Topic 5: Fundamental Networks

This will provide an overview of network principles, standards, and purposes. The following types of networks will be discussed in this chapter:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Wireless LAN (WLAN)

The different types of network topologies, protocols, and logical models as well as the hardware needed to create a network will also be discussed. You will also learn about network software, communication methods, and hardware relationships.

Principles of Networking

Networks are systems that are formed by links. Websites that allow individuals to link to each other's pages are called social networking sites. A set of related ideas can be called a conceptual network. The connections you have with all your friends can be called your personal network.

People use the following networks every day:

- Mail delivery system
- Telephone system
- Public transportation system
- Corporate computer network
- The Internet

Computers can be linked by networks to share data and resources. A network can be as simple as two computers connected by a single cable or as complex as hundreds of computers connected to devices that control the flow of information. Converged data networks can include general purpose computers, such as PCs and servers, as well as devices with more specific functions, including printers, phones, televisions, and game consoles.

All data, voice, video, and converged networks share information and use various methods to direct how this information flows. The information on the network goes from one place to another, sometimes via different paths, to arrive at the appropriate destination.

The public transportation system is similar to a data network. The cars, trucks, and other vehicles are like the messages that travel within the network. Each driver defines a starting point (source) and an ending point (destination). Within this system, there are rules such as stop signs and traffic lights that control the flow from the source to the destination.

Computer Networks

A computer data network is a collection of hosts connected by networking devices. A host is any device that sends and receives information on the network. Peripherals are devices that are connected to hosts. Some devices can serve either as hosts or peripherals. For example, a printer connected to your laptop which is on a network is acting as a peripheral. If the printer is connected directly to a networking device, such as a hub, switch, or router, it is acting as a host.

Computer networks are used globally in businesses, homes, schools, and government agencies. Many of the networks are connected to each other through the Internet.

Many different types of devices can connect to a network:

- Desktop computers
- Laptop computers
- Printers
- Scanners
- PDAs
- Smartphones
- File/print servers

A network can share many different types of resources:

- Services, such as printing or scanning
- Storage space on removable devices, such as hard drives or optical drives
- Applications, such as databases

You can use networks to access information stored on other computers, print documents using shared printers, and synchronize the calendar between your computer and your Smartphone.

Network devices link together using a variety of connections:

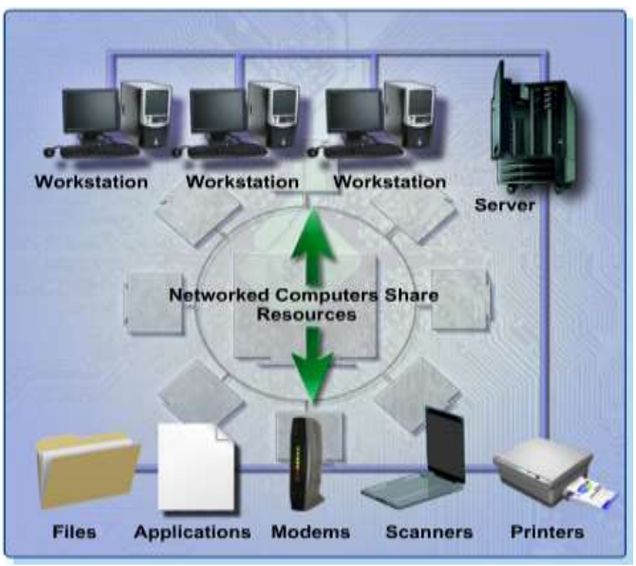
- Copper cabling – Uses electrical signals to transmit data between devices
- Fiber-optic cabling – Uses glass or plastic wire, also called fiber, to carry information as light pulses
- Wireless connection – Uses radio signals, infrared technology (laser), or satellite transmissions

Benefits of Networking

The benefits of networking computers and other devices include lower costs and increased productivity. With networks, resources can be shared, which results in less duplication and corruption of data.

Fewer Peripherals Needed

The Figure shows that many devices can be connected on a network. Each computer on the network does not need to have its own printer, scanner, or backup device. Multiple printers can be set up in a central location and shared among the network users. All network users send print jobs to a central print server that manages the print requests. The print server can distribute print jobs over multiple printers, or queue jobs that require a specific printer.



Increased Communication Capabilities

Networks provide several different collaboration tools that can be used to communicate between network users. Online collaboration tools include e-mail, forums and chats,

voice and video, and instant messaging. With these tools, users can communicate with friends, family, and colleagues.

Avoid File Duplication and Corruption
A server manages network resources. Servers store data and share it with users on a network. Confidential or sensitive data can be protected and shared with the users who have permission to access that data. Document tracking software can be used to prevent users from overwriting files, or changing files that others are accessing at the same time.

Lower Cost Licensing
Application licensing can be expensive for individual computers. Many software vendors offer site licenses for networks, which can dramatically reduce the cost of software. The site license allows a group of people or an entire organization to use the application for a single fee.

Centralized Administration
Centralized administration reduces the number of people needed to manage the devices and data on the network, reducing time and cost to the company. Individual network users do not need to manage their own data and devices. One administrator can control the data, devices, and permissions of users on the network. Backing up data is easier because the data is stored in a central location.

Conserve Resources
Data processing can be distributed across many computers to prevent one computer from becoming overloaded with processing tasks.

Types of Networks

Data networks continue to evolve in complexity, use, and design. To communicate about networks, different types of networks are given different descriptive names. A computer network is identified by the following specific characteristics:

- The area it serves
- How the data is stored
- How the resources are managed
- How the network is organized
- The type of networking devices used
- The type of media used to connect the devices

Local Area Network (LAN)

Local Area Network (LAN) refers to a group of interconnected devices that is under the same administrative control. In the past, LANs were considered to be small networks that existed in a single physical location. Àlthough LANs can be as small as a single local network installed in a home or small office, over time, the definition of LANs has evolved to include interconnected local networks consisting of many hundreds of devices, installed in multiple buildings and

locations. The important thing to remember is that all of the local networks within a LAN are under one administrative control group that governs the security and access control policies that are in force on the network. In this context, the word “Local” in Local Area Network refers to local consistent control rather than being physically close to each other. Devices in a LAN may be physically close, but it is not a requirement.

Wide Area Network (WAN)

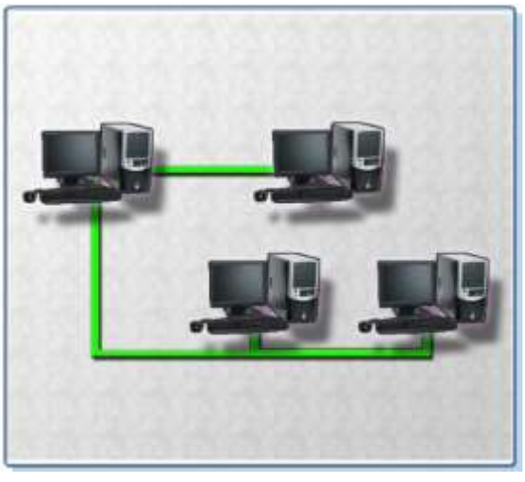
Wide Area Networks (WANs) are networks that connect LANs in geographically separated locations. The most common example of a WAN is the Internet. The Internet is a large WAN that is composed of millions of interconnected LANs. Telecommunications service providers (TSP) are used to interconnect these LANs at different locations.

Wireless Local Area Network (WLAN)

In a traditional LAN, devices are connected together using copper cabling. In some environments, installing copper cabling may not be practical, desirable, or even possible. In these situations, wireless devices are used to transmit and receive data using radio waves. These networks are called wireless LANs, or WLANs. As with LANs, on a WLAN you can share resources, such as files and printers, and access the Internet.

In a WLAN, wireless devices connect to access points within a specified area. Access points are typically connected to the network using copper cabling. Instead of providing copper cabling to every network host, only the wireless access point is connected to the network with copper cabling. WLAN coverage can be small and limited to the area of a room or can have greater range.

Peer-to-peer Networks



In a peer-to-peer network, devices are connected directly to each other without any additional networking devices between them. In this type of network, each device has equivalent capabilities and responsibilities. Individual users are responsible for their own resources and can decide which data and devices to share. Because individual users are responsible for the resources on their

own computers, there is no central point of control or administration in the network.

Peer-to-peer networks work best in environments with ten or fewer computers. Because individual users are in control of their own computers, there is no need to hire a dedicated network administrator.

Peer-to-peer networks have several disadvantages:

- There is no centralized network administration which makes it difficult to determine who controls resources on the network.
- There is no centralized security. Each computer must use separate security measures for data protection.
- The network becomes more complex and difficult to manage as the number of computers on the network increases.
- There may be no centralized data storage. Separate data backups must be maintained. This responsibility falls on the individual users.

Peer-to-peer networks still exist inside larger networks today. Even on a large client network, users can still share resources directly with other users without using a network server. In your home, if you have more than one computer, you can set up a peer-to-peer network. You can share files with other computers, send messages between computers, and print documents to a shared printer.

Client/Server Networks

In a client/server network, the client requests information or services from the server. The server provides the requested information or service to the client. Servers on a client/server network commonly perform some of the processing work for client machines; for example, sorting through a database before delivering only the records requested by the client.

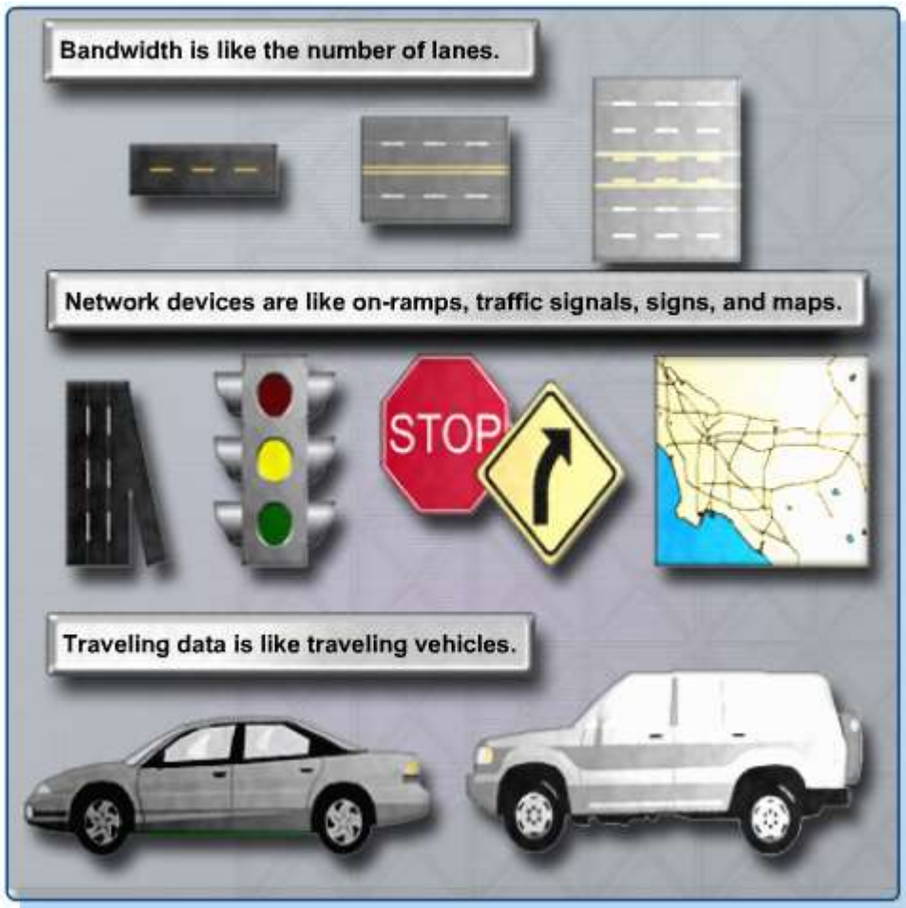
One example of a client/server network is a corporate environment in which employees use a company e-mail server to send, receive, and store e-mail. The e-mail client on an employee computer issues a request to the e-mail server for any unread e-mail. The server responds by sending the requested e-mail to the client.

