are not sure whether they refer to the company's own network of computers or its connection to the outside world.

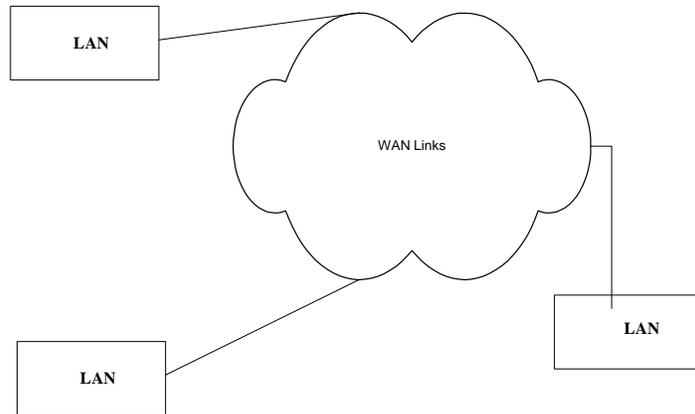


Figure 6-2. The WAN or the link up of LAN's is often shown as a cloud

6.2.2 NETWORK MODELS

6.2.2.1 CLIENT/SERVER NETWORKS

A client/server network consists of a group of user-oriented PCs (called clients) that issue requests to a server (Figure 6-3). The client PC is responsible for issuing requests for services to be rendered. The server's function on the network is to service these requests. Servers generally are higher-performance systems that are optimized to provide network services to other PCs. The server machine often has a faster CPU, more memory, and more disk space than a typical client machine.

Some examples of client/server-based networks are Novell NetWare, Windows NT Server, and Banyan Vines. Some common server types include file servers, print servers, fax servers and application servers. In a client/server network, the server machines are not even set up to do the tasks that a client machine can do. On a Novell or Banyan server, for example, a person cannot run a spreadsheet from the server console. Other systems, such as Windows NT and UNIX machines, enable a person to do this even though it is not the intended use of the system.

An example of a client/server system is Microsoft Exchange Server. Your PC is responsible for constructing and displaying e-mail messages, to name a couple of the possible tasks. The Exchange Server is responsible for delivering outgoing email and for receiving email intended for you.

6.2.2.2 PEER-TO-PEER NETWORKS

A peer-to-peer network consists of a group of PCs that operate as equals (Figure 6-4). Each PC is called a peer. The peers share resources (such as files and printers) just like in a server-based network, although

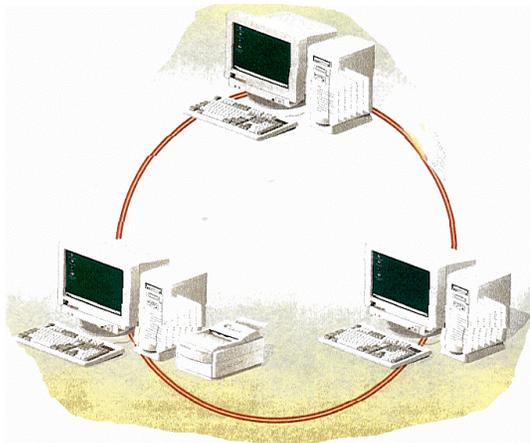


Figure 6-4. Peer to Peer Network

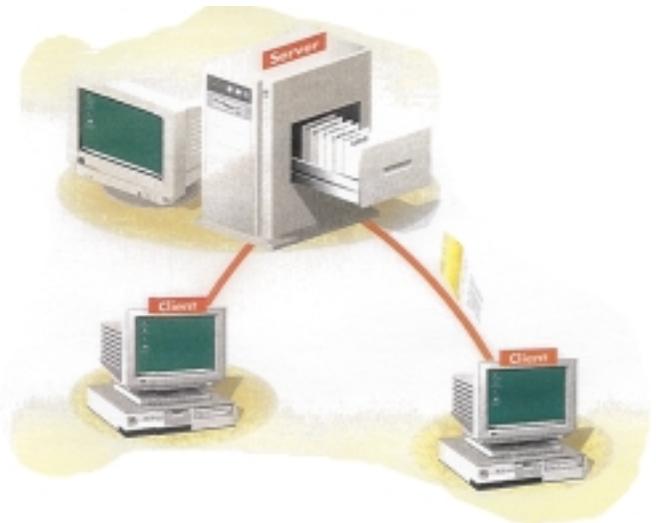


Figure 6-3. Client/Server Network

no specialized or dedicated server machines exist. In short, each PC can act as a client or a server. No one machine is set up with a higher powered set of devices, nor is any one PC set up simply to provide one service, such as storing files. Small networks – usually with fewer than 10 machines – can work well in this configuration. Examples of peer-to-peer networks include Windows for Workgroups, Windows 95, Windows 98, Windows NT Workstation, and Windows 2000.

6.3 SOFTWARE TO OPERATE A NETWORK

Each computer on the network requires several networking software components. Some are always required; others are required if you need certain functionality, such as file and printer sharing, or dial-up networking capability. Two software components required in all cases are protocols and network adapter drivers.

6.3.1 REQUIRED SOFTWARE COMPONENTS

You need protocol software and a network adapter driver, however, for whatever kind of network you want to build or use.

6.3.2 PROTOCOLS

Protocols are the communication language. They are sets of rules for sending information over a network. These rules govern the context, format, timing, sequencing, and error control of the data as it

crosses the network. Computers use protocols to communicate - to request and send data. Just as a person can be multilingual, a computer can run several protocols at once. Regardless of how many languages two people know, however, they must have at least one language in common to talk with each other. Two computers must have at least one protocol in common to communicate.

Protocols are optimized to suit specific communication needs. Microsoft supplies several protocols for its operating systems, including TCP/IP, NetBEUI, DLC, AppleTalk, and the combination of NWLink (Microsoft's version of Novell's IPX protocol) and NWNBLink. The characteristics, advantages, and disadvantages of these protocols will depend on your use of it.

6.3.3 NETWORK ADAPTER DRIVERS

The network adapter drivers coordinate communications between the network card and the computer's hardware and other software. A network adapter connects a PC to the rest of the network, and the PC needs a network adapter driver to control it. There are hundreds of network adapter makes and models, which offer a variety of features and prices.

Drivers are often specific to a make and model of adapter, and a driver written for one operating system rarely runs on others. Consequently, driver availability affects your choice of adapters. You will find that an adapter may work fine with one operating system while being incompatible with another. Each of the Windows networking operating systems supplies drivers for hundreds of the most popular network adapters and modems, and Microsoft makes new drivers available as soon as they are developed and tested. Oftentimes, hardware vendors supply drivers for their new products. It is worth the effort to periodically check the manufacturer's web site for updated drivers.

If you use Dial-Up Networking or Remote Access, your modem is, in effect, your network adapter. The file that details the modem's capabilities is, in effect, your network adapter driver.

6.3.4 REMOTE ACCESS

You can link computers over telephone lines, effectively extending your office network. This action (called Dial-Up Networking in Windows 95, Windows NT Workstation and Server) primarily provides the capability to dial into servers. Remote Access service in Windows NT Workstation and Server provides the service to accept those calls. These features require special software, which is most easily discussed in terms of a client computer that dials into a server computer.

If the client computer runs Windows 95, Windows 98, Windows NT Server, Windows NT Workstation, or Windows for Workgroups, the client software is on the operating system's setup diskettes or CD-ROM. Most of this server software allows one dial-in connection at a time, and gives the client computer access to files and printers shared by the server computer. The Windows NT Server software can accept up to 256 clients' calls at a time, and clients can access resources on the server and anywhere on the server's LAN. An entire deployment team, for instance, has the same access to files and printers dialing in from a laptop that they have when they are in the office using a desktop computer.

6.4 HARDWARE

Each computer on the network requires additional hardware in the form of a network adapter and cabling. Depending on the type of network you choose, you may need other hardware to join the cables (hubs or switches) in a LAN, or to join several LANs (routers) into a WAN.

