DATA COMMUNICATIONS AND COMPUTER NETWORKS

Media Interference

Depending on where network cabling (commonly called media) is installed, interference can be a major consideration. Two types of media interference can adversely affect data transmissions over network media: electromagnetic interference (EMI) and crosstalk.

EMI is a problem when cables are installed near electrical devices, such as air conditioners or fluorescent light fixtures. If a network medium is placed close enough to such a device, the signal within the cable might become corrupt. Network media vary in their resistance to the effects of EMI. Standard unshielded twisted pair (UTP) cable is susceptible to EMI, whereas fiber cable, with its light transmissions, is resistant to EMI. When deciding on a particular medium, consider where it will run and the impact EMI can have on the installation. A second type of interference is crosstalk. Crosstalk refers to how the data signals on two separate media interfere with each other. The result is that the signal on both cables can become corrupt. As with EMI, media varies in its resistance to crosstalk, with fiber-optic cable being the most resistant.

Attenuation

Attenuation refers to the weakening of data signals as they travel through a medium. Network media vary in their resistance to attenuation. Coaxial cable generally is more resistant than UTP, STP is slightly more resistant than UTP, and fiber-optic cable does not suffer from attenuation at all. That’s not to say that a signal does not weaken as it travels over fiber-optic cable, but the correct term for this weakening is chromatic dispersion rather than attenuation.

It’s important to understand attenuation or chromatic dispersion and the maximum distances specified for network media. Exceeding a medium’s distance without using repeaters can cause hard-to-troubleshoot network problems. A repeater is a network device that amplifies data signals as they pass, allowing them to travel farther. Most attenuation- or chromatic dispersion-related difficulties on a network require using a network analyzer to detect them.

Data Transmission Rates

One of the more important media considerations is the supported data transmission rate or speed. Different media types are rated to certain maximum speeds, but whether they are used to this maximum depends on the networking standard being used and the network devices connected to the network.

Transmission rates normally are measured by the number of data bits that can traverse the medium in a single second. In the early days of data communications, this measurement was expressed in bits per second (bps), but today’s networks are measured in Mbps (megabits per second) and Gbps (gigabits per second).

The different network media vary greatly in the transmission speeds they support. Many of today’s application-intensive networks require more than the 10Mbps offered by the older networking standards. In some cases, even 100Mbps, which is found in many modern LANs, is simply not enough to meet current network needs. For this reason, many organizations deploy 1Gbps networks, and some now even go for 10Gbps implementations.

Network Media

Whatever type of network is used, some type of network medium is needed to carry signals between computers. Two types of media are used in networks: cable-based media, such as twisted pair, and the media types associated with wireless networking, such as radio waves.

In networks using cable-based media, there are three basic choices:

- Twisted pair
- Coaxial
- Fiber-optic

Twisted pair and coaxial cables both use copper wire to conduct the signals electronically; fiber-optic cable uses a glass or plastic conductor and transmits the signals as light.
For many years, coaxial was the cable of choice for most LANs. Today, twisted pair has proven to be far and away the cable medium of choice, thus retiring coaxial to the confines of storage closets. Fiber-optic cable has also seen its popularity rise, but because of cost it has been primarily restricted to use as a network backbone where segment length and higher speeds are needed. Fiber is now increasingly common in server room environments as a server-to switch connection method, and in building-to-building connections in what are called metropolitan area networks (MANs).

Twisted-Pair Cabling

Twisted-pair cabling has been around for a very long time. It was originally created for voice transmissions and has been widely used for telephone communication. Today, in addition to telephone communication, twisted pair is the most widely used medium for networking.

The popularity of twisted pair can be attributed to the fact that it is lighter, more flexible, and easier to install than coaxial or fiber-optic cable. It is also cheaper than other media alternatives and can achieve greater speeds than its coaxial competition. These factors make twisted pair the ideal solution for most network environments.

Two main types of twisted-pair cabling are in use today: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP). UTP is significantly more common than STP and is used for most networks. Shielded twisted pair is used in environments in which greater resistance to EMI and attenuation is required. The greater resistance comes at a price, however. The additional shielding, plus the need to ground that shield (which requires special connectors), can significantly add to the cost of a cable installation of STP.

STP provides the extra shielding by using an insulating material that is wrapped around the wires within the cable. This extra protection increases the distances that data signals can travel over STP but also increases the cost of the cabling.