In a client/server model, the servers are maintained by network administrators. Data backups and security measures are implemented by the network administrator. The network administrator also controls user access to the network resources. All of the data on the network is stored on a centralized file server. Shared printers on the network are managed by a centralized print server. Network users with the proper permissions can access both the data and shared printers. Each user must provide an authorized username and password to gain access to network resources that they are permitted to use. For data protection, an administrator performs a routine backup of all the files on the servers. If a computer crashes, or data is lost, the administrator can easily recover the data from a recent backup.

Networking Concepts and Technologies

As a computer technician, you will be required to configure and troubleshoot computers on a network. To effectively configure a computer on the network, you should understand IP addressing, protocols, and other network concepts.

Bandwidth and Data Transmission



Bandwidth is the amount of data that can be transmitted within a fixed time period. When data is sent over a computer network, it is broken up into small chunks called packets. Each packet contains headers. A header is information added to each packet that contains the source and destination of the packet. A header also contains information that describes how to put all of the packets back together again at the destination. The size of the bandwidth determines the amount of information that can be transmitted.

Bandwidth is measured in bits per second and is usually denoted by any of the following units of measure:

- bps – bits per second
- Kbps – kilobits per second
- Mbps – megabits per second

NOTE: One byte is equal to 8 bits, and is abbreviated with a capital B. One MBps is approximately 8 Mbps.

The figure shows how bandwidth on a network can be compared to a highway. In the highway example, the cars and trucks represent the data. The number of lanes on the highway

represents the amount of cars that could travel on the highway at the same time. An eight-lane highway can handle four times the number of cars that a two-lane highway can hold.

The data that is transmitted over the network can flow using one of three modes: simplex, half-duplex, or full-duplex.

Simplex
Simplex, also called unidirectional, is a single, one-way transmission. An example of simplex transmission is the signal that is sent from a TV station to your home TV.

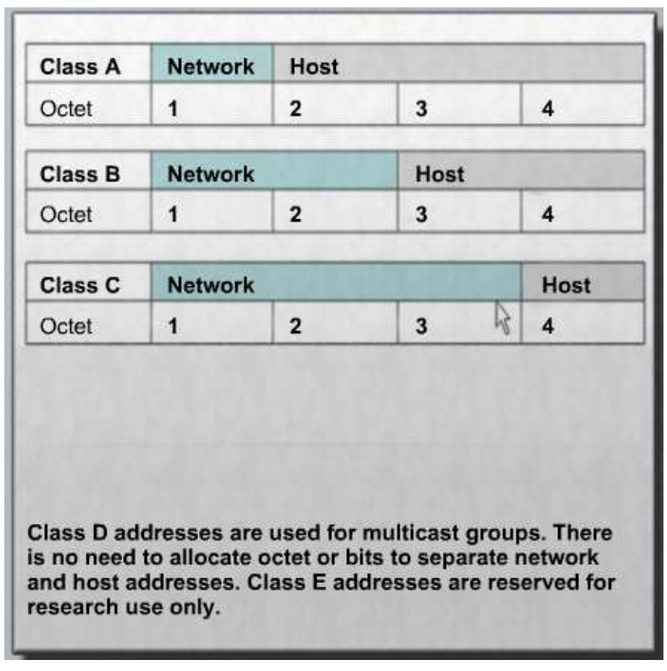
Half-Duplex
When data flows in one direction at a time, it is known as half-duplex. With half-duplex, the channel of communications allows alternating transmission in two directions, but not in both directions simultaneously. Two-way radios, such as police or emergency communications mobile radios, work with half-duplex transmissions. When you press the button on the microphone to transmit, you cannot hear the person on the other end. If people at both ends try to talk at the same time, neither transmission gets through.

Full-Duplex
When data flows in both directions at the same time, it is known as full-duplex. Although the data flows in both directions, the bandwidth is measured in only one direction. A network cable with 100 Mbps in full-duplex mode has a bandwidth of 100 Mbps.

A telephone conversation is an example of full-duplex communication. Both people can talk and be heard at the same time.

Full-duplex networking technology increases network performance because data can be sent and received at the same time. Broadband technology allows multiple signals to travel on the same wire simultaneously. Broadband technologies, such as digital subscriber line (DSL) and cable, operate in full-duplex mode. With a DSL connection, for example, users can download data to the computer and talk on the telephone at the same time.

IP Addressing



An IP address is a number that is used to identify a device on the network. Each device on a network must have a unique IP address to communicate with other network devices. As noted earlier, a host is a device which sends or receives information on the network. Network devices are devices that move data across the network including hubs, switches, and routers. On a LAN, each host and network device must have an IP address within the same network to be able to communicate with each other.

A person's name and fingerprints usually do not change. They provide a label or address for the physical aspect of the person – the body. A person's mailing address, on the other hand, relates to where the person lives or picks up mail. This address can change. On a host, the Media Access Control (MAC) address (explained below) is assigned to the host NIC and is known as the physical address. The physical address remains the same regardless of where the host is placed on the network in the same way that fingerprints remain with the person regardless of where the person goes.

The IP address is similar to the mailing address of a person. It is known as a logical address because it is logically assigned based on the host location. The IP address, or network address, is based on the local network and is assigned to each host by a network administrator. This process is similar to the local government assigning a street address based on the logical description of the city or village and neighborhood.

An IP address consists of a series of 32 binary bits (ones and zeros). It is very difficult for humans to read a binary IP address. For this reason, the 32 bits are grouped into four 8-bit bytes called octets. An IP address, even in this grouped format, is hard for humans to read, write and remember; therefore, each octet is presented as its decimal value, separated by a decimal point or period. This format is referred to as dotted-decimal notation. When a host is configured with an IP address, it is entered as a dotted decimal number, such as 192.168.1.5. Imagine if you had to enter the 32-bit binary equivalent of this: 11000000101010000000000100000101. If just one bit were mistyped, the address would be different and the host may not be able to communicate on the network.

The logical 32-bit IP address is hierarchical and is composed of two parts. The first part identifies the network and the second part identifies a host on that network. Both parts are required in an IP address. As an example, if a host has IP address 192.168.18.57, the first three octets, 192.168.18, identify the network portion of the address, and the last octet, 57 identifies the host. This is known as hierarchical addressing, because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network and not the location of each individual host.

IP addresses are divided into the following five classes:

- Class A – Large networks, implemented by large companies and some countries
- Class B – Medium-sized networks, implemented by universities
- Class C – Small networks, implemented by ISP for customer subscriptions
- Class D – Special use for multicasting
- Class E – Used for experimental testing

Subnet Mask

The subnet mask is used to indicate the network portion of an IP address. Like the IP address, the subnet mask is a dotted decimal number. Usually all hosts within a LAN use the same subnet mask. Figure 1 shows default subnet masks for usable IP addresses that are mapped to the first three classes of IP addresses:

- 255.0.0.0 – Class A, which indicates that the first octet of the IP address is the network portion
- 255.255.0.0 – Class B, which indicates that the first two octets of the IP address is the network portion
- 255.255.255.0 – Class C, which indicates that the first three octets of the IP address is the network portion

If an organization owns one Class B network but needs to provide IP addresses for four LANs, the organization would have to subdivide the Class B address into four smaller parts. Subnetting is a logical division of a network. It provides the means to divide a network, and the subnet mask specifies how it is subdivided. An experienced network administrator typically performs subnetting. After the subnetting scheme has been created, the proper IP addresses and subnet masks can be configured on the hosts in the four LANs. These skills are taught in the Cisco Networking Academy courses related to CCNA level networking skills.

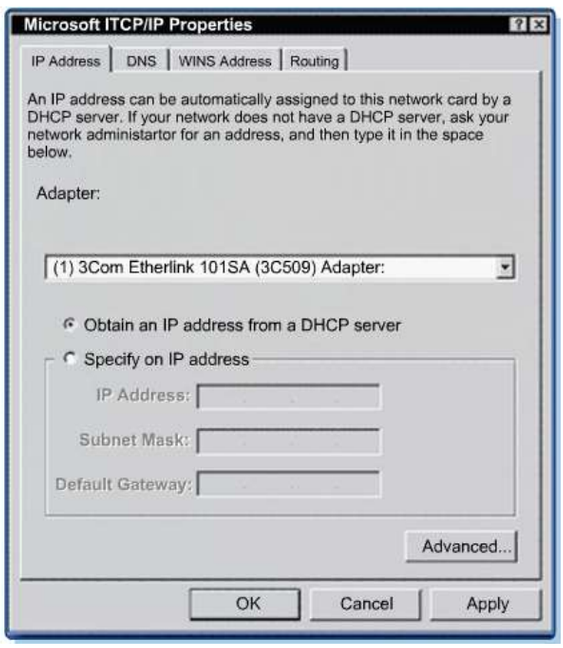
Manual Configuration

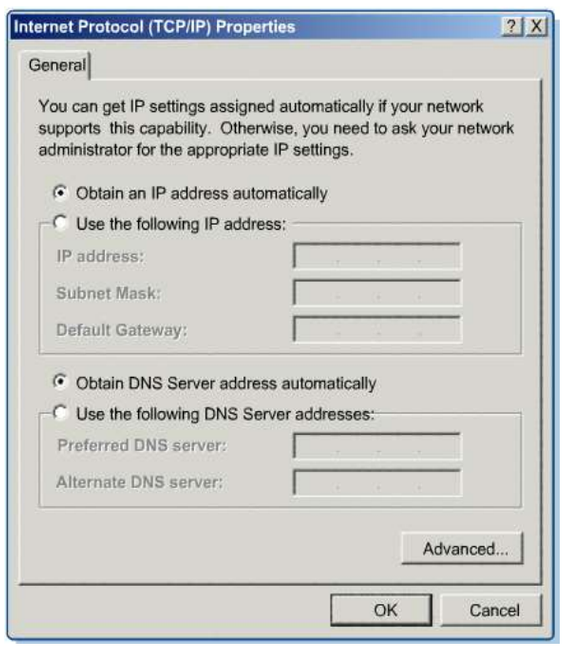
In a network with a small number of hosts, it is easy to manually configure each device with the proper IP address. A network administrator who understands IP addressing should assign the addresses and should know how to choose a valid address for a particular network. The IP address that is entered is unique for each host within the same network or subnet.