6.4.1 NETWORK ADAPTER

As mentioned above, each computer on the network needs its own network adapter. Consider the following criteria when selecting adapters:

- **Is a driver available for this adapter and for your operating system?**
Different models in a hardware vendor's model line can vary widely, yet have very similar names. Verify that a driver exists for the exact make and model. Also, drivers written for one operating system are rarely usable by other operating systems: support for one operating system does not imply support for other operating systems. The best way to verify support is to look for the exact make and model on the operating system's Hardware Compatibility List. The network adapter manufacturer will also have this information.
- **Will the adapter plug into your computer?**
This is an obvious consideration, but a crucial one. A network adapter plugs into a "slot" in the PC. There are several different standards for these slots. Each PC typically supports only one or two of those standards, so you need to know what kinds of slots are available in your computers before you buy network adapters. The network adapter's name often includes the name of the slot for which it is designed (such as ISA, EISA, PCI, VESA Local Bus (VLB)), Microchannel (abbreviated MC or MCA), PCMCIA, or PC Card. Consult your PC documentation to see which slots are supported.
- **Can the adapter plug into your cabling?**
There are several different kinds of networks, and each has a different standard for cabling and connectors. Network adapters usually support only one or two of these standards. A network adapter's name often includes hints about the type of cabling that the adapter supports. Ethernet adapters often include "Ether" in their name. Thin Ethernet adapters may identify themselves with "BNC," "Co-ax," or "Coaxial." Thick Ethernet adapters may include "AUI" or "DIX." Twisted pair Ethernet adapters may have "T," "TP," "UTP," "STP," or "RJ-45" in their names.

6.4.2 HUBS

When connecting networks, there must be a way to “bring” the cables together. In the case of a bus topology network, this is done in a line. However, in other types of topologies, we use something called a Hub. A Hub, also called wiring concentrators, provide a central attachment point for network cabling.

Hubs come in three types:

- **Passive** – These hubs do not contain any electronic components and do not process the data signal in any way. The only purpose of a passive hub is to combine the signals from several network cable segments. All devices attached to a passive hub receive all the packets that pass through the hub.

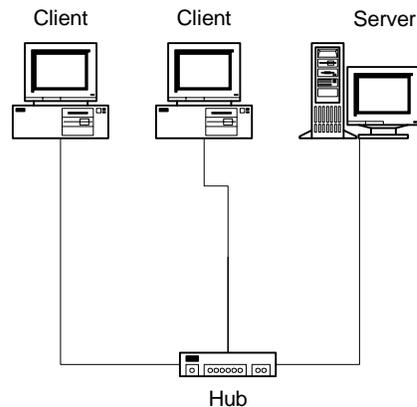


Figure 6-5. All Systems Plug into Hub



Figure 6-6. Ethernet Hub

- **Active** – Active hubs incorporate electronic components that can amplify and clean up the electronic signals that flow between devices on the network. This process of cleaning up the signals is called signal regeneration.
- **Intelligent** – Intelligent hubs are enhanced active hubs. They offer the capability to do hub management and possibly switching.

6.5 NETWORK TOPOLOGIES

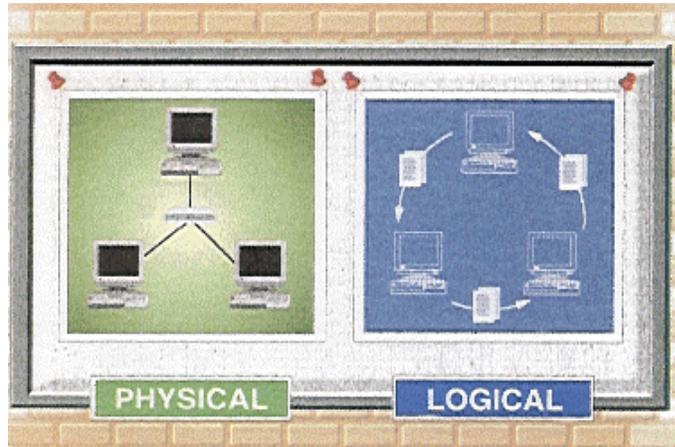
A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. Two categories form the basis for all discussions of topologies:

- **Physical topology.** Describes the actual layout of the network transmission media.
- **Logical topology.** Describes the logical pathway a sign follows as it passes among the network nodes.

Another way to think about this distinction is that a physical topology defines the way the network looks, and a logical topology defines the way the data passes among the node. Topologies can be mixed. For example, a network with a star physical topology, may actually have a bus or a ring logical topology.

Physical and logical topologies can take several forms. The most common and the most important for understanding the Ethernet and token-ring topologies are the following:

- Bus topologies
- Ring topologies
- Star topologies



6.5.1 BUS TOPOLOGIES

A bus physical topology is one in which all devices connect to a common, shared cable (sometimes called the backbone). Ethernet typically uses bus as a physical topology. Even 10 BASE-T Ethernet networks use the bus as a logical topology but are configured in a star physical topology.

Most bus networks broadcast signals in both directions on the backbone cable, enabling all devices to directly receive the signal. Some buses, however, are unidirectional: Signals travel in only one direction and can reach only downstream devices. A special connector called a terminator must be placed at the end of the backbone cable to prevent signals from reflecting back on the cable and causing interference. In the case of a unidirectional bus, the cable must be terminated in such a way that signals can go down the cable but do not reflect back up the cable and reach other devices, causing disruption.

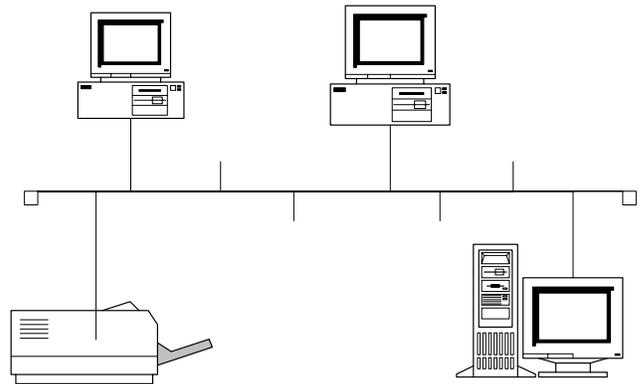


Figure 6-8. Bus Physical Topology

6.5.2 STAR TOPOLOGIES

Star topologies require that all devices connect to a central hub. The hub receives signals from other network devices and routes the signals to the proper destinations. Star hubs can be interconnected for a tree, or hierarchical, network topologies. A star physical topology is often used to implement a bus or ring logical topology. The path the data takes among the nodes and through the hub, depends on the design of the hub, the design of the cabling, and the hardware and software configuration of the nodes.

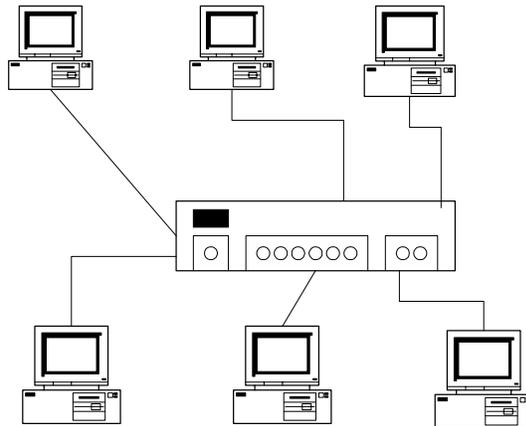


Figure 6-9. Star Physical Topology

6.5.3 RING TOPOLOGIES

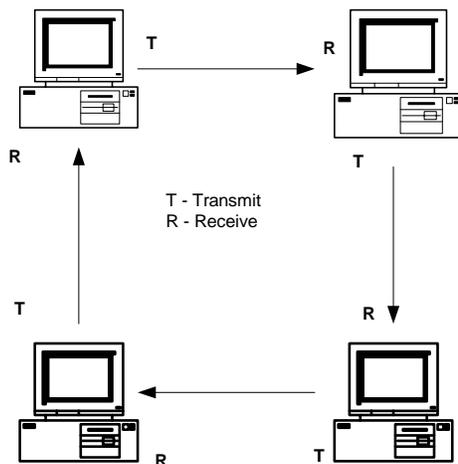


Figure 6-10. Ring Physical Topology

Ring Topologies are wired in a circle. Each node is connected to its neighbors on either side, and data passes around the ring in direction only. Each device incorporates a receiver and a transmitter and serves as a repeater that passes the signal on to the next device in the ring. Because the signal is regenerated at each device, signal degeneration is low.

Ring topologies are ideally suited for token passing access methods. The token passes around the ring, and only the node that holds the token can transmit data.