- Category 3: Data-grade cable that can transmit data up to 10Mbps with a possible bandwidth of 16MHz. For many years, Category 3 was the cable of choice for twisted-pair networks. As network speeds pushed the 100Mbps speed limit, Category 3 became ineffective.
- Category 4: Data-grade cable that has potential data throughput of 16Mbps. Category 4 cable was often

implemented in the IBM Token- Ring Network. Category 4 cable is no longer used.

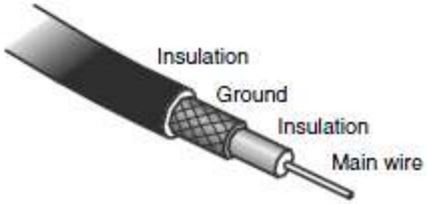
- Category 5: Data-grade cable that typically was used with Fast Ethernet operating at 100Mbps with a transmission range of 100 meters. Although Category 5 was a popular media type, this cable is an outdated standard. Newer implementations use the 5e standard. Category 5 provides a minimum of 100MHz of bandwidth. Category 5, despite being used primarily for 10/100 Ethernet networking, can go faster. The IEEE 802.11ae standard specifies 1000Mbps over Category 5 cable.
- Category 5e: Data-grade cable used on networks that run at 10/100Mbps and even up to 1000Mbps. Category 5e cabling can be used up to 100 meters, depending on the implementation and standard used. Category 5e cable provides a minimum of 100MHz of bandwidth.
- Category 6: High-performance UTP cable that can transmit data up to 10Gbps. Category 6 has a minimum of 250MHz of bandwidth and specifies cable lengths up to 100 meters with 10/100/1000Mbps transfer, along with 10Gbps over shorter distances. Category 6 cable typically is made up of four twisted pairs of copper wire, but its capabilities far exceed those of other cable types. Category 6 twisted pair uses a longitudinal separator, which separates each of the four pairs of wires from each other. This extra construction significantly reduces the amount of crosstalk in the cable and makes the faster transfer rates possible.
- Category 6a: Also called augmented 6. Offers improvements over Category 6 by offering a minimum of 500MHz of bandwidth. It specifies transmission distances up to 100 meters with 10Gbps networking speeds.

Categories and the speeds they support in common network implementations.

Category	Common Application
1	Analog voice applications
2	1Mbps
3	16Mbps
4	20Mbps
5	100Mbps
5e	1000Mbps
6	10/100/1000Mbps plus 10Gbps
6a	10Gbps and beyond networking

Coaxial

Coaxial cable, or coax as it is commonly called, has been around for a long time. Coax found success in both TV signal transmission and network implementations. As shown in the figure, coax is constructed with a copper core at the center that carries the signal, plastic insulation, braided metal shielding, and an outer plastic covering. Coaxial cable is constructed in this way to add resistance to attenuation (the loss of signal strength as the signal travels over distance), crosstalk (the degradation of a signal, caused by signals from other cables running close to it), and EMI. Two types of coax are used in networking: thin coax, also known as thinnet, and thick coax, also known as thicknet. Neither is particularly popular anymore, but you are most likely to encounter thin coax. Thick coax was used primarily for backbone cable. It could be run through plenum spaces because it offered significant resistance to EMI and crosstalk and could run in lengths up to 500 meters. Thick coax offers speeds up to 10Mbps, far too slow for today’s network environments.



Thin Coax

Thin coax is much more likely to be seen than thick coax in today’s networks, but it isn’t common. Thin coax is only .25 inches in diameter, making it fairly easy to install. Unfortunately, one of the disadvantages of all thin coax types is that they are prone to cable breaks, which increase the difficulty when installing and troubleshooting coaxial-based networks.

Several types of thin coax cable exist, each of which has a specific use. The table below summarizes these categories.