To manually enter an IP address on a host, go to the TCP/IP settings in the Properties window for the Network Interface Card (NIC). The NIC is the hardware that enables a computer to connect to a network. It has an address called the Media Access Control (MAC) address. Whereas the IP address is a logical address that is defined by the network administrator, a MAC address is "burned-in" or permanently programmed into the NIC when it is manufactured. The IP address of a NIC can be changed, but the MAC address never changes. The main difference between an IP address and a MAC address is that the MAC address is used to deliver frames on the LAN, while an IP address is used to transport frames outside the LAN. A frame is a data packet, along with address information added to the beginning and end of the packet before transmission over the network. Once a frame is delivered to the destination LAN, the MAC address is used to deliver the frame to the end host on that LAN.

Dynamic Host Configuration Protocol (DHCP)

If more than a few computers comprise the LAN, manually configuring IP addresses for every host on the network can be time-consuming and prone to errors. In this case, the use of a Dynamic Host Configuration Protocol (DHCP) server would automatically assign IP addresses and greatly simplify the addressing process.





Dynamic Host Configuration Protocol (DHCP) is a software utility used to dynamically assign IP addresses to network devices. This dynamic process eliminates the need for manually assigning IP addresses. A DHCP server can be set up and the hosts can be configured to automatically obtain an IP address. When a computer is set to obtain an IP address automatically, all of the other IP addressing configuration boxes are dimmed, as shown in the Figure (left). The server maintains a list of IP addresses to assign, and manages the process so that every device on the network receives a unique IP address. Each address is held for a predetermined amount of time. When the time expires, the DHCP server can use this address for any computer that joins the network.

This is the IP address information that a DHCP server can assign to hosts:

- IP address
- Subnet mask
- Default gateway
- Optional values, such as a Domain Name System (DNS) server address

The DHCP server receives a request from a host. The server then selects IP address information from a set of predefined addresses that are stored in a database. Once the IP address information is selected, the DHCP server offers these values to the requesting host on the network. If the host accepts the offer, the DHCP server leases the IP address for a specific period of time.

Using a DHCP server simplifies the administration of a network because the software keeps track of IP addresses. Automatically configuring TCP/IP also reduces the possibility of assigning duplicate or invalid IP addresses. Before a computer on the network can take advantage of the DHCP server services, the computer must be able to identify the server on the local network. A computer can be configured to accept an IP address from a DHCP server by clicking the "Obtain an IP address automatically" option in the NIC configuration window.

If your computer cannot communicate with the DHCP server to obtain an IP address, the Windows operating system will automatically assign a private IP address. If your computer is assigned an IP address in the range of 169.254.0.0 to 169.254.255.255, your computer will only be able to communicate with other computers in the same range. An example of when these private addresses would be useful is in a classroom lab where you want to prevent access outside of your network. This operating system feature is called Automatic Private IP Addressing (APIPA). APIPA will continually request an IP address from a DHCP server for your computer.

Internet Protocols and Applications

A protocol is a set of rules. Internet protocols are sets of rules governing communication within and between computers on a network. Protocol specifications define the format of the messages that are exchanged. A letter sent through the postal system also uses protocols. Part of the protocol specifies the position on the envelope that the delivery address needs to be written. If the delivery address is written in the wrong place, the letter cannot be delivered.

Timing is crucial to network operation. Protocols require messages to arrive within certain time intervals so that computers will not wait indefinitely for messages that may have been lost. Therefore, systems maintain one or more timers during transmission of data. Protocols also initiate alternative actions if the network does not meet the timing rules. Many protocols consist of a suite of other protocols that are stacked in layers. These layers depend on the operation of the other layers in the suite to function properly.

These are the main functions of protocols:

- Identifying errors
- Compressing the data
- Deciding how data is to be sent
- Addressing data
- Deciding how to announce sent and received data

To understand how networks and the Internet work, you must be familiar with the commonly used protocols. These protocols are used to browse the web, send and receive e-mail, and transfer data files. You will encounter other protocols as your experience in IT grows, but they are not used as often as the common protocols described here.

Protocol	Description
TCP/IP	A protocol used to transport data on the Internet
NETBEUI\NETBIOS	A small, fast protocol designed for a workgroup network that requires no connection to the Internet
IPX/SPX	A protocol used to transport data on a Novell Netware network
HTTP/HTTPS	A protocol that defines how files are exchanged on the Web
FTP	A protocol that provides services for file transfer and manipulation
SSH	A protocol that is used to connnect computers together securely
Telnet	A protocol that uses a text-based connection to a remote TCP/IP computer
POP	A protocol used to download e-mail messages from an e-mail server
IMAP	A protocol used to download e-mail messages from an e-mail server
SMTP	A protocol used to send mail in a TCP/IP network

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is used by devices on a network to send control and error messages to computers and servers. There are several different uses for ICMP, such as announcing network errors, announcing network congestion, and troubleshooting.

Packet internet groper (ping) is commonly used to test connections between computers. Ping is a simple but highly useful command line utility used to determine whether a specific IP address is accessible. You can ping the IP address to test IP connectivity. Ping works by sending an ICMP echo request to a destination computer or other network device. The receiving device then sends back an ICMP echo reply message to confirm connectivity.

Ping is a troubleshooting tool used to determine basic connectivity. The command line switches that can be used with the ping command are shown in the Figure. Four ICMP echo requests (pings) are sent to the destination computer. If it is reachable, the destination computer

responds with four ICMP echo replies. The percentage of successful replies can help you to determine the reliability and accessibility of the destination computer.

You can also use ping to find the IP address of a host when the name is known. If you ping the name of a website, for example, www.cisco.com, the IP address of the server displays.

Other ICMP messages are used to report undelivered packets, data on an IP network that includes source and destination IP addresses, and whether a device is too busy to handle the packet. Data, in the form of a packet, arrives at a router, which is a networking device that forwards data packets across networks toward their destinations. If the router does not know where to send the packet, the router deletes it. The router then sends an ICMP message back to the sending computer informing it that the data was deleted. When a router becomes very busy, it may send a different ICMP message to the sending computer indicating that it should slow down because there is congestion on the network.

Physical Components of a Network

There are many devices that can be used in a network to provide connectivity. The device you use will depend on how many devices you are connecting, the type of connections that they use, and the speed at which the devices operate. These are the most common devices on a network:

- Computers
- Hubs
- Switches
- Routers
- Wireless access points

The physical components of a network are needed to move data between these devices. The characteristics of the media determine where and how the components are used. These are the most common media used on networks:

- Twisted-pair
- Fiber-optic cabling
- Radio waves

Network Devices

To make data transmission more extensible and efficient than a simple peer-to-peer network, network designers use specialized network devices, such as hubs, switches, routers, and wireless access points, to send data between devices.

Hubs

Hubs are devices that extend the range of a network by receiving data on one port, and then regenerating the data and sending it out to all other ports. This process means that all traffic from a device connected to the hub is sent to all the other devices connected to the hub every time the hub transmits data. This causes a great amount of network traffic. Hubs are also called concentrators, because they serve as a central connection point for a LAN.

Bridges and Switches

Files are broken up into small pieces of data, called packets, before they are transmitted over a network. This process allows for error checking and easier retransmission if the packet is lost or corrupted. Address information is added to the beginning and to the end of packets before they are transmitted. The packet, along with the address information, is called a frame.

LANs are often divided into sections called segments, similar to the way a company is divided into departments. The boundaries of segments can be defined using a bridge. A bridge is a device used to filter network traffic between LAN segments. Bridges keep a record of all the devices on each segment to which the bridge is connected. When the bridge receives a frame, the destination address is examined by the bridge to determine if the frame is to be sent to a different segment, or dropped. The bridge also helps to improve the flow of data by keeping frames confined to only the segment to which the frame belongs.

Switches, shown in the figure, are sometimes called multiport bridges. A typical bridge may have just two ports, linking two segments of the same network. A switch has several ports, depending on how many network segments are to be linked. A switch is a more sophisticated device than a bridge. A switch maintains a table of the MAC addresses for computers that are connected to each port. When a frame arrives at a port, the switch compares the address information in the frame to its MAC address table. The switch then determines which port to use to forward the frame.

Routers

Whereas a switch connects segments of a network, routers, shown in the Figure, are devices that connect entire networks to each other. Switches use MAC addresses to forward a frame within a single network. Routers use IP addresses to forward frames to other networks. A router can be a computer with special network software installed, or a router can be a device built by network equipment manufacturers. Routers contain tables of IP addresses along with optimal destination routes to other networks.

Wireless Access Points

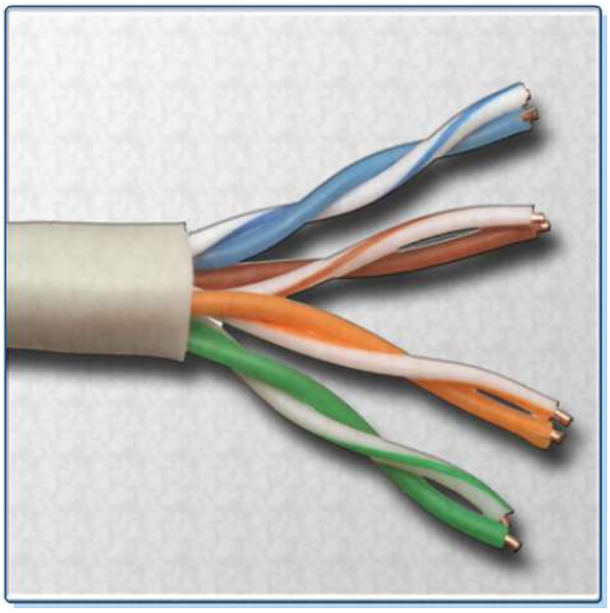
Wireless access points provide network access to wireless devices such as laptops and PDAs. The wireless access point uses radio waves to communicate with radios in computers, PDAs, and other wireless access points. An access point has limited range of coverage. Large networks require several access points to provide adequate wireless coverage.

Multipurpose Devices

There are network devices that perform more than one function. It is more convenient to purchase and configure one device that serves all of your needs than to purchase a separate device for each function. This is especially true for the home user. In your home, you would purchase a multipurpose device instead of a switch, a router, and a wireless access point. The Linksys 300N,

shown in the figure, is an example of a multipurpose device.

Common Network Cables



Until recently, cables were the only medium used to connect devices on networks. A wide variety of networking cables are available. Coaxial and twisted-pair cables use copper to transmit data. Fiber-optic cables use glass or plastic to transmit data. These cables differ in bandwidth, size, and cost. You need to know what type of cable to use in different situations so that you are able to install the correct cables for the job. You will also need to be able to troubleshoot and repair problems that you encounter.

Twisted-Pair

Twisted-pair is a type of copper cabling that is used for telephone communications and most Ethernet networks. A pair of wires forms a circuit that can transmit data. The pair is twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs of wires in the cable. Pairs of copper wires are encased in color-coded plastic insulation and twisted together. An outer jacket protects the bundles of twisted pairs.