Ring physical topologies are quite rare. The ring topology is almost always implemented as a logical topology. Token ring, for example, the most widespread token-passing network, always arranges nodes a physical star (with all nodes connecting to a central but passes data in a logical ring).

6.6 NETWORK ARCHITECTURE

A network architecture is the design specifications of the physical layout of connected devices. This includes the cable being used (or wireless media being deployed), the types of network cards being deployed, and the mechanism through which data is sent on the network and passed to each device. Network architecture, in short, encompasses the total design and layout of the network.

We will discuss different network architectures here and later in this module we will cover the different types of cabling to implement some of these architectures.

6.6.1 ETHERNET

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The different varieties of Ethernet networks are commonly referred to as Ethernet topologies. Typically Ethernet networks can use a bushy physical topology, although, many varieties of Ethernet such as 10BASE-T use a star physical topology and bus logical topology.

Note that the name each Ethernet topology begins with a number (10 or 100). That number specifies the transmission speed for the network. For instance, 10BASE5 is designed to operate at 10Mbps, and 100BASE-X operates at 100Mbps. “BASE” specifies that baseband transmissions are being used. The “T” is for unshielded twisted-pair wiring, “FL” is for fiber optic cable, “VG-ANYLAN” implies Voice Grade, and “X” implies multiple media types.

Some of the different Ethernet topologies include:

6.6.1.1 10BASE2

The 10BASE2 cabling topology (Thinnet) generally uses the on-board transceiver of the network interface card to translate the signals to and from the rest of the network. Thinnet cabling uses BNC T-connectors that directly attach to the network adapter. Each end of the cable should have a terminator, and you must use a grounded terminator on one end.

The main advantage of using 10BASE2 in your network is cost. When any given cable segment on the network doesn't have to be run further than 185 meters (607 feet), 10BASE2 is often the cheapest network cabling option. 10BASE2 is also relatively simple to connect. Each network node connects directly to the network cable by using a T-connector attached to the network adapter. For a successful installation, you must adhere to several rules in 10BASE2 Ethernet environments, including the following:

- The minimum cable distance between clients must be 0.5 meters (1.5 feet).
- *Pig tails*, also known as *drop cables*, from T-connectors shouldn't be used to connect to the BNC connector on the network adapter. The T-connector must be connected directly to the network adapter. You may not exceed the maximum network segment limitation of 185 meters (607 feet).
- The entire network cabling scheme cannot exceed 925 meters (3,035 feet).
- The maximum number of nodes per network segment is 30 (this includes clients and repeaters).

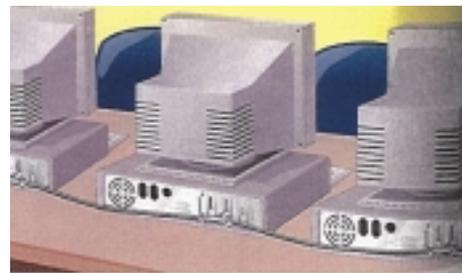


Figure 6-11. 10 Base2 Network Connections

- A 50-ohm terminator must be used on each end of the bus with only one of the terminators having either a grounding strap or a grounding wire that attaches it to the screw holding an electrical outlet cover in place.
- You may not have more than five segments on a network. These segments may be connected with a maximum of four repeaters, and only three of the five segments may have network nodes.

6.6.1.2 10BASE5

The 10BASE5 cabling topology (Thicknet) uses an external transceiver to attach to the network adapter card (see figure. 6.12). The external transceiver clamps to the Thicknet cable an Attachment Universal Interface (AUI) cable runs from the transceiver to a DIX connector on the back of the network adapter card. As with Thinnnet, each network segment must be terminated at both ends, with one end using a grounded terminator.

The primary advantage of 10BASE5 is its capability to exceed the cable restrictions that apply to 10BASE2. 10BASE5 does pose restrictions of its own, however, which you should consider when installing or troubleshooting a 10BASE5 network. As with 10BASE2 networks, the first consideration when troubleshooting a 10BASE5 network should be the established cabling rules and guidelines. You must follow several additional guidelines, along with the 5-4-3 rule, when configuring Thicknet networks, such as the following:

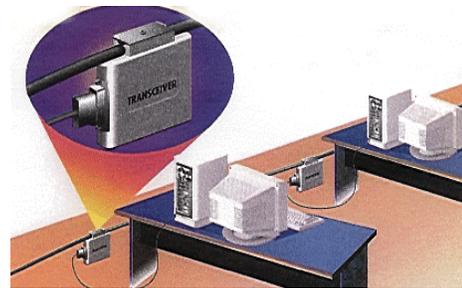


Figure 6-12. 10 Base5 Network Connections

- The minimum cable distance between transceivers is 2.5 meters (8 feet).
- You may not go beyond the maximum network segment length of 500 meters (1,640 feet).
- The entire network cabling scheme cannot exceed 2,500 meters (8,200 feet).
- One end of the terminated network segment must be grounded.
- Drop cables (transceiver cables) can be as short as required but cannot be longer than 50 meters from transceiver to computer.
- The maximum number of nodes per network segment is 100. (This includes all repeaters.)

The length of the drop cables (from the transceiver to the computer) is not included in measurements of the network segment length and total network length. Figure 6-12 shows two segments using Thicknet and the appropriate hardware.

6.6.1.3 10BASE-T

The trend in wiring Ethernet networks is to use unshielded twisted-pair (UTP) cable. 10BASE-T, which uses UTP cable, is one of the most popular implementations for Ethernet. It is based on the IEEE 802.3 standard. 10BASE-T supports a data rate of 10 Mbps using baseband.

10BASE-T cabling is wired in a star topology. The nodes are wired to a central hub, which serves as a multiport repeater. A 10BASE-T network functions logically as a linear bus. The hub repeats the signal to all nodes, and the nodes contend for access to the transmission medium as if they were connected along a linear bus. The cable uses RJ-45 connectors, and the network adapter card can have RJ-45 jacks built into the back of the card.

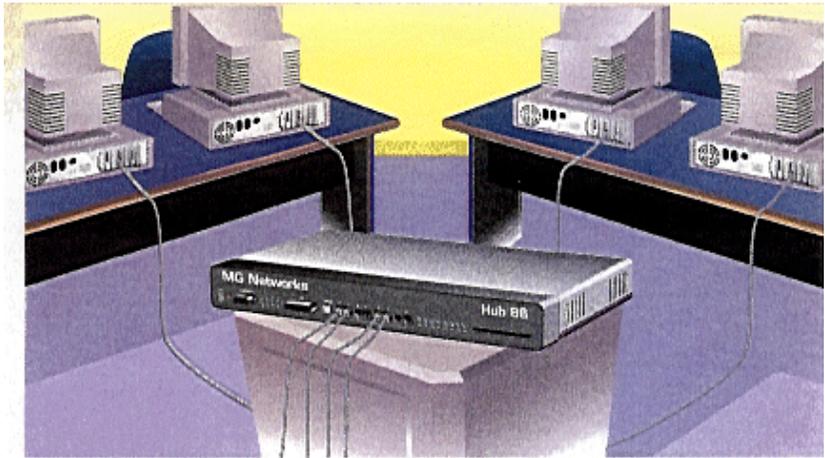


Figure 6-13. 10 BaseT Network Connections

10BASE-T segments can be connected by using coaxial or fiber-optic backbone segments. Some hubs provide connectors for Thinnet and Thicknet cables (in addition to 10BASE-T UTP-type connectors).

By attaching a 10BASE-T transceiver to the AUI port of the network adapter, you can use a computer set up for Thicknet on a 10BASE-T network.

The star wiring of 10BASE-T provides several advantages, particularly in larger networks. First, the network is more reliable and easier to manage because 10BASE-T networks use a concentrator (a centralized wiring hub). These hubs are “intelligent” in that they can detect defective cable segments and route network traffic around them. This capability makes locating and repairing bad cable segments easier.

10BASE-T enables you to design and build your LAN one segment at a time, growing, as your network needs to grow. This capability makes 10BASE-T more flexible than other LAN cabling options.

10BASE-T is also relatively inexpensive to use compared to other cabling options. In some cases in which a data-grade phone system already has been used in an existing building, the data-grade phone cable can be used for the LAN.