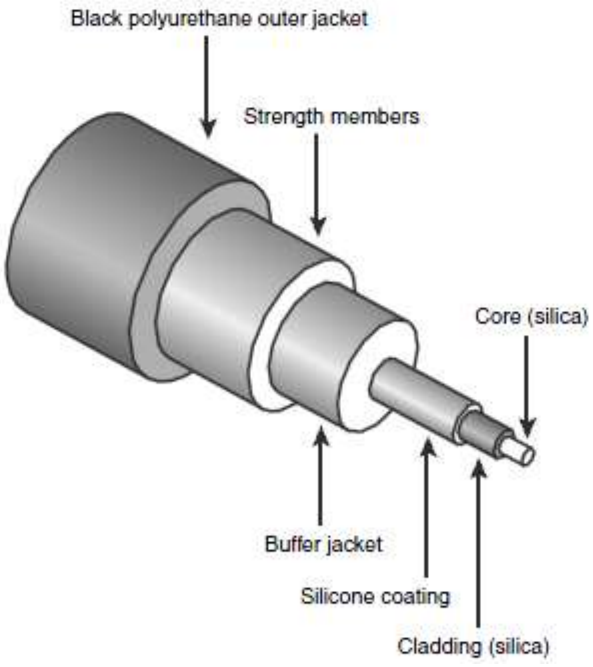
RG-59 /U	Used to generate low-power video connections. The RG- 59 cable cannot be used over long distances because of its high-frequency power losses. In such cases, RG-6 cables are used instead.
RG-58 /U	Has a solid copper core. Used for radio communication and thin Ethernet (10Base2).
RG-58 A/U	Has a stranded wire core. Used for radio communication and thin Ethernet (10Base2).
RG-58 C/U	Used for military specifications.
RG-6	Often used for cable TV and cable modems.

Fiber-Optic Cable

In many ways, fiber-optic media addresses the shortcomings of copper-based media. Because fiber-based media use light transmissions instead of electronic pulses, threats such as EMI, crosstalk, and attenuation become non-issues. Fiber is well suited for the transfer of data, video, and voice transmissions. In addition, fiber-optic is the most secure of all cable media. Anyone trying to access data signals on a fiber-optic cable must physically tap into the medium. Given the composition of the cable, this is a particularly difficult task.

Unfortunately, despite the advantages of fiber-based media over copper, it still does not enjoy the popularity of twisted-pair cabling. The moderately difficult installation and maintenance procedures of fiber often require skilled technicians with specialized tools. Furthermore, the cost of a fiber-based solution limits the number of organizations that can afford to implement it. Another sometimes hidden drawback of implementing a fiber solution is the cost of retrofitting existing network equipment. Fiber is incompatible with most electronic network equipment. This means that you have to purchase fiber-compatible network hardware.

As shown in the figure, fiber-optic cable is composed of a core glass fiber surrounded by cladding. An insulated covering then surrounds both of these within an outer protective sheath.



Two types of fiber-optic cable are available:

- Multimode fiber: Many beams of light travel through the cable, bouncing off the cable walls. This strategy actually weakens the signal, reducing the length and speed at which the data signal can travel.
- Single-mode fiber: Uses a single direct beam of light, thus allowing for greater distances and increased transfer speeds.

Some of the common types of fiber-optic cable include the following:

- 62.5-micron core/125-micron cladding multimode
- 50-micron core/125-micron cladding multimode
- 8.3-micron core/125-micron cladding single mode

In the ever-increasing search for bandwidth that will keep pace with the demands of modern applications, fiber-optic cables are sure to play a key role.

Media Connectors

A variety of connectors are used with the associated network media. Media connectors attach to the transmission media and allow the physical connection into the computing device.

BNC Connectors

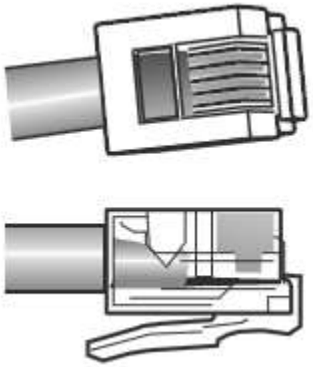
BNC connectors are associated with coaxial media and 10Base2 networks. BNC connectors are not as common as they once were, but they still are used on some networks, older network cards, and older hubs. Common BNC connectors include a barrel connector, T-connector, and terminators. The following figures show two terminators and two T-connectors.

RJ-11 Connectors

RJ- (registered jack) 11 connectors are small plastic connectors used on telephone cables. They have capacity for six small pins. However, in many cases, not all the pins are used. For example, a standard telephone connection uses only two pins, and a cable used for a DSL modem connection uses four. RJ-11 connectors are somewhat similar to RJ-45 connectors, which are discussed next, although they are a little smaller. Both RJ-11 and RJ-45 connectors have a small plastic flange on top of the connector to ensure a secure connection. The figure shows two views of an RJ-11 connector.