When electricity flows through a copper wire, a magnetic field is created around the wire. A circuit has two wires, and in a circuit, the two wires have oppositely-charged magnetic fields. When the two wires of the circuit are next to each other, the magnetic fields cancel each other out. This is called the cancellation effect. Without the cancellation effect, your network communications become slow due to the interference caused by the magnetic fields.

There are two basic types of twisted-pair cables:

- **Unshielded twisted-pair (UTP)** – Cable that has two or four pairs of wires. This type of cable relies solely on the cancellation effect produced by the twisted-wire pairs that limits signal degradation caused by electromagnetic interface (EMI) and radio frequency interference (RFI). UTP is the most commonly used cabling in networks. UTP cables have a range of 328 feet (100 m).
- **Shielded twisted-pair (STP)** – Each pair of wires is wrapped in metallic foil to better shield the wires from noise. Four pairs of wires are then wrapped in an overall metallic braid or foil. STP reduces electrical noise from within the cable. It also reduces EMI and RFI from outside the cable.

Although STP prevents interference better than UTP, STP is more expensive because of extra shielding, and more difficult to install because of the thickness. In addition, the metallic shielding must be grounded at both ends. If improperly grounded, the shield acts like an antenna picking up unwanted signals. STP is primarily used outside North America.

Category Rating

UTP comes in several categories that are based on two factors:

- The number of wires in the cable
- The number of twists in those wires

Category 3 is the wiring used for telephone systems and for Ethernet LAN at 10 Mbps. Category 3 has four pairs of wires.

Category 5 and Category 5e have four pairs of wires with a transmission rate of 100 Mbps. Category 5 and 5e are the most common network cables used. Category 5e has more twists per foot than Category 5 wiring. These extra twists further prevent interference from outside sources and the other wires within the cable.

Some Category 6 cables use a plastic divider to separate the pairs of wires, which prevents interference. The pairs also have more twists than Category 5e cable.

Coaxial Cable

Coaxial cable is a copper-cored cable surrounded by a heavy shielding. Coaxial cable is used to connect computers in a network. There are several types of coaxial cable:

- **Thicknet or 10BASE5** – Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 500 meters
- **Thinnet 10BASE2** – Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 185 meters
- **RG-59** – Most commonly used for cable television in the U.S.
- **RG-6** – Higher quality cable than RG-59, with more bandwidth and less susceptibility to interference

Fiber-Optic Cable

An optical fiber is a glass or plastic conductor that transmits information using light. Fiber-optic cable, shown in the Figure , has one or more optical fibers enclosed in a sheath or jacket. Because it is made of glass, fiber-optic cable is not affected by electromagnetic interference or radio frequency interference. All signals are converted to light pulses to enter the cable, and converted back into electrical signals when they leave it. This means that fiber-optic cable can deliver signals that are clearer, can go farther, and have greater bandwidth than cable made of copper or other metals.

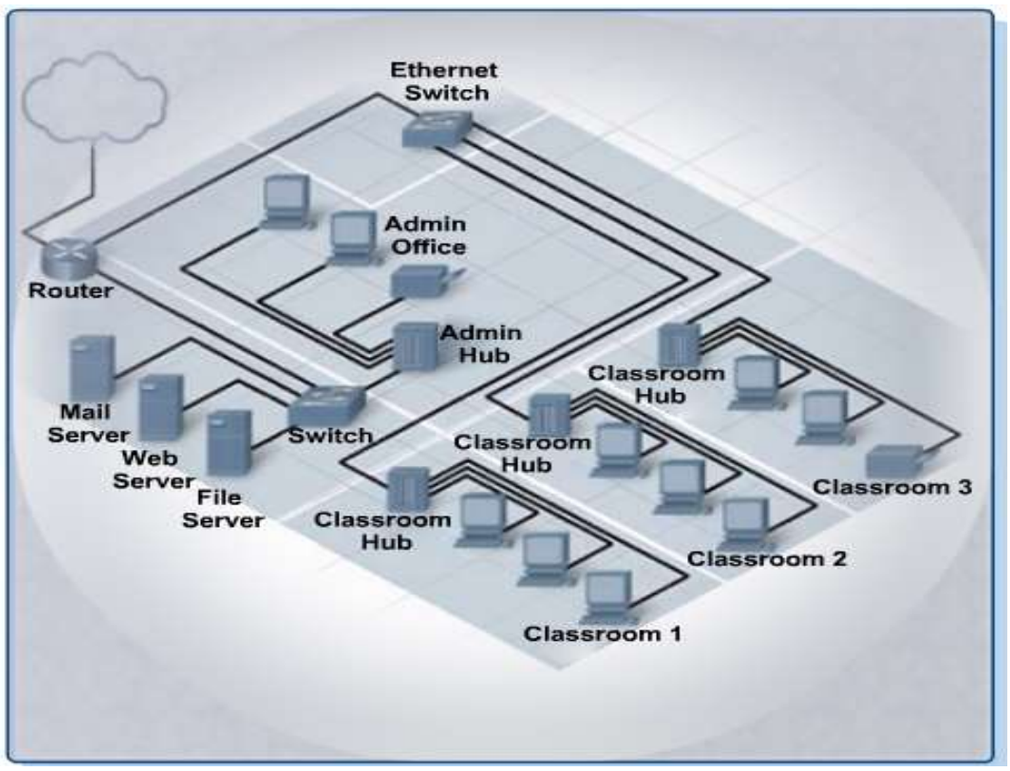
Fiber-optic cable can reach distances of several miles or kilometers before the signal needs to be regenerated. Fiber-optic cable is usually more expensive to use than copper cable and the connectors are more costly and harder to assemble. Common connectors for fiber-optic networks are SC, ST, and LC. These three types of fiber-optic connectors are half-duplex, which allows data to flow in only one direction. Therefore, two cables are needed.

These are the two types of glass fiber-optic cable:

- **Multimode** – Cable that has a thicker core than single-mode cable. It is easier to make, can use simpler light sources (LEDs), and works well over distances of a few kilometers or less.
- **Single-mode** – Cable that has a very thin core. It is harder to make, uses lasers as a light source, and can transmit signals dozens of kilometers with ease.

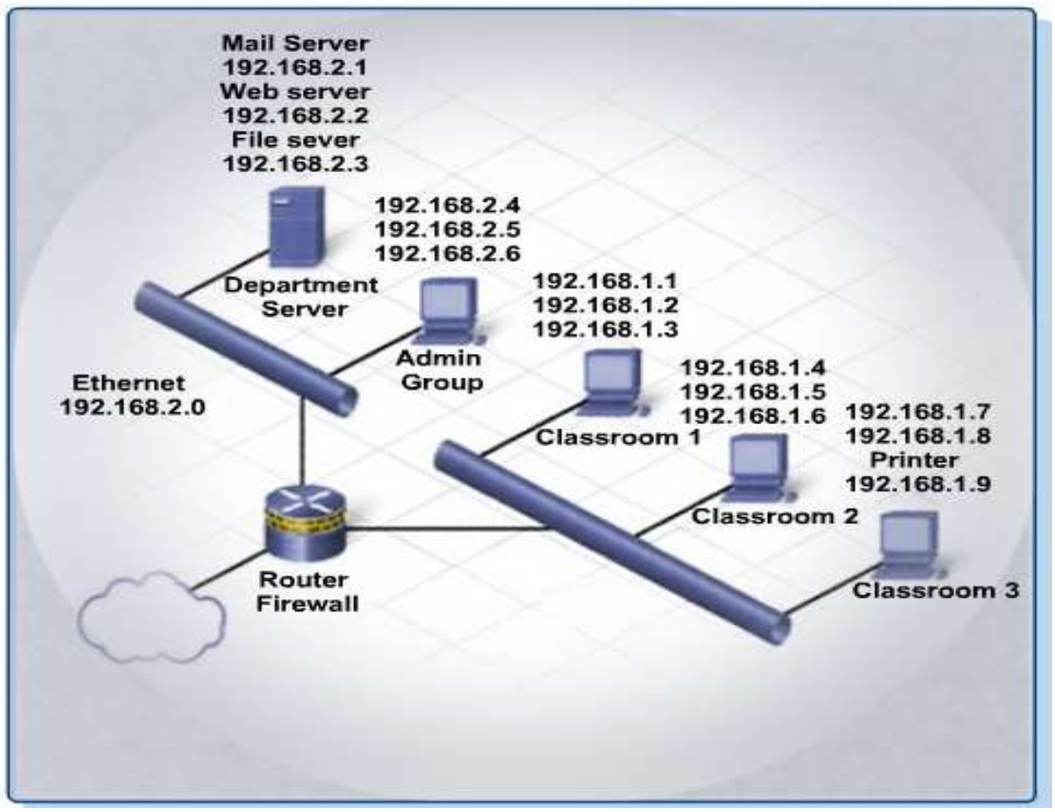
LAN Topologies and Architectures

Most of the computers that you work on will be part of a network. Topologies and architectures are building blocks for designing a computer network. While you may not build a computer network, you need to understand how they are designed in order to work on computers that are part of a network.

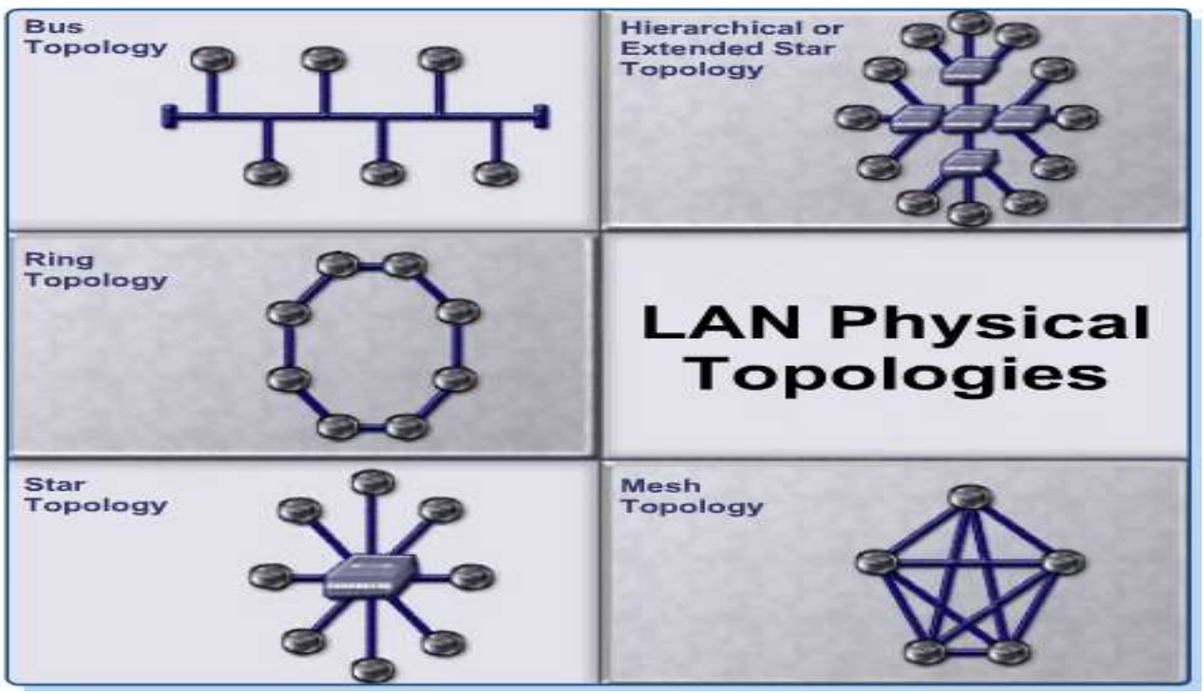


There are two types of LAN topologies: physical and logical. A physical topology, shown in Figure above, is the physical layout of the components on the network. A logical topology, shown in Figure below, determines how the hosts communicate across a medium, such as a cable or the airwaves. Topologies are commonly represented as network diagrams.