The rules for a 10BASE-T network are as follows:

- The maximum number of computers on a LAN is 1,024.
- The cabling should be UTP Category 3, 4, or 5. (Shielded twisted-pair cabling, STP, can be used in place of UTP.)
- The maximum unshielded cable segment length (hub to transceiver) is 100 meters (328 feet).
- The cable distance between computers is 2.5 meters (8 feet).

6.6.1.4 10BASE-FL

10BASE-FL is a specification for Ethernet over fiber-optic cables. The 10BASE-FL specification calls for a 10 Mbps data rate using baseband.

The most important advantages are long cabling runs (10BASE-FL supports a maximum cabling distance of about 2,000 meters) and the elimination of any potential electrical complications.

6.6.1.5 100VG-ANYLAN

100VG-AnyLAN is defined in the IEEE 802.12 standard. *IEEE 802.12* is a standard for transmitting Ethernet and Token Ring packets (IEEE 802.3 and 802.5) at 100 Mbps. 100VG-AnyLAN is sometimes called 100BASE-VG. The “VG” in the name stands for voice grade.

100VG-AnyLAN uses a *cascaded star* topology, which calls for a hierarchy of hubs. Computers are attached to *child hubs*, and the child hubs are connected to higher-level hubs called *parent hubs*.

The maximum length for the two longest cables attached to a 100VG-AnyLAN hub is 250 meters (820 ft). The specified cabling is Category 3, 4, or 5 twisted-pair or fiber-optic. 100VG-AnyLAN is compatible with 10BASE-T cabling.

6.6.1.6 100BASE-X

100BASE-X uses a star bus topology similar to 10BASE-T's. 100BASE-X provides a data transmission speed of 100 Mbps using baseband.

The 100BASE-X standard provides the following cabling specifications:

- **100BASE-TX.** Two twisted-pairs of Category 5 UTP or STP
- **100BASE-FX.** Fiber-optic cabling using 2-strand cable
- **100BASE-T4.** Four twisted-pairs of Category 3, 4, or 5 UTP

100BASE-X is sometimes referred to as “Fast Ethernet.” Like 100VG-AnyLAN, 100BASE-X provides compatibility with existing 10BASE-T systems and thus enables plug-and-play upgrades from 10BASE-T.

6.6.2 TOKEN RING

Token ring uses a token passing architecture that adheres to the IEEE 802.5 standard. The topology is physically a star, but token ring uses a logical ring to pass the token from one station to station. Each node must be attached to a concentrator called a multistation access unit (MSAU or MAU). This is often thought of as a hub, however, a MAU only works on a token ring network.

Token-ring network interface cards can run at 4Mbps or 16Mbps. The 16Mbps cards can run at 4Mbps or 16Mbps, whereas, the 4Mbps can only run at 4. All cards on a given network ring must run at the same rate. If all cards are not configured this way, either the machine connected to the card cannot have network access, or the entire network can be ground to a halt.

To pass data on a token ring network, a frame called a token perpetually circulates around a token ring. The computer that holds the token has control of the transmission medium. The actual process is as follows:

- A computer in the ring captures the token.
- If the computer has data to transmit, it holds the token and transmits a data frame.
- Each computer in the ring checks to see whether it is the intended recipient of the frame.
- When the frame reaches the destination address, the destination PC copies the frame to a receive buffer, update the frame status field of the data frame, and puts the frame back on the ring.
- When the computer that originally sent the frame receives it from the ring, it acknowledges a successful transmission, takes the frame off the ring, and places the token back on the ring.

6.6.3 ARCNET

ARCNet is an older architecture that is not found too often in the business world, but does have a presence in many older networks and school systems who often receive hand-me-downs from the business sector.

ARCNet utilizes a token-passing protocol that can have a star or bus physical topology. These segments can be connected with either active or passive hubs. ARCNet, when connected in a star topology, can use either twisted pair or coaxial cable. If coax is used to create a star topology, the ends of the cable are attached directly to a BNC connector, without



Figure 6-14. Token Ring Network

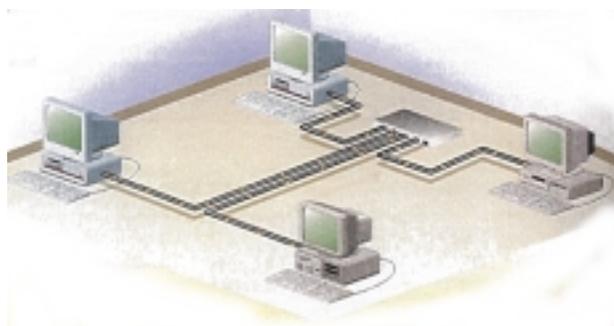


Figure 6-15. ARCNet Network

a terminator. When in a bus topology, ARCNet uses a 93-ohm terminator, which is attached to each end of the bus in a similar fashion to an ethernet bus.

Each ARCNet card has a set of DIP switches built onto it. You can change the setting of the DIP switches to give each card a separate hardware address. Based upon these addresses, tokens are passed to the card with the next highest address on the network. Due to the “access to the network passing,” ARCNet shares some characteristics with a token passing network.

6.6.4 FDDI

Fiber Distributed Data Interface (FDDI) is very similar to token ring in that it relies on a node to have the token before it can use the network. It differs from token ring in that it utilizes fiber-optic cable as its transmission media, allowing for transmissions of up to 100Km. This standard permits up to 100 devices on the network with a maximum distance between stations of up to 2 kilometers.

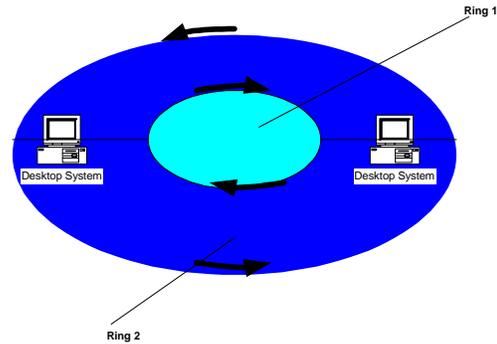


Figure 6-16. FDDI Network

FDDI has two different configurations: Class A and B. Class A uses two counteracting rings. Devices are attached to both rings. If one of these rings develops a fault, the other ring can still be used to transmit data. Class B uses a single ring to transmit data.

6.7 THE VAST MAJORITY OF NETWORKS TODAY CABLING

The vast majority of networks today are connected by some sort of cabling that acts as a network transmission medium that carries signals between computers. Many cable types are available to meet the varying needs and sizes of networks, from small to large.

Cable types can be confusing. Belden, a leading cable manufacturer, publishes a catalog that list more than 2200 types of cabling. Fortunately, only three major groups of cabling connect the majority of networks.

6.7.1 COAXIAL CABLE

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial cable's wide usage: it was relatively inexpensive, and it was light, flexible, and easy to work with. In its simplest form, coaxial cable consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. There are two basic types of coaxial cable. Thin (thinnet) cable and Thick (thicknet) cable. Which type of cable you select depends on the needs of your particular network. You can connect thinnet to thicknet using something called a transceiver.

6.7.1.1 THINNET

Thinnet cable is a flexible coaxial cable about 0.64 centimeters (.25 inches) thick. Because this type of coaxial cable is flexible



Figure 6-17a. Coaxial Cable

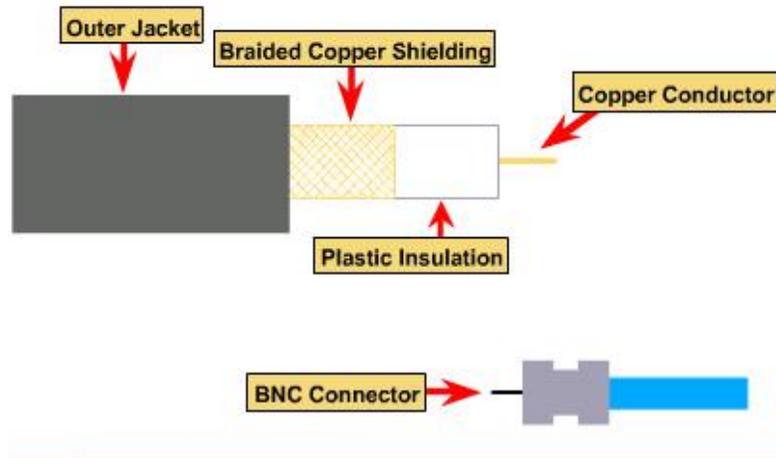
and easy to work with, it can be used in almost any type of network installation. Thinnet cable can connect directly to the computer's network interface card.

Thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters before the signal starts to suffer from attenuation.

6.7.1.2 THICKNET

Thicknet cable is a relatively rigid coaxial cable about 1.27 centimeters in diameter. Thicknet cable is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet. Thicknet cable's copper core is thicker than a thinnet cable core.

The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet cable. Thicknet cable can carry a signal for 500 meters. Therefore, because of the thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.



- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Inexpensive
- ◆ Media and connector size: Medium
- ◆ Maximum cable length: 500m (medium)

Figure 6-17b. Coaxial Cable

6.7.1.3 COAXIAL CABLE CONNECTION HARDWARE

Both thinnet and thicknet cable use a connection component, known as a BNC connector, to make connections between the cable and computers. There are several important components in the BNC family, including the following:

- **The BNC cable connector** – This connector is either soldered or crimped to the end of a cable.
- **The BNC T connector** – This connector joins the network interface card (NIC) in the computer to the network cable.
- **The BNC barrel connector** - This connector is used to join two lengths of thinnet cable to make on longer length.



Figure 6-18. Coaxial Cable with T Connector



Figure 6-19. Terminators for Coaxial Cable

- **The BNC terminator** – The terminator closes each end of the bus cable to absorb stray signals. Otherwise, the signal will bounce and all network activity can come to a stop due to collisions.

6.7.1.4 COAXIAL-CABLING CONSIDERATIONS

Consider the following coaxial capabilities when making a decision about which type of cabling to use. Use coaxial cable if you need a medium that can:

- Transmit voice, video, and data.
- Transmit data for greater distances than is possible with less expensive cabling.
- Offer a familiar technology with reasonable data security.

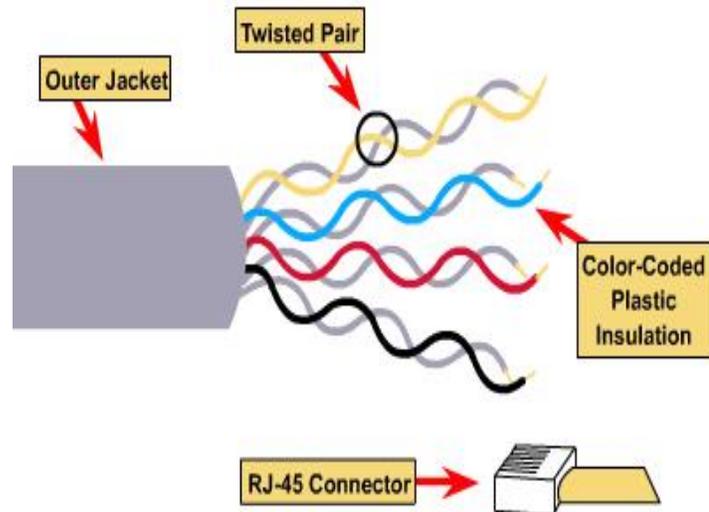
6.7.2 TWISTED PAIR CABLE

In its simplest form, twisted-pair cable consists of two insulated strands of copper wire twisted around each other. There are two types of twisted-pair cable: unshielded twisted pair (UTP) and shielded twisted pair (STP). A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The total number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays and transformers.

6.7.2.1 UNSHEILDED TWISTED PAIR (UTP)

UTP, use the 10BASET specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters.

Traditional UTP cable consists of two insulated copper wires. UTP specifications govern how many twists are permitted per foot of cable; the number of twists allowed depends on the purpose to which the cable will put. In North America, UTP cable is the most commonly used cable for existing telephone systems and is already installed in many office buildings.



- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Least Expensive
- ◆ Media and connector size: Small
- ◆ Maximum cable length: 100m (short)

The 568A Commercial Building Wiring Standard of Electronic Industries Association and the Telecommunications Industries Associate (EIA/TIA) specifies the type of UTP cable that is to be used in a variety of building and wiring situations. The objective is to ensure consistency of products for customers. There are five categories of UTP:

- **Category 1** – This refers to traditional UTP telephone cable that can carry voice but not data transmissions. Most telephone cable prior to 1983 was Category 1.
- **Category 2** – This category certifies UTP cable for data transmissions up to 4 megabits per second (Mbps). It consists of four twisted pairs of copper wire.
- **Category 3** – The category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted pairs of copper wire with three twists per foot.
- **Category 4** – This category certifies UTP cable for data transmissions up to 20 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5** – This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted pairs of copper wire.

Figure 6-20. Twisted Pair Unshielded Outline

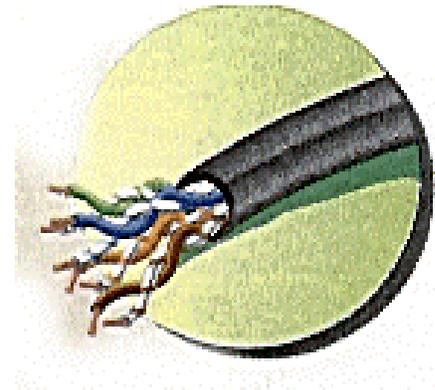


Figure 6-21. UTP Cable

Most telephone systems use a type of UTP. In fact, one reason why UTP is so popular is because any buildings are pre-wired for twisted-pair telephone systems. As part of the pre-wiring process, extra UTP is often installed to meet future cabling needs. If preinstalled twisted-pair cable is of sufficient grade to support data transmission, it can be used in a computer network. Caution is required, however, because

common telephone wire might not have the twisting and other electrical characteristics required for clean, secure, computer data transmission.

6.7.2.2 SHIELDED TWISTED-PAIR (STP) CABLE

STP cable uses woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. STP uses a foil wrap around each of the wire pairs. This gives STP excellent shielding to protect the transmitted data from outside interference's with in turn allows it to support higher transmission rates over longer distances than UTP.

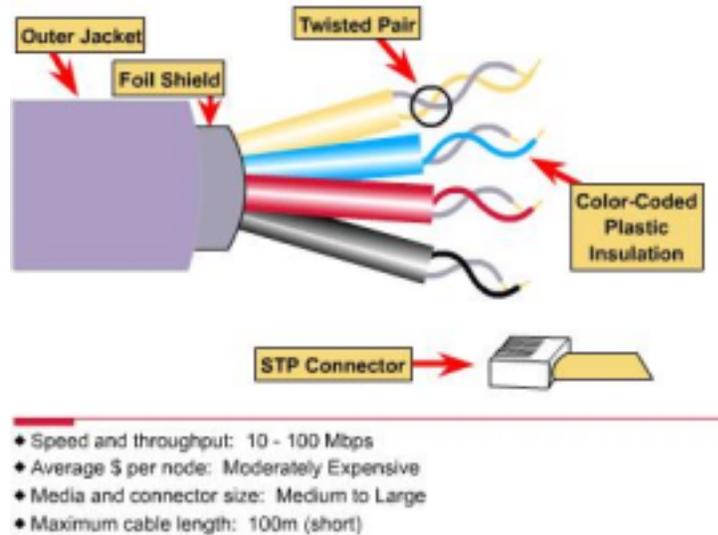


Figure 6-22. Twisted Cable Shielded Outline

6.7.2.3 TWISTED-PAIR CONNECTION HARDWARE

Twisted-pair cabling uses RJ-45 telephone connectors to connect to a computer. These are similar to RJ-11 telephone connectors. Although RJ-11 and RJ-45 connectors look alike at first glance, there are crucial differences between them.

The RJ-45 connector is slightly larger and will not fit into the RJ-11 telephone jack. The RJ-45 connector houses eight cable connections, while the RJ-11 houses only four.

Several components are available to help organize large UTP installations and make them easier to work with. Some of these are:

- **Distribution racks and rack shelves.** Distribution racks and rack shelves can create more room for cables where there isn't much floor space. Using them is a good way to organize a network that has a lot of connections.
- **Expandable patch panels.** These come in various versions that support up to 96 ports and transmission speed of up to 100 Mbps.
- **Jack couplers.** These single or double RJ-45 jacks snap into patch panels and wall plates and support data rates up to 100 Mbps.
- **Wall plates.** These support two or more couplers.