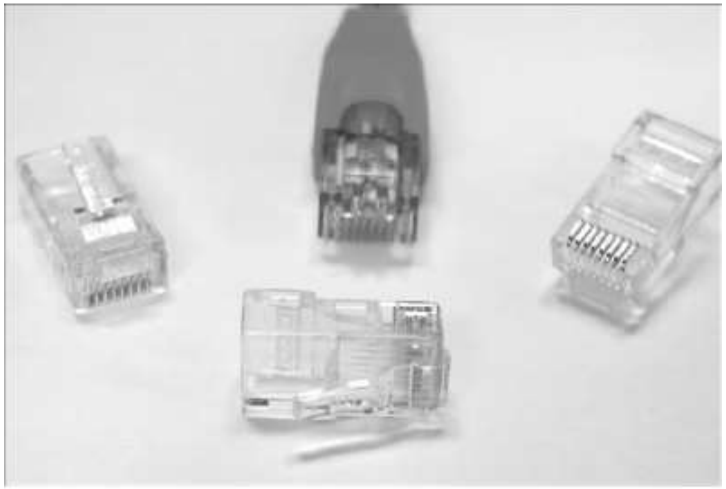
RJ-45 Connectors

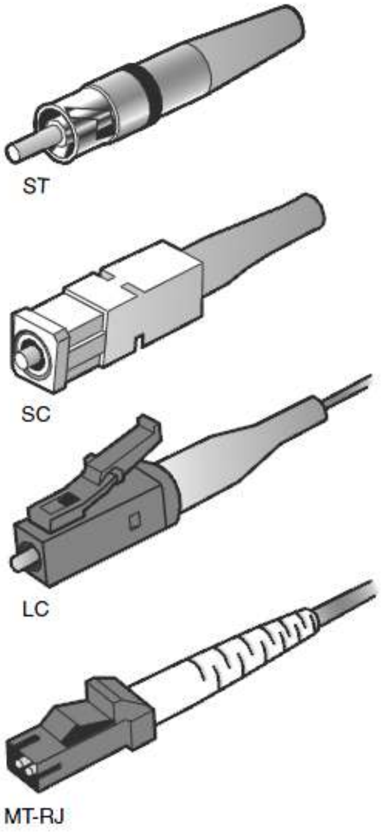
RJ-45 connectors, shown in the figure, are the ones you are most likely to encounter in your network travels. RJ-45 connectors are used with twisted-pair cabling, the most prevalent network cable in use today. RJ-45 connectors resemble the aforementioned RJ-11 phone jacks, but they support up to eight wires instead of the six supported by RJ-11 connectors. RJ-45 connectors are also larger.



F-Type Connectors and RG-59 and RG-6

F-Type connectors are screw-on connections used to attach coaxial cable to devices. This includes RG-59 and RG-6 cables. In the world of modern networking, F-Type connectors are most commonly associated with connecting Internet modems to cable or satellite Internet service providers' (ISPs') equipment. However, they are also used to connect to some proprietary peripherals.





The ST connector uses a half-twist bayonet type of lock.

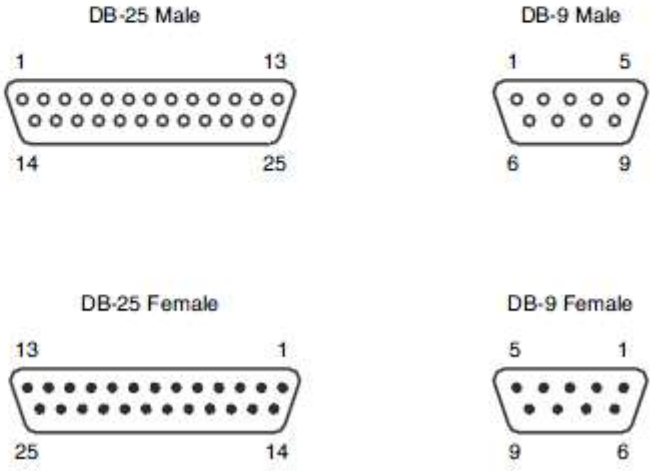
The SC uses a push-pull connector similar to common audio and video plugs and sockets.

LC connectors have a flange on top, similar to an RJ-45 connector, that aids secure connection.

MT-RJ is a popular connector for two fibers in a very small form factor.