A LAN architecture is built around a topology. LAN architecture comprises all the components that make up the structure of a communications system. These components include the hardware, software, protocols, and sequence of operations.



LAN Topologies



A physical topology defines the way in which computers, printers, and other devices are connected to a network. A logical topology describes how the hosts accesses the medium and communicates on the network. The type of topology determines the capabilities of the network, such as ease of setup, speed, and cable lengths.

Physical Topologies

Figure shows the common LAN physical topologies:

- Bus
- Ring

- Star
- Hierarchical or Extended Star
- Mesh

Bus Topology
In the bus topology, each computer connects to a common cable. The cable connects one computer to the next, like a bus line going through a city. The cable has a small cap installed at the end, called a terminator. The terminator prevents signals from bouncing back and causing network errors.

Ring Topology
In a ring topology, hosts are connected in a physical ring or circle. Because the ring topology has no beginning or end, the cable does not need to be terminated. A specially-formatted frame, called a token, travels around the ring, stopping at each host. If a host wants to transmit data, the host adds the data and the destination address to the frame. The frame then continues around the ring until the frame stops at the host with the destination address. The destination host takes the data out of the frame.

Star Topology
The star topology has a central connection point, which is normally a device such as a hub, switch, or router. Each host on a network has a cable segment that attaches the host directly to the central connection point. The advantage of a star topology is that it is easy to troubleshoot. Each host is connected to the central device with its own wire. If there is a problem with that cable, only that host is affected. The rest of the network remains operational.

Hierarchical or Extended Star Topology
A hierarchical or extended star topology is a star network with an additional networking device connected to the main networking device. Typically, a network cable connects to one hub, and then several other hubs connect to the first hub. Larger networks, such as those of corporations or universities, use the hierarchical star topology.

Mesh Topology
The mesh topology connects all devices to each other. When every device is connected to every other device, a failure of any cable will not affect the network. The mesh topology is used in WANs that interconnect LANs.

Logical Topologies
The two most common types of logical topologies are broadcast and token passing.

In a broadcast topology, each host addresses either data to a particular host or to all hosts connected on a network. There is no order that the hosts must follow to use the network – it is first come, first served for transmitting data on the network.

Token passing controls network access by passing an electronic token sequentially to each host. When a host receives the token, it can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.

LAN Architectures

Architecture	Physical Topology	Logical Topology
Ethernet	Bus Star Extended Star	Bus
Token Ring	Star	Ring
Fiber-Distributed Data Interface (FDDI)	Double Ring	Ring

LAN architecture describes both the physical and logical topologies used in a network. Figure shows the three most common LAN architectures.

Ethernet

The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network use the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access control method. In CSMA/CD, hosts access the network using the first come, first served broadcast topology method to transmit data.

Ethernet uses a logical bus or broadcast topology and either a bus or star physical topology. As networks expand, most Ethernet networks are implemented using an extended star or hierarchical star topology, as shown in the Figure. Standard transfer rates are 10 Mbps and 100 Mbps, but new standards outline Gigabit Ethernet, which is capable of attaining speeds up to 1000 Mbps (1 Gbps).

Token Ring

IBM originally developed Token Ring as a reliable network architecture based on the token-passing access control method. Token Ring is often integrated with IBM mainframe systems. Token Ring is used with computers and mainframes.

Token Ring is an example of an architecture in which the physical topology is different from its logical topology. The Token Ring topology is referred to as a star-wired ring because the outer appearance of the network design is a star. The computers connect to a central hub, called a multistation access unit (MSAU). Inside the device, however, the wiring forms a circular data path, creating a logical ring. The logical ring is created by the token traveling out of an MSAU port to a computer. If the computer does not have any data to send, the token is sent back to the MSAU port and then out the next port to the next computer. This process continues for all computers and therefore resembles a physical ring.

FDDI

FDDI is a type of Token Ring network. The implementation and topology of FDDI differs from the IBM Token Ring LAN architecture. FDDI is often used to connect several buildings in an office complex or on a university campus.

FDDI runs on fiber-optic cable. FDDI combines high-speed performance with the advantages of the token-passing ring topology. FDDI runs at 100 Mbps on a dual-ring topology. The outer ring is called the primary ring and the inner ring is called the secondary ring.

Normally, traffic flows only on the primary ring. If the primary ring fails, the data automatically flows onto the secondary ring in the opposite direction.

An FDDI dual ring supports a maximum of 500 computers per ring. The total distance of each length of the cable ring is 62 miles (100 km). A repeater, which is a device that regenerates signals, is required every 1.2 miles (2 km). In recent years, many token ring networks have been replaced by faster Ethernet networks.

Standard Organizations

Several worldwide standards organizations are responsible for setting networking standards. Standards are used by manufacturers as a basis for developing technology, especially communications and networking technologies. Standardizing technology ensures that the devices you use will be compatible with other devices using the same technology. The standards groups create, examine, and update standards. These standards are applied to the development of technology to meet the demands for higher bandwidth, efficient communication, and reliable service.

Standards Organizations	
CCITT	*Comit Consultatif International Tlphonique et Tlgraphique* – This committee defines international communications standards. The CCITT defined the standard for sending fax documents and the standards that define data transmission over telephone lines such as V.90 that allows transmissions up to 56000 bps. After 1992, this organization became the ITU Telecommunication Standardization Sector (ITU-T).
IEEE	The IEEE is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. Founded in 1884, the organization is composed of engineers, scientists, and students. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology, and telecommunications to electric power, aerospace, and consumer electronics. IEEE has more than 860 active standards with 700 under development. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.
ISO	International Organization for Standardization (ISO) is an international organization composed of national standards bodies from over 140 countries. American National Standards Institute (ANSI), for example, is a member of ISO. ISO is a non-governmental organization established to promote the development of standardization and related activities. ISO's work results in international agreements, which are published as International Standards. ISO has defined a number of important computer standards, the most significant of which is perhaps the Open Systems Interconnection (OSI) model, a standardized architecture for designing networks. ISO together with International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) have built a strategic partnership with World Trade Organization (WTO).

IAB	The Internet Architecture Board (IAB) is committee that oversees the technical and engineering development of the Internet by the Internet Society (ISOC). This committee oversees the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). When the internet transitioned to a public entity in 1992, the name was changed to what it is today from the Internet Architecture Board, originally formed by the US Department of Defense.
IEC	Founded in 1906, the International Electrotechnical Commission (IEC) is the global organization that prepares and publishes international standards for all electrical, electronic, and related technologies. The IEC was founded because of a resolution passed at the International Electrical Congress held in St. Louis (USA) in 1904. The membership consists of more than 60 participating countries, including all the world's major trading nations and a growing number of industrialized countries. The IEC's mission is to promote, through its members, international cooperation on all questions related to electrotechnologies including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety, and the environment. The IEC is one of the bodies recognized by the World Trade Organization (WTO) and entrusted by it for monitoring the national and regional organizations agreeing to use the IEC's international standards as the basis for national or regional standards as part of the WTO's Technical Barriers to Trade Agreement.
ANSI	American National Standards Institute (ANSI) is a private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI identifies industrial and public requirements for national consensus standards and coordinates and manages their development, resolves national standards problems, and ensures effective participation in international standardization. Since 1918, the Institute's mission is to enhance both the global competitiveness of U.S. business and quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and safeguarding their integrity. ANSI does not develop standards itself. Rather it facilitates development by establishing consensus processes among qualified groups. This is why their acronym is seen on many standards.
TIA/EIA	Telecommunications Industry Association (TIA) and Electronic Industries Alliance (EIA) are trade associations that jointly develop and publish a series of standards covering structured voice and data wiring for LANs. These industry standards evolved after the U.S. telephone industry deregulation in 1984, which transferred responsibility for on premises cabling to the building owner. Prior to that, AT&T used proprietary cables and systems.

Ethernet Standards

Ethernet protocols describe the rules that control how communication occurs on an Ethernet network. To ensure that all Ethernet devices are compatible with each other, the IEEE

developed standards for manufacturers and programmers to follow when developing Ethernet devices.

Cabled Ethernet Standards

	10BASE-T	100BASE-TX	1000BASE-T
Media	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 5, 5e UTP, two pair	EIA/TIA Category 5, 5e UTP, four pair
Maximum Segment Length	100 m (328 feet)	100 m (328 feet)	100 m (328 feet)
Topology	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)

IEEE 802.3
The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implement the CSMA/CD access control method.

In CSMA/CD, all end stations "listen" to the network wire for clearance to send data. This process is similar to waiting to hear a dial tone on a phone before dialing a number. When the end station detects that no other host is transmitting, the end station will attempt to send data. If no other station sends any data at the same time, this transmission will arrive at the destination computer with no problems. If another end station observed the same clear signal and transmitted at the same time, a collision will occur on the network media.

The first station that detects the collision, or the doubling of voltage, sends out a jam signal that tells all stations to stop transmitting and to run a backoff algorithm. A backoff algorithm calculates random times in which the end station will start to try network transmission again. This random time is typically in one or two milliseconds (ms), or thousandths of a second. This sequence occurs every time there is a collision on the network and can reduce Ethernet transmission by up to 40%.

Ethernet Technologies
The IEEE 802.3 standard defines several physical implementations that support Ethernet. Some of the common implementations are described here.

Ethernet
10BASE-T is an Ethernet technology that uses a star topology. 10BASE-T is a popular Ethernet architecture whose features are indicated in its name:

- The ten (10) represents a speed of 10 Mbps.
- BASE represents baseband transmission. In baseband transmission, the entire bandwidth of a cable is used for one type of signal.
- The T represents twisted-pair copper cabling.

Advantages of 10BASE-T:

- Installation of cable is inexpensive compared to fiber-optic installation.
- Cables are thin, flexible, and easier to install than coaxial cabling.
- Equipment and cables are easy to upgrade.

Disadvantages of 10BASE-T:

- The maximum length for a 10BASE-T segment is only 328 feet (100 m).
- Cables are susceptible to electromagnetic interference (EMI).

Fast Ethernet

The high bandwidth demands of many modern applications, such as live video conferencing and streaming audio, have created a need for higher data-transfer speeds. Many networks require more bandwidth than 10 Mbps Ethernet.

100BASE-TX is much faster than 10BASE-T and has a theoretical bandwidth of 100 Mbps.