Figure 6-23. RJ45 Connector for Twisted Pair

6.7.2.4 TWISTED-PAIR CABLING CONSIDERATIONS

Use twisted-pair cable if:

- Your LAN is under budget constraints.
- You want a relatively easy installation in which computer connections are simple.

Do not use twisted-pair if:

- Your LAN requires a high level of security and you must be absolutely sure of data integrity.
- You must transmit data over long distances at high speeds.

6.7.3 FIBER-OPTIC CABLE

In fiber-optic cable, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fiber-optic cable. This means that fiber-optic cable cannot be tapped, and its data cannot be stolen.

Fiber-optic cable is a good choice for very high-speed, high capacity data transmissions because of the purity of the signal and lack of attenuation.

An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. The fibers are sometimes made of plastic. Plastic is easier to install, but cannot carry the light pulses for as long a distance as glass. Because each glass strand passes signals in only one direction, a cable includes two strands in separate jackets. One strand transmits and one receives. A reinforcing layer of plastic surrounds each glass strand, and Kevlar fibers provide strength. The Kevlar fibers in the fiber-optic connector are placed between the two cables. Just as their counterparts (twisted-pair and coaxial) are, fiber-optic cables are encased in a plastic coating for protection.

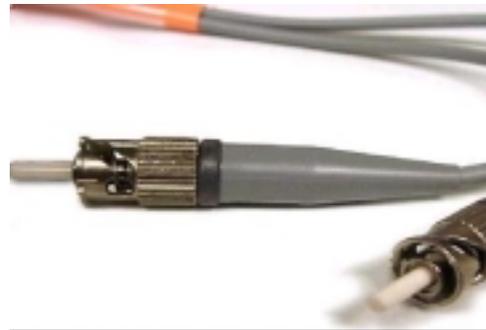
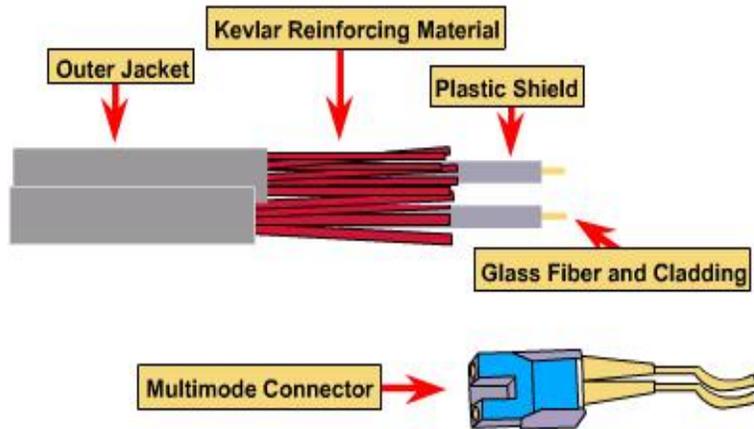


Figure 6-24 Fiber Optic Cable

Fiber-optic cable transmissions are not subject to electrical interference and are extremely fast, currently transmitting about 100 Mbps with demonstrated rates of up to 1 gigabit per second (Gbps). They can carry a signal – the light pulse – for many miles.



- ◆ Speed and throughput: 100+ Mbps
- ◆ Average \$ per node: Most Expensive
- ◆ Media and connector size: Small
- ◆ Maximum cable length: Up to 2km
- ◆ Single mode: One stream of laser-generated light
- ◆ Multimode: Multiple streams of LED-generated light

Figure 6-25. Fiber Optic Cable Outline

6.7.3.1 FIBER-OPTIC CABLING CONSIDERATIONS

Use fiber-optic cable if you:

- Need to transmit data at very high speeds over long distances in very secure media.

Do not use fiber-optic cable if you:

- Are under a tight budget.
- Do not have expertise available to properly install it and connect devices to it.

6.7.4 SELECTING CABLE

So exactly what is the best cable for your job? To determine which cable to use, answer the following questions:

- How heavy will the network traffic be?
- What level of security does the network require?
- What distances must the cable cover?
- What are the cable options?
- What is the budget for cabling?

See Table 6-1 a cable comparison summary:

Characteristics	Thinnet coaxial 10BASE2 cable	Thicknet coaxial 10BASE5	Twisted-pair 10BASET cable	Fiber-optic cable
Cable Cost	More than UTP	More than thinnet	UTP: Least expensive STP: More than thinnet	More than thinnet, but less than thicknet
Usable Cable length	185 meters (about 607 feet)	500 meters (about 1640 feet)	UTP and STP: 100 meters (about 328 feet)	2 kilometers (6562 feet)
Transmission rate	4-100 Mbps	4-100 Mbps	UTP: 4-100 Mbps STP: 16-500 Mbps	100 Mbps or more (>1 Gbps)
Flexibility	Fairly flexible	Less flexible than thinnet	UTP: Most flexible STP: Less flexible than UTP	Less flexible than thicknet
Ease of installation	Easy to install	Moderately easy to install	UTP: Very easy; often preinstalled STP: Less flexible than UTP	Difficult to install
Susceptibility to interference	Good resistance to interference	Good resistance to interference	UTP: Very susceptible STP: Good resistance	Not susceptible to interference
Special features	Electronic support components are less expensive than twisted –pair cable.	Electronic support components are less expensive than twisted –pair cable.	UTP: Same as telephone wire; often preinstalled in buildings STP: Supports higher transmission rate than UTP	Supports voice, data, and video
Preferred uses	Medium to large sites with high security needs.	Linking thinnet networks	UTP: a smaller sites on a budget. STP: Token ring in any size	Any size installation requiring speed and high data security.

Table 6-1. Cable Comparison Summary

6.8 OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

Having a model in mind helps you understand how the pieces of the network puzzle fit together. The most commonly used model is the Open Systems Interconnection (OSI) reference model. The OSI model, first released in 1984 by the International Standards Organization (ISO), provides a useful structure for defining and describing the various processes underlying networking communications.

The OSI model is a blueprint for vendors to follow when developing protocol implementations. The OSI model organizes communication protocols into seven layers. Each layer addresses a narrow portion of the communication process. Figure 6-26 illustrates the layers of the OSI model.

A good way to remember which layer goes into what order is:

Top Down **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
Bottom Up **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

When data is being transferred over a network, it must pass through each layer of the OSI model. As the data passes through each layer, information is added to the data.

When the data reaches the destination, the data again pass through the layers of the OSI model. The additional information is removed at each layer. Figure 6-27 illustrates this.

The seven levels of the OSI model is:

- **Application Layer** is responsible for exchanging information between the programs running on a computer and other services on a network, such as a database or print service.

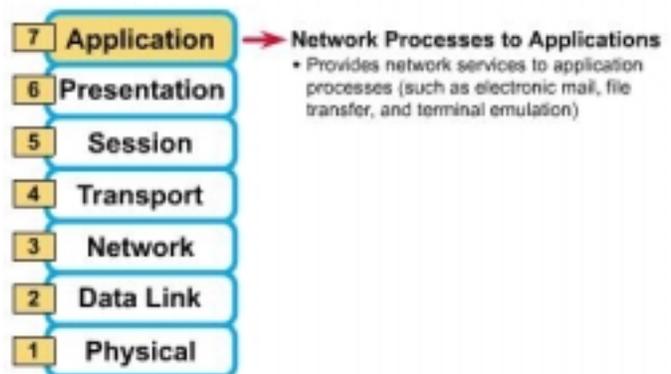


Figure 6-27. Application Layer



Figure 6-26. OSI Model

- **Presentation Layer**
formats information so that a software Application can read the information.

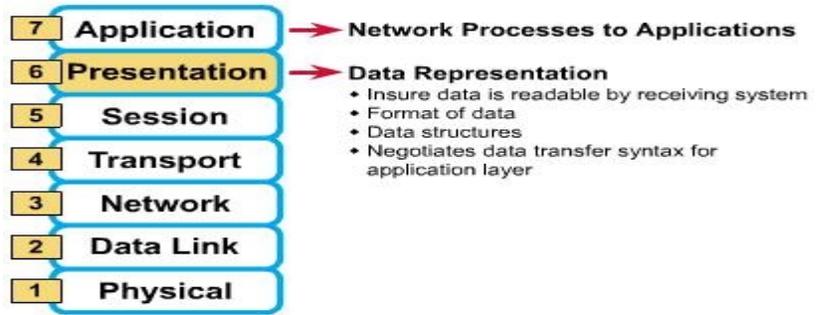


Figure 6-28. Presentation Layer

- **Session Layer**
determines how two devices communicate as well as establishes and monitors connections between computers.