RS-232 Standard

RS-232 (Recommended Standard 232) is a TIA/EIA standard for serial transmission between computers and peripheral devices such as modems, mice, and keyboards. The RS-232 standard was introduced way back in the 1960s and is still used today. However, peripheral devices are more commonly connected using USB or wireless connections. RS-232 commonly uses a 25-pin DB-25 connector or a nine-pin DB-9 connector. The figure below shows an example ofRS-232 standard connectors.

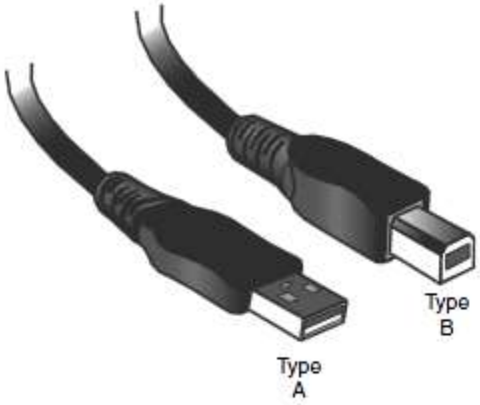


Serial connectors need to attach to a serial cable. Serial cables often use four to six wires to attach to the connectors. Similar to other cable types, they can come in both an unshielded and shielded type. Shielding reduces interference and EMI for the cable. The distance that a length of serial cable can run varies somewhat. It depends on the characteristics of the serial port and, of course, the quality of the serial cable. The RS-232 standard specifies serial cable distances up to 50 feet and a transfer speed up to 20kbps. Other serial standards increase this range and speed.

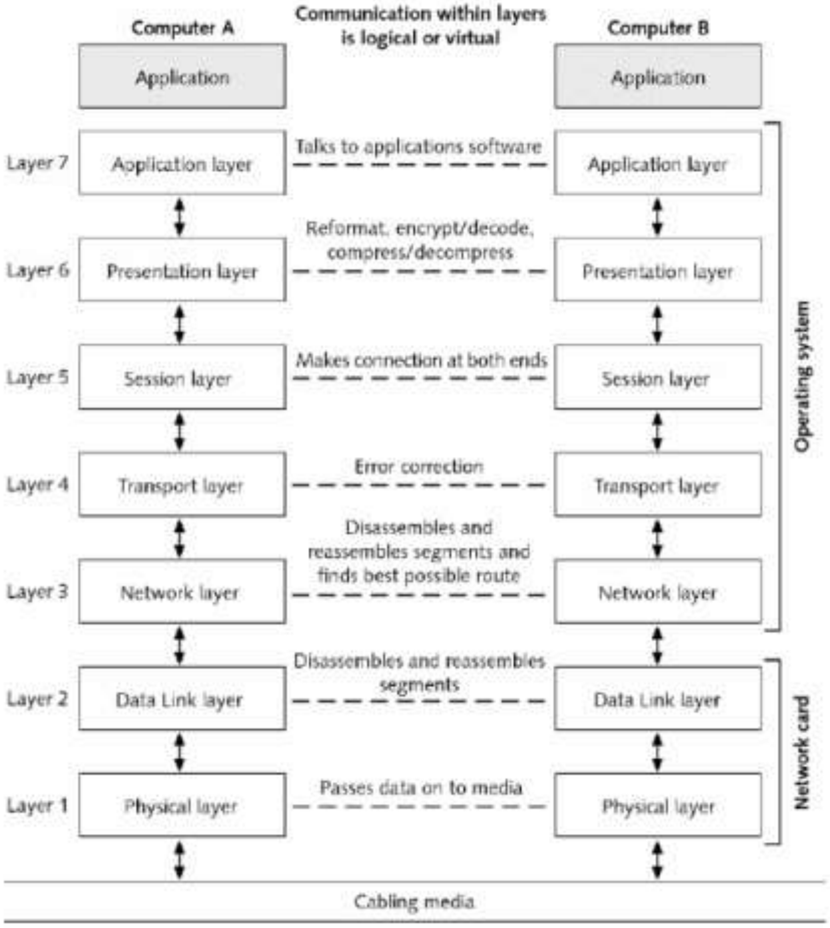
Universal Serial Bus (USB)

Universal Serial Bus (USB) ports are now an extremely common sight on both desktop and laptop computer systems. Like IEEE 1394, USB is associated more with connecting consumer peripherals such as MP3 players and digital cameras than with networking. However, many manufacturers now make wireless network cards that plug directly into a USB port. Most desktop and laptop computers have between two and four USB ports, but USB hubs are available that provide additional ports if required.