Advantages of 100BASE-TX:

- At 100 Mbps, transfer rates of 100BASE-TX are ten times that of 10BASE-T.
- 100BASE-X uses twisted-pair cabling, which is inexpensive and easy to install.

Disadvantages of 100BASE-TX:

- The maximum length for a 100BASE-TX segment is only 328 feet (100 m).
- Cables are susceptible to electromagnetic interference (EMI).

1000BASE -T is commonly known as Gigabit Ethernet. Gigabit Ethernet is a LAN architecture.

Advantages of 1000BASE-T:

- The 1000BASE-T architecture supports data transfer rates of 1 Gbps. At 1 Gbps, it is ten times faster than Fast Ethernet, and 100 times faster than Ethernet. This increased speed makes it possible to implement bandwidth-intensive applications, such as live video.
- The 1000BASE-T architecture has interoperability with 10BASE-T and 100BASE-TX.

Disadvantages of 1000BASE-T:

- The maximum length for a 1000BASE-T segment is only 328 feet (100 m).
- It is susceptible to interference.
- Gigabit NICs and switches are expensive.
- Additional equipment is required.

10BASE-FL, 100BASE-FX, 1000BASE-SX and LX are fiber-optic Ethernet Technologies.

Ethernet Standards

Standard	Bandwidth	Frequency	Range	Interoperability
IEEE 802.11a	Up to 54 Mbps	5 GHz band	150 ft (45.7 m)	Not interoperable with 802.11b, 802.11g, 802.11n
IEEE 802.11b	Up to 11 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11g
IEEE 802.11g	Up to 54 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11b
IEEE 802.11n (Pre - standard)	Up to 540 Mbps	2.4 GHz band	984 ft (250 m)	Interoperable with 802.11b, 802.11g

IEEE 802.11 is the standard that specifies connectivity for wireless networks. IEEE 802.11, or Wi-Fi, refers to the collective group of standards – 802.11a, 802.11b, 802.11g, and 802.11n. These protocols specify the frequencies, speeds, and other capabilities of the different Wi-Fi standards.

802.11a

Devices conforming to the 802.11a standard allow WLANs to achieve data rates as high as 54 Mbps. IEEE 802.11a devices operate in the 5 GHz radio frequency range and within a maximum range of 150 feet (45.7 m).

802.11b

802.11b operates in the 2.4 GHz frequency range with a maximum theoretical data rate of 11 Mbps. These devices operate within a maximum range of 300 feet (91 m).

802.11g

IEEE 802.11g provides the same theoretical maximum speed as 802.11a, which is 54 Mbps, but operates in the same 2.4 GHz spectrum as 802.11b. Unlike 802.11a, 802.11g is backward-compatible with 802.11b. 802.11g also has a maximum range of 300 feet (91 m).

802.11n

802.11n is a newer wireless standard that has a theoretical bandwidth of 540 Mbps and operates in either the 2.4 GHz or 5 GHz frequency range with a maximum range of 984 feet (250 m).

OSI and TCP/IP Data Models

TCP/IP Model	OSI Model
Application	Application Presentation Session
Transport	Transport
Internet	Network
Network Access	Data Link Physical

An architectural model is a common frame of reference for explaining Internet communications and developing communication protocols. It separates the functions of protocols into manageable layers. Each layer performs a specific function in the process of communicating over a network.

The TCP/IP model was created by researchers in the U.S. Department of Defense (DoD). The TCP/IP model is a tool used to help explain the TCP/IP suite of protocols, which is the dominant standard for transporting data across networks. This model has four layers, as shown in Figure 1.

In the early 1980s, the International Standards Organization (ISO) developed the Open Systems Interconnect (OSI) model, which was defined in ISO standard 7498-1, to standardize the way devices communicate on a network. This model has seven layers, as shown in the Figure. This model was a major step forward toward ensuring that there would be interoperability between network devices.

TCP/IP Model

The TCP/IP reference model provides a common frame of reference for the development of the protocols used on the Internet. It consists of layers that perform functions necessary to prepare data for transmission over a network. The chart in the Figure shows the four layers of the TCP/IP model.

TCP/IP Model	Layer	Description
Application	4	Where high-level protocols such as SMTP and FTP operate
Transport	3	Where flow-control and connection protocols exist
Internet	2	Where IP addressing and routing take place
Network Access	1	Where MAC addressing and physical components of network exist

A message begins at the top layer, the Application layer and moves down the TCP/IP layers to the bottom layer, the Network Access layer. Header information is added to the message as it moves down through each layer and is then transmitted. After reaching the destination, the message travels back up through each layer of the TCP/IP model. The header information that was added to the message is stripped away as the message moves up through the layers toward its destination.

Application Protocols

Application layer protocols provide network services to user applications such as web browsers and e-mail programs. Explore some of the more common Internet protocols in the Figure below, the Application layer, to learn more about the protocols that operate in this layer.

HTTPS	Hypertext Transfer Protocol (HTTP)-HTTP governs how files such as text, graphics, sounds, and video are exchanged on the internet or world wide web (WWW). HTTP is an Application layer protocol. A web server runs an HTTP service or daemon. A daemon is a program that service HTTP requests. These requests are transmitted by HTTP client software, which is another name for web browser.
TELNET	Telnet is an application that you can use to access, control, and troubleshoot remote computers and network devices.
FTP	File Transfer Protocol (FTP) is a set of rules governing how files are transferred. FTP allows multiple simultaneous connections to remote file systems.
SMTP	Simple Mail Transport Protocol (SMTP) provides messaging services over TCP/IP and supports most Internet e-mail programs.
DNS	Domain Name System (DNS) translates domain names, such as www.cisco.com, to IP addresses.
HTML	Notepad Hypertext Markup Language (HTML) is a page description language. Web designers use HTML to indicate to web browser software how the page should look. HTML includes tags to indicate boldface type, italics, line breaks, paragraph breaks, hyperlinks, and insertion of tables, among other instructions.

Transport Protocols

Transport layer protocols provide end-to-end management of the data. One of the functions of these protocols is to divide the data into manageable segments for easier transport across the network. Explore each of the protocols in the Figure below, the Transport layer, to learn more about the protocols that operate in this layer.

TCP	Transmission Control Protocol (TCP) is the primary Internet protocol for the reliable delivery of data. TCP includes facilities for end-to-end connection establishment, error detection and recovery, and metering the rate of data flow into the network. Many standard applications, such as e-mail, web browser, file transfer, and telnet, depend on the services of TCP.
UDP	User Datagram Protocol (UDP) offers a connectionless service for delivery of data. UDP uses lower overhead than TCP and doesn't handle issues of reliability. Network management applications, network file system, and simple file transport use UDP.

Internet Protocols

Internet layer protocols operate in the third layer from the top in the TCP/IP model. These protocols are used to provide connectivity between hosts in the network. Explore each of the protocols in the Figure below, the Internet layer, to learn more about the protocols that operate in this layer.

IP	Internet Protocol (IP) provides source and destination addressing, much like the address and return address on a postal envelope. In conjunction with routing protocols, IP provides packet forwarding information from one network to another.
ICMP	Internet Control Message Protocol (ICMP) is used for network testing and troubleshooting. It enables diagnostic and error messages. ICMP echo message are used by the ping application to test if a remote device is reachable.
RIP	Routing In formation Protocol (RIP) operates between router devices to discover paths between networks. In an internet, routers depend on a routing protocol to build and maintain information about how to forward packets toward the

	destination. RIP choose routes based on the distance or hop count to the destination.
ARP	Address Resolution Protocol (ARP) is used to map the MAC address of a node on the network when its IP address is known. End stations as well as routers use ARP to discover MAC addresses.

Network Access Protocols

Network Access layer protocols describe the standards that hosts use to access the physical media. The IEEE 802.3 Ethernet standards and technologies, such as CSMA/CD and 10BASE-T are defined in this layer.

Open System Interconnect (OSI) Model

OSI Model	Layer	Description
Application	7	Responsible for network services to applications
Presentation	6	Transforms data formats to provide a standard interface for the Application layer
Session	5	Establishes, manages and terminates the connections between the local and remote application
Transport	4	Provides reliable transport and flow control across a network
Network	3	Responsible for logical addressing and the domain of routing
Data Link	2	Provides physical addressing and media access procedures
Physical	1	Defines all the electrical and physical specifications for devices

The OSI model is an industry standard framework that is used to divide network communications into seven distinct layers. Although other models exist, most network vendors today build their products using this framework.

A system that implements protocol behavior consisting of a series of these layers is known as a protocol stack. Protocol stacks can be implemented either in hardware or software, or a combination of both. Typically, only the lower layers are implemented in hardware, and the higher layers are implemented in software.

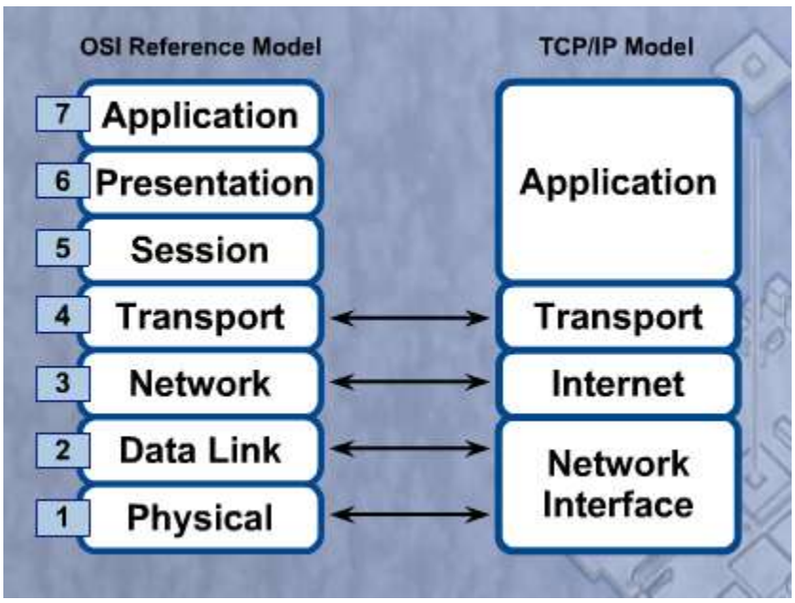
Each layer is responsible for part of the processing to prepare data for transmission on the network. The chart in the Figure shows what each layer of the OSI model does.

In the OSI model, when data is transferred, it is said to virtually travel down the OSI model layers of the sending computer, and up the OSI model layers of the receiving computer.

When a user wants to send data, such as an e-mail, the encapsulation process starts at the Application layer. The Application layer is responsible for providing network access to applications. Information flows through the top three layers and is considered to be data when it gets down to the Transport layer.

At the Transport layer, the data is broken down into more manageable segments, or Transport layer protocol data units (PDUs), for orderly transport across the network. A PDU describes data as it moves from one layer of the OSI model to another. The Transport layer PDU also contains information such as port numbers, sequence numbers, and acknowledgement numbers, which is used for reliable data transport.