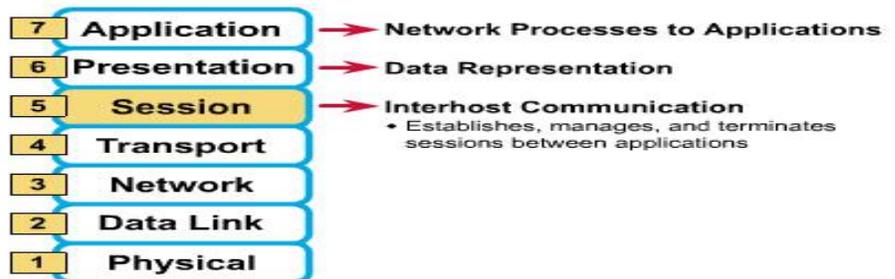


Figure 6-29. Session Layer

- **Transport Layer**
corrects transmission errors and ensures that information is delivered reliably.

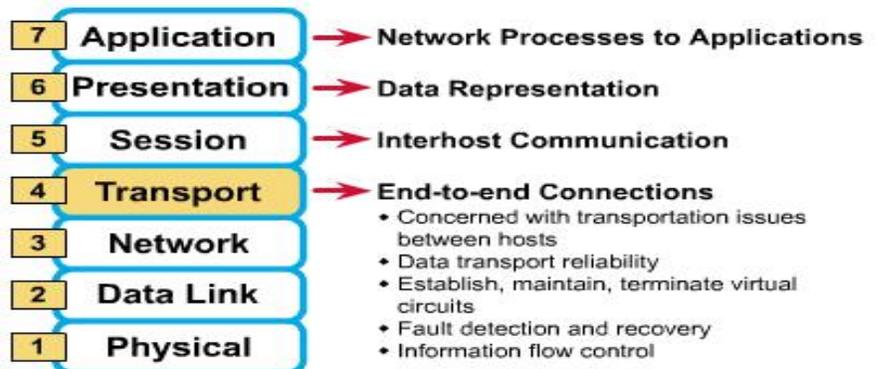


Figure 6-30. Transport Layer

- **Network Layer** identifies computers on a network and determines how to direct information transferring over a network.

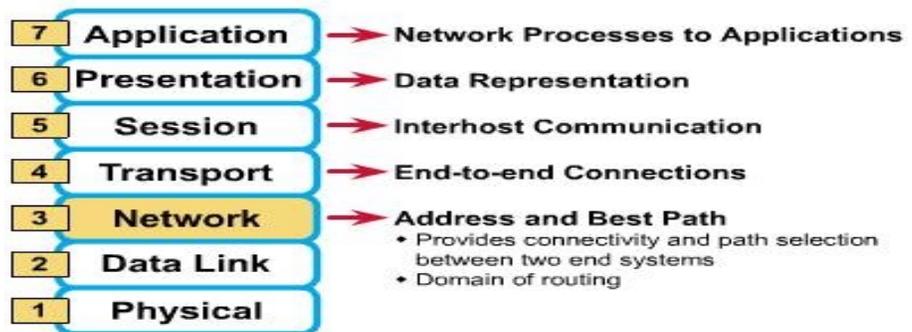


Figure 6-31. Network Layer

- **Data Link Layer** groups data into sets to prepare the data for transferring over a network.

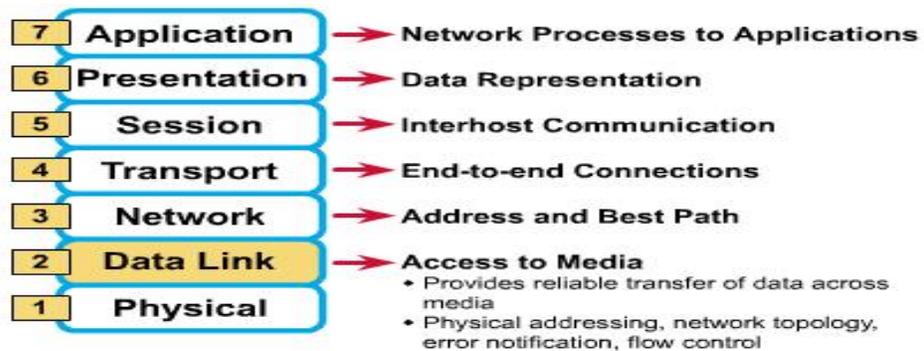


Figure 6-32. Data Link Layer

- **Physical Layer** defines how a transfer medium, such as cables, connects to a computer. This layer also specifies how electrical information transfers on the transmission media.

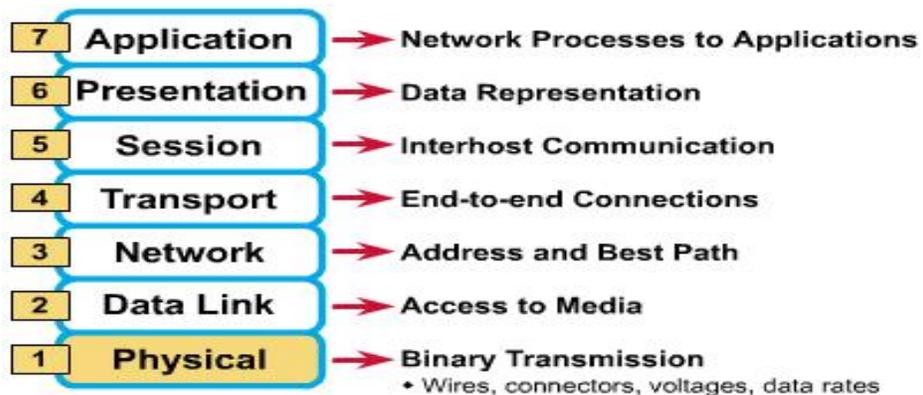


Figure 6-33. Physical Layer

6.9 ENCAPSULATION OF OSI MODEL

6.9.1 DATA ENCAPSULATION

You know that all communications on a network originate at a source, and are sent to a destination, and that the information that is sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another computer (host B), the data must first be packaged by a process called encapsulation.

Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information. (Note: The word "header" means that address information has been added.)

6.9.2 DATA ENCAPSULATION EXAMPLE

To see how encapsulation occurs, let's examine the manner in which data travels through the layers as illustrated in the Figure. Once the data is sent from the source, as depicted in the Figure, it travels through the application layer down through the other layers. As you can see, the packaging and flow of the data that is exchanged goes through changes as the networks perform their services for end-users. As illustrated in the Figures, networks must perform the following five conversion steps in order to encapsulate data:

1. **Build the data.**
As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.

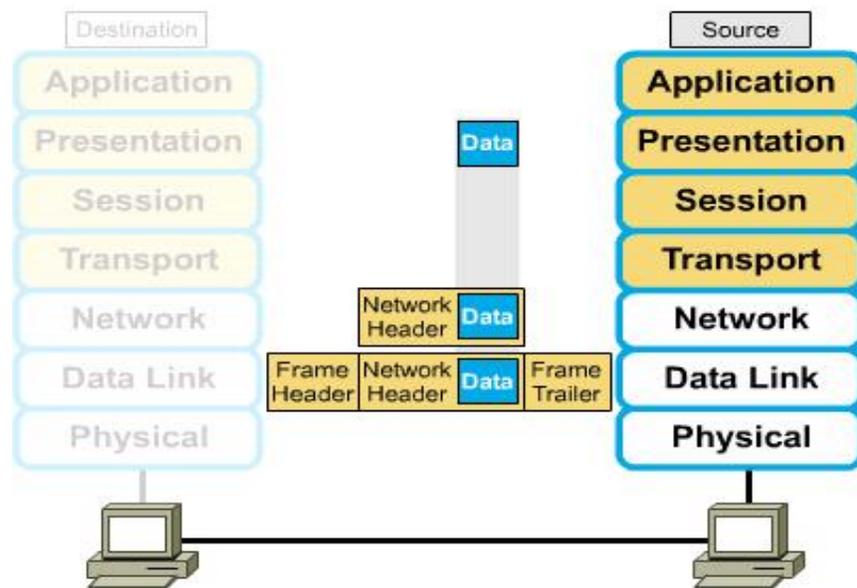


Figure 6-34. Data Encapsulation

2. **Package the data for end-to-end transport.**

The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.