A number of connectors are associated with USB ports, but the two most popular are Type A and Type B. Type A connectors are the more common of the two and are the type used on PCs. Although many peripheral devices also use a Type A connector, an increasing number now use a Type B.



The Open Systems Interconnection (OSI) model is a standard means of describing a network operating system by defining it as a series of layers, each with specific input and output. It describes a theoretical model of what happens to information being sent from one computer to another on a network. The sending computer works from the Application layer down, and the receiving computer works on the transmitted data from the Physical layer up. The OSI model was developed by the International Standards Organization (ISO) and has seven layers that are numbered in order from the bottom (Layer 1) to the top (Layer 7). (See figure below)



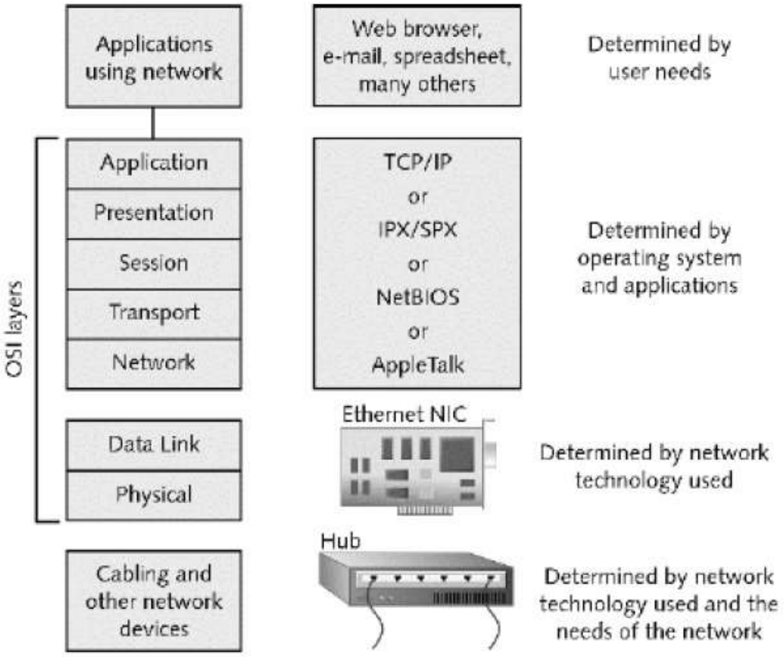
The names of the various layers, starting from the top, are as follows:

- Layer 7—Application layer (top layer), the layer in which applications on a network node (computer) access network services, such as file transfers, electronic mail, and database access.
- Layer 6—Presentation layer, the layer that translates application layer data to an intermediate form that provides security, encryption, and compression for the data.
- Layer 5—Session layer, the layer that establishes and controls data communication between applications operating on two different computers, regulating when each can send data and how much.
- Layer 4—Transport layer, the layer that divides long communications into smaller data packages, handles error recognition and correction, and acknowledges the correct receipt of data.
- Layer 3—Network layer, the layer that addresses data messages, translates logical addresses into actual physical addresses, and routes data to addresses on the network.
- Layer 2—Data Link layer, the layer that packages bits of data from the physical layer into frames (logical, structured data packets), transfers them from one computer to another, and receives acknowledgement from the addressed computer.
- Layer 1—Physical layer (bottom layer), the layer that transmits bits (binary digits) from one computer to another and regulates the transmission stream over a medium (wire, fiber optics, or radio waves).

All parts of network operating systems function in one of these seven layers. If you can visualize the layer in which an operating system functions, you have a clearer understanding of how it relates to the rest of the network operating system.

The OSI model applied to local area networking

The applications, operating systems, and network technology you choose determine how the OSI model is applied to your network.


Applications using network
Web browser, e-mail, spreadsheet, many others
Determined by user needs
Application
Presentation
Session
Transport
Network
TCP/IP
or
IPX/SPX
or
NetBIOS
or
AppleTalk
Determined by operating system and applications
OSI layers
Data Link
Physical
Ethernet NIC
Determined by network technology used
Cabling and other network devices
Hub
Determined by network technology used and the needs of the network