OSI vs. TCP/IP



The OSI model and the TCP/IP model are both reference models used to describe the data communication process. The TCP/IP model is used specifically for the TCP/IP suite of protocols and the OSI model is used for development of standard communication for equipment and applications from different vendors.

The TCP/IP model performs the same process as the OSI model, but uses four layers instead of seven. The chart in the Figure shows how the layers of the two models compare.

Configuring NIC and a Modem

A network interface card (NIC) is required to connect to the Internet. The NIC may come preinstalled or you may have to purchase one on your own. In rare cases, you may need to update the driver. You can use the driver disc that comes with the motherboard or adapter card, or you can supply a driver that you downloaded from the manufacturer.

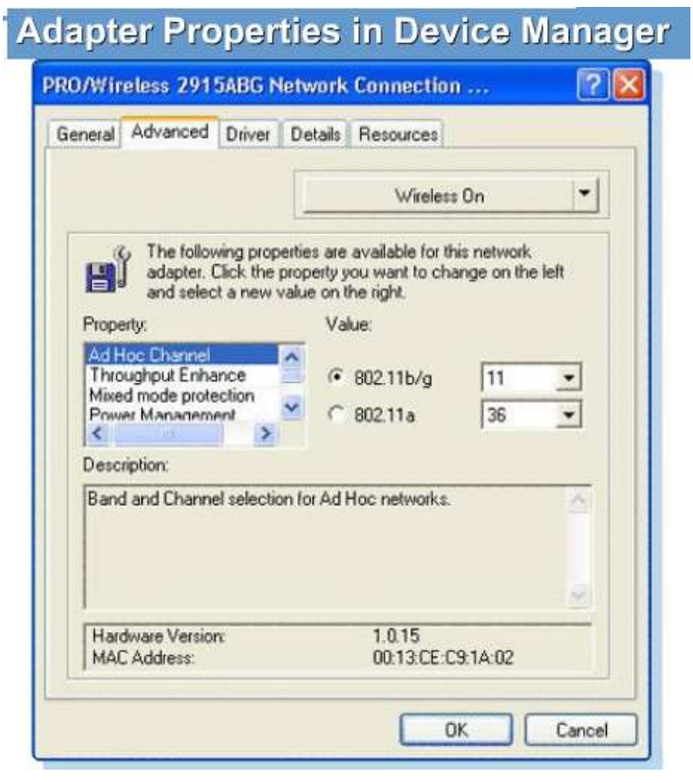
After the NIC and the driver have been installed, you can connect the computer to the network.

In addition to installing a NIC, you may also need to install a modem to connect to the Internet.

Install or Update a NIC Driver

Sometimes, a manufacturer will publish new driver software for a NIC. A new driver may enhance the functionality of the NIC, or it may be needed for operating system compatibility.

When installing a new driver, be sure to disable virus protection software so that



none of the files is incorrectly installed. Some virus scanners detect a driver update as a possible virus attack. Also, only one driver should be installed at a time; otherwise, some updating processes may conflict updating processes may conflict.

A best practice is to close all applications that are running so that they are not using any files associated with the driver update. Before updating a driver, you should visit the manufacturer's website. In many cases, you can download a self-extracting executable driver file that will automatically install or update the driver. Alternatively, you can click the **Update Driver** button in the toolbar of the Device Manager.

The "+" next to the Network adapters category allows you to expand the category and show the network adapters installed in your system. To view and change the properties of the adapter, or update the driver, double-click the adapter. In the adapter properties window select the **Driver** tab.

After the update has been completed, it is a good idea to reboot the computer even if you do not receive a message telling you to reboot. Rebooting the computer will ensure that the installation has gone as planned and that the new driver is working properly. When installing multiple drivers, reboot the computer between each update to make sure that there are no conflicts. This step takes extra time but will ensure a clean installation of the driver.

Uninstall a NIC Driver

If a new NIC driver does not perform as expected after it has been installed, the driver can be uninstalled, or rolled back, to the previous driver. Double-click the adapter in the Device Manager. In the Adapter Properties window, select the **Driver** tab and click **Roll Back Driver**. If there was no driver installed before the update, this option will not be available. In that case, you will need to find a driver for the device and install it manually if the operating system could not find a suitable driver for the NIC.

Attach a Computer to Existing Network

Now that the NIC drivers are installed, you are ready to connect to the network. Plug a network cable, also called an Ethernet patch or straight-through cable, into the network port on the computer. Plug the other end into the network device or wall jack.

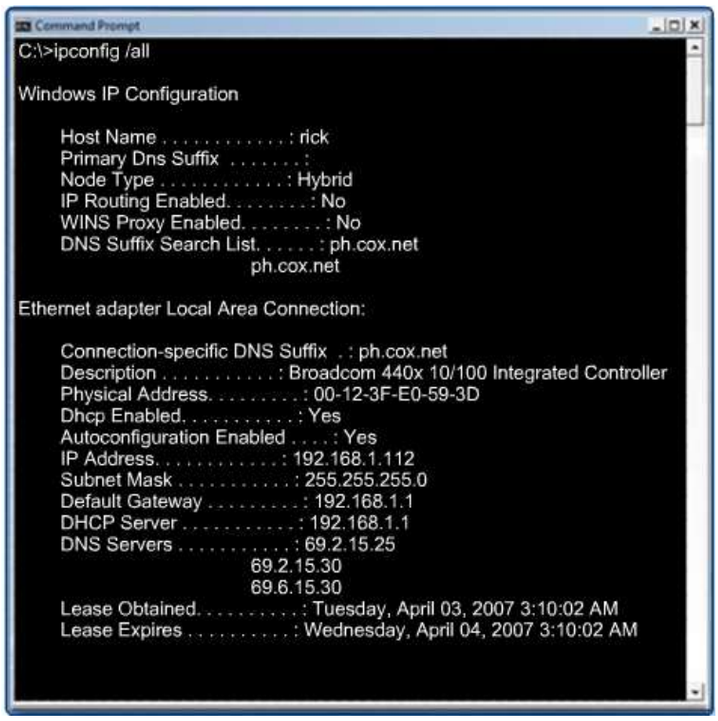
After connecting the network cable, look at the LEDs, or link lights, next to the Ethernet port on the NIC to see if there is any activity. Figure 1 shows network activity on a NIC. If there is no activity, this may indicate a faulty cable, a faulty hub port, or even a faulty NIC. You may have to replace one or more of these devices to correct the problem.

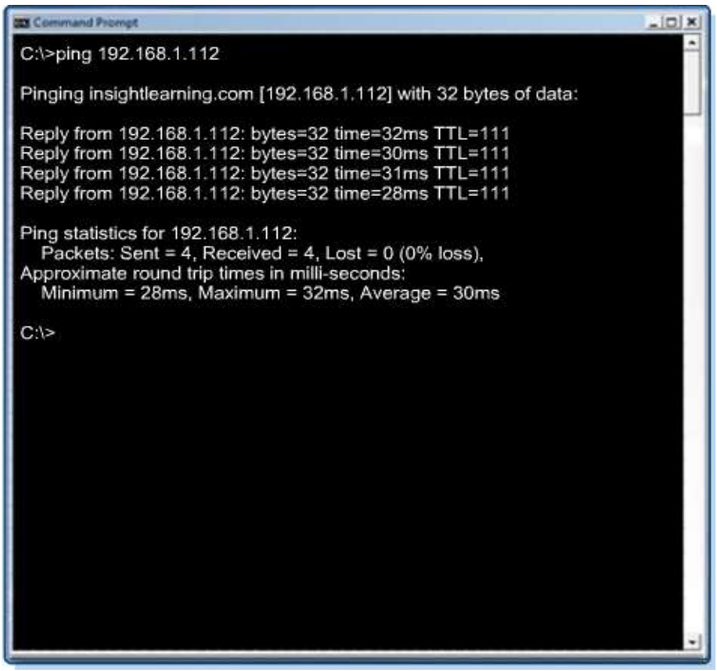
After you have confirmed that the computer is connected to the network and the link lights on the NIC indicate a working connection, the computer will need an IP address. Most networks are set up so that the computer will receive an IP address automatically from a local DHCP server. If the computer does not have an IP address, you will need to enter a unique IP address in the TCP/IP properties of the NIC.

Every NIC must be configured with the following information:

- **Protocols** – The same protocol must be implemented between any two computers that communicate on the same network.
- **IP address** – This address is configurable and must be unique to each device. The IP address can be manually configured or automatically assigned by DHCP.
- **MAC address** – Each device has a unique MAC address. The MAC address is assigned by the manufacturer and cannot be changed.

After the computer is connected to the network, you should test connectivity with the **ping** command. Use the **ipconfig** command, shown in the Figure, to find out what your IP address is. Ping your own IP address to make sure that your NIC is working properly. After you have determined that your NIC is working, ping your default gateway or another computer on your network, as shown in the Figure. A default gateway allows a host to communicate outside of your network. If you have an Internet connection, ping a popular website, such as www.cisco.com. If you can ping an Internet site or another computer on your network successfully, everything is working properly with your connection. If you cannot ping one of these, you will begin troubleshooting the connection.





Describe the Installation of a Modem

A modem is an electronic device that transfers data between one computer and another using analog signals over a telephone line. Examples of modems are shown in the Figure. The modem converts digital data to analog signals for transmission. The modem at the receiving end reconverts the analog signals back to digital data to be interpreted by the computer. The process of converting analog signals to digital and back again is called modulation/demodulation. Modem-based transmission is very accurate, despite the fact that telephone lines can be noisy due to clicks, static, and other problems.

An internal modem plugs into an expansion slot on the motherboard. To configure a modem, jumpers may have to be set to select the IRQ and I/O addresses. No configuration is needed for a plug-and-play modem, which can only be installed on a motherboard that supports plug-and-

play. A modem using a serial port that is not yet in use must be configured. Additionally, the software drivers that come with the modem must be installed for the modem to work properly. Drivers for modems are installed the same way drivers are installed for NICs.

External modems connect to a computer through the serial and USB ports.

When computers use the public telephone system to communicate, it is called dial-up networking (DUN). Modems communicate with each other using audio tone signals. This means that modems are able to duplicate the dialing characteristics of a telephone. DUN creates a Point-to-Point Protocol (PPP) connection between two computers over a phone line.

After the line connection has been established, a "handshaking sequence" takes place between the two modems and the computers. The handshaking sequence is a series of short communications that occur between the two systems. This is done to establish the readiness of the two modems and computers to engage in data exchange. Dial-up modems send data over the serial telephone line in the form of an analog signal. Because the analog signals change gradually and continuously, they can be drawn as waves. In this system, the digital signals are represented by 1s and 0s. The digital signals must be converted to a waveform to travel across telephone lines. They are converted back to the digital form, 1s and 0s, by the receiving modem so that the receiving computer can process the data.

AT Commands

All modems require software to control the communication session. Most modem software uses the Hayes-compatible command set. The Hayes command set is based on a group of instructions that always begins with a set of attention characters (AT), followed by the command characters. These are known as AT commands. The AT command set is shown below.