3. **Append (add) the network address to the header.**

The data is put into a packet or datagram that contains a network header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.

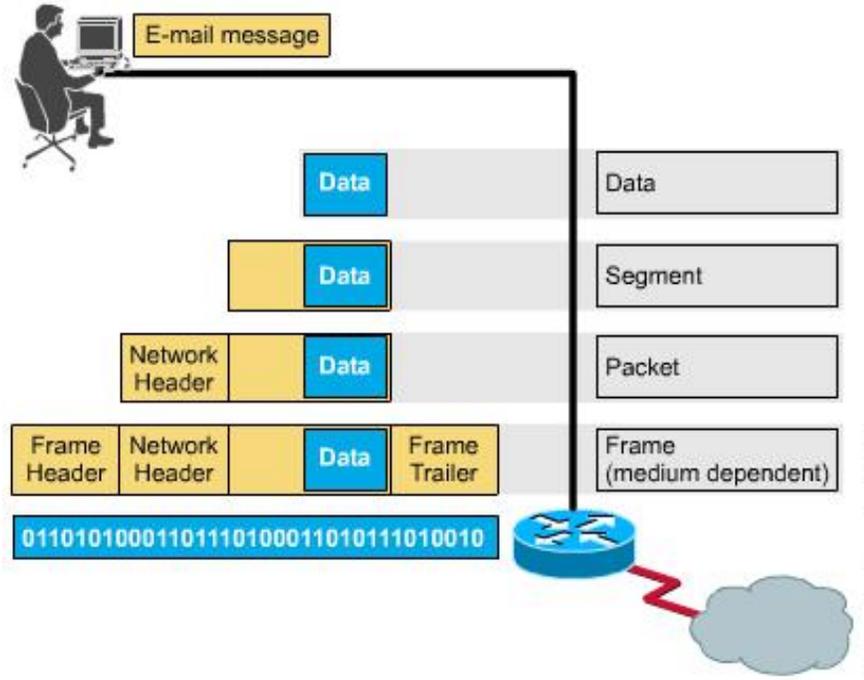


Figure 6-35. Data Encapsulation

4. **Append (add) the local address to the data link header.**

Each network device must put the packet into a frame. The frame allows connection to the next directly-connected network device on the link. Each device in the chosen network path requires framing in order for it to connect to the next device.

5. **Convert to bits for transmission.**

The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium (usually a wire). A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN. Headers and trailers are added as data moves down through the layers of the OSI model.

6.10 LINKING NETWORKS

Each network type covers a limited physical area and supports a limited number of computers. You can overcome these limits by linking networks together with additional hardware. For example, you can plug two thin Ethernet segments into a device called a repeater, or you can cable together two twisted pair hubs. You can even connect two networks of different types by connecting them to a device called a bridge. If two networks are too far apart to plug both into a repeater or bridge, you need routers.

6.10.1 REPEATERS

A repeater is a connector that takes a signal that is being transferred on a network and re-transmits the information. Repeaters allow signals to travel farther along a network.

Repeaters are used to extend the length of transmission media, such as cables, which connects computer devices together on a network. Repeaters are especially useful in areas where long lengths of cables are required to connect the computer devices together, such as a network in a large warehouse.



Figure 6-36. Repeater

Repeaters are very simple devices that do not operate efficiently when they have to transfer large amounts of information. Repeaters should not be used to extend the length of a busy network.

6.10.2 BRIDGES

A bridge is a device that allows the computers on individual networks or separate parts of a network to exchange information. Bridges are also used to split an overloaded network into smaller parts. Splitting an overload network reduces the amount of information transferring in each part of the network.

Bridges determine if information is going to a destination on the same network or the network on the other side of the bridge. If the destination is on the network on the other side of the bridge, the bridge forwards the information to that network. A bridge improves efficiency because information is only forwarded to a different network when necessary.

Bridges can only transfer information from one network to another. Since bridges cannot change the information in any way, bridges can only connect similar types of networks.

6.10.3 ROUTERS

Routers are connectors that are used to link different networks together. Routers can direct, or route, information to the correct destination. On a large network, there may be more than one route that information can take to get to its destination.

Routes that are not normally used to transfer information are called redundant paths. If a section of the network has been shut down for maintenance or due to malfunction, then the redundant paths can be used to transfer information.

Most routers can automatically determine the best route for information. With older routers, called static routers, a network administrator had to manually configure each route information could take. Newer routers, called dynamic routers, can automatically configure the available routes on the network.

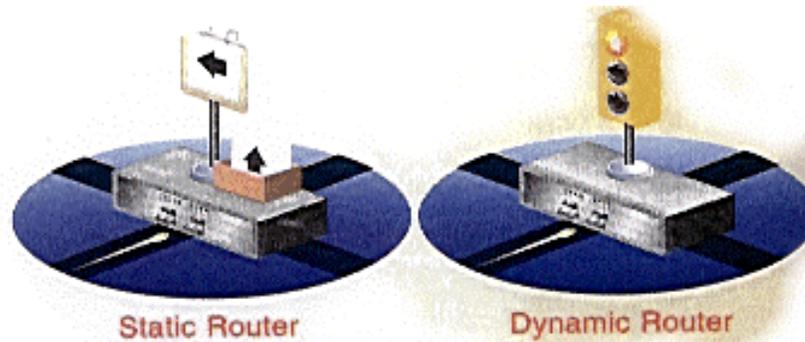


Figure 6-37. Static and Dynamic Router

Routers map networks and divide them into individual segments. Each segment is assigned to a

specific address. The network segment address and the address of the destination computer help the router determine the best route for the information to take through the network.

Unlike some other types of network connectors, routers are often used to connect different types of networks together. Along with the ability to analyze the information and then determine the best route, routers can also translate the information into a form that can be transmitted on another type of network.

Routers are often used to connect local area networks to a wide are network. Routers can also be used to break up the side area network into segments. This helps reduce the amount of information being transferred over the network and improves the efficiency of the wide are network.

6.10.4 DIAL-UP NETWORKING HARDWARE

Dial-up networking requires telecommunications hardware. The most common equipment is a modem with a throughput of 14.4, 28.8, 33.6 Kbps, or 57.6 (the newer models) Kbps. Slower modems usually result in unacceptable performance. Desktop computers, needing frequent access to remote networks, sometimes use ISDN adapters to connect to ISDN lines. ISDN allows voice and data over the same line at the same time and has a high data transfer rate (64 Kbps per B-line 128 Kbps duplexed).

Dial-up networking trades performance for convenience. Your laptop can access your office network from any telephone line, but it does so at a relatively slow speed. Typical Ethernet networks have a theoretical throughput of 10 Mbps, but usually use about 20% of that capacity (which is 2 Mbps or 2,000 Kbps). Compare that with a modem that relies on compressible data and clean phone lines to achieve its upper limit of 28.8 or 33.6 Kbps.

6.11 RESOURCES

Teach Yourself Networking Visually, IDG Book

MCSE Training Kit Networking Essentials Plus 3rd Edition, Microsoft Press

MCSE Training Guide Networking Essentials, Jose Casad and Dan Newland, New Riders

6.12 SUMMARY

In this section, we discussed your networking environment. While you will not have to design it, you will have the responsibility to manage it. Having an understanding of the concept and terminology is your first step. We discussed the hardware and software requirements giving us the network capability. We discussed how we expand our LANs and connect to other LANs, forming WANs. We talked about different topologies and architectures and the basics of the OSI model. We talked about the OSI Encapsulation and how it works. Finally, we showed that with the use of modems, we have virtual connections from any computer.

6.13 REVIEW QUESTIONS

1. What is networking?
2. What are the characteristics of a LAN?
3. Name some differences between client/server and peer-to-peer networks?
4. What should you consider when selecting an adapter?
5. List the three types of HUBs.
6. What are the differences between bus, star, and ring topologies?
7. What are three common types of network cabling?
8. What are the seven layers of the OSI model?