AT Command	Function
AT	Attention code that precedes all modem action commands.
AP	Dial the phone number, xxxxxxx, using pulse dialing.
ATDT xxxxxxx	Dial the phone number, xxxxxxx, using tone dialing.
ATA	Answer the phone immediately.
ATHO	Hang up the phone immediately.
ATZ	Reset the modem to its power up settings.
ATF	Reset modem parameters and settings to the factory defaults.
AT+++	Break the signal, change from data mode to command mode.
P	Signifies pulse dialing.
T	Signifies tone dialing.
W	Indicates that the modem will wait.

The AT commands are modem control commands. The AT command set is used to issue dial, hang up, reset, and other instructions to the modem. Most user manuals that come with a modem contain a complete listing of the AT command set.

The standard Hayes-compatible code to dial is ATDxxxxxxx. There are usually no spaces in an AT string. If a space is inserted, most modems will ignore it. The "x" signifies the number dialed. There will be seven digits for a local call and 11 digits for a long-distance call. A W indicates that the modem will wait for an outside line, if necessary, to establish a tone before proceeding. Sometimes, a T is added to signify tone dialing or a P is added to signify pulse dialing.

Technology for Connectivity

There are many ways to connect to the Internet. Phone, cable, satellite, and private telecommunications companies offer Internet connections for businesses and home use.

In the 1990s, the Internet was typically used for data transfer. Transmission speeds were slow compared to the high-speed connections that are available today. Most Internet connections were analog modems that used the "plain old telephone system" (POTS) to send and receive data. In recent years, many businesses and home users have switched to high-speed Internet connections. The additional bandwidth allows for transmission of voice and video as well as data.

You should understand how users connect to the Internet and the advantages and disadvantages of different connection types.

Telephone Technologies

There are several WAN solutions available for connecting between sites or to the Internet. WAN connection services provide different speeds and levels of service. Before committing to any type of Internet connection, research all available services to determine the best solution to match the needs of your customer.

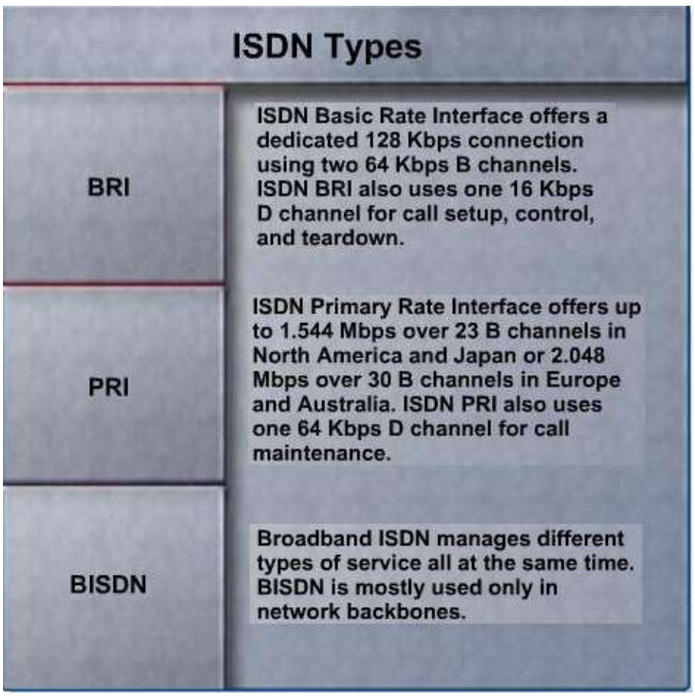
Analog Telephone

This technology uses standard voice telephone lines. This type of service uses a modem to place a telephone call to another modem at a remote site, such as an Internet Service provider. There are two major disadvantages of using the phone line with an analog modem. The first is that the telephone line cannot be used for voice calls while the modem is in use. The second is the limited bandwidth provided by analog phone service. The maximum bandwidth using an analog modem is 56 Kbps, but in reality, it is usually much lower than that. An analog modem is not a good solution for the demands of busy networks.

Integrated Services Digital Network (ISDN)

The next advancement in WAN service is ISDN. ISDN is a standard for sending voice, video, and data over normal telephone wires. ISDN technology uses the telephone wires as an analog telephone service. However, ISDN uses digital technology to carry the data. Because it uses digital technology, ISDN provides higher-quality voice and higher-speed data transfer than traditional analog telephone service.

There are three services offered by ISDN digital connections: Basic Rate Interface (BRI), Primary Rate Interface (PRI), and Broadband ISDN (BISDN). ISDN uses two different types of communications channels. The "B" channel is used to carry the information – data, voice, or video – and the "D" channel is usually used for controlling and signaling, but can be used for data.



Digital Subscriber Line (DSL)
DSL is an "always-on" technology. "Always on" means that there is no need to dial up each time to connect to the Internet. DSL uses the existing copper telephone lines to provide high-speed digital data communication between end users and telephone companies. Unlike ISDN, where the digital data communications replaces the analog voice communications, DSL shares the telephone wire with analog signals.

The telephone company limits the bandwidth of the analog voice on the lines. This limit allows the DSL to place digital data on the phone wire in the unused portion of the bandwidth. This sharing of the phone wire allows voice calls to be placed while DSL is connecting to the Internet.

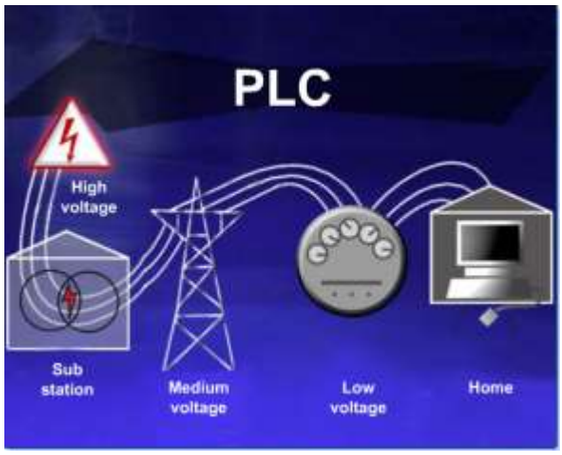
There are two major considerations when selecting DSL. DSL has distance limitations. The phone lines used with DSL were designed to carry analog information. Therefore, the length that the digital signal can be sent is limited and cannot pass through any form of multiplexer used with analog phone lines. The other consideration is that the voice information and the data carried by DSL must be separated at the customer site. A device called a splitter separates the conne**ction to the phones and the connection to the local network devices.**

ADSL	Asymmetric DSL currently is the most common implementation. It has speeds that vary from 384 Kbps to more than 6 Mbps downstream. The upstream speed is typically lower.
HDSL	High Data Rate DSL provides equal bandwidth in both directions. It is 1.544 Mbps in North America and 2.048 Mbps in Europe.
SDSL	Symmetric DSL provides the same speed, up to 3Mbps, for uploads and downloads.
VDSL	Very High Data Rate DSL is capable of bandwidths between 13 and 52 Mbps downstream, and 16 Mbps upstream.
IDSL	ISDN DSL is actually DSL over ISDN lines. It is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire, as well as over other media, with a top speed of 144 Kbps. ISDN is available in areas that do not qualify for other DSL implementations. An ISDN adapter at both ends, user side in place of the modem and service provider, is required. ISDN is generally available in urban areas in the United States and Europe from the local phone company.

Asymmetric Digital Subscriber Line (ADSL)
ADSL is currently the most commonly used DSL technology. ADSL has different bandwidth capabilities in each direction. ADSL has a fast downstream speed – typically 1.5 Mbps.

Downstream is the process of transferring data from the server to the end user. This is beneficial to users who are downloading large amounts of data. The high speed upload rate of ADSL is slower. ADSL does not perform well when hosting a web server or FTP server, both of which involve upload-intensive Internet activities.

Power Line Communication



Power line communication (PLC) is a communication method that uses power distribution wires (local electric grid) to send and receive data.

PLC is known by other names:

- Power Line Networking (PLN)
- Mains Communication
- Power Line Telecoms (PLT)

With PLC, an electric company can superimpose an analog signal over the standard 50 or 60 Hz AC that travels in power lines. The analog signal can carry voice and data signals.

PLC may be available in areas where other high-speed connections are not. PLC is faster than an analog modem, and may cost much less than other high-speed connection types. As this technology matures, it will become more common to find and may increase in speed.

You can use PLC to network computers within your home instead of installing network cabling or wireless technology. PLC connections can be used anywhere there is an electrical outlet. You can control lighting and appliances using PLC without installing control wiring.

Broadband

Broadband is a technique used to transmit and receive multiple signals using multiple frequencies over one cable. For example, the cable used to bring cable television to your home can carry computer network transmissions at the same time. Because the two transmission types use different frequencies, they do not interfere with each other.

Broadband is a signaling method that uses a wide range of frequencies that can further be divided into channels. In networking, the term broadband describes communication methods that transmit two or more signals at the same time. Sending two or more signals simultaneously increases the rate of transmission. Some common broadband network connections include cable, DSL, ISDN, and satellite.

Cable

A cable modem connects your computer to the cable company using the same coaxial cable that connects to your cable television. A cable modem is shown in Figure 1. You

can plug your computer directly into the cable modem, or you can connect a router, switch, hub, or multipurpose network device so that multiple computers can share the connection to the Internet.

DSL

With DSL, the voice and data signals are carried on different frequencies on the copper telephone wires. A filter is used to prevent DSL signals from interfering with phone signals. A DSL filter is shown in Figure 2. Plug the filter into a phone jack and plug the phone into the filter.

The DSL modem does not require a filter. The DSL modem is not affected by the frequencies of the telephone. Like a cable modem, a DSL modem can connect directly to your computer, or it can be connected to a networking device to share the Internet connection with multiple computers.

ISDN

ISDN is another example of broadband. ISDN uses multiple channels and can carry different types of services; therefore, it is considered a type of broadband. ISDN can carry voice, video, and data.

Satellite

Broadband satellite is an alternative for customers who cannot get cable or DSL connections. A satellite connection does not require a phone line or cable, but uses a satellite dish for two-way communication. Download speeds are typically up to 500 Kbps; uploads are closer to 56 Kbps. It takes time for the signal from the satellite dish to relay to your Internet Service Provider (ISP) through the satellite orbitting the Earth.

People who live in rural areas often use satellite broadband because they need a faster connection than dial-up and no other broadband connection is available.

VOIP

Voice over IP (VoIP) is a method to carry telephone calls over the data networks and Internet. VoIP converts the analog signals of our voices into digital information that is transported in IP packets. VoIP can also use an existing IP network to provide access to the public switched telephone network (PSTN).

When using VoIP, you are dependent on an Internet connection. This can be a disadvantage if the Internet connection experiences an interruption in service. When a service interruption occurs, the user cannot make phone calls.

Adapted and Compiled from:

CCNA IT Essential, “PC Hardware and Software” version 4.0, Cisco Networking Academy
CCNA Discovery 1, “Networking for Home and Small Businesses”, Cisco Networking Academy
CCNA Discovery 2, “Working at a Small-to-Medium Business of ISP”, Cisco Networking Academy
CCNA Exploration 1, “Network Fundamentals”, Cisco Networking Academy
Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide, Cisco Press