PDHonline Course E175 (8 PDH)

Introduction to Computer Networking

Instructor: Dale W. Callahan, Ph.D., P.E. and Lea B. Callahan, P.E.

2012

PDH Online | PDH Center

5272 Meadow Estates Drive
Fairfax, VA 22030-6658
Phone & Fax: 703-988-0088
www.PDHonline.org
www.PDHcenter.com

An Approved Continuing Education Provider

Introduction to Computer Networking

Dale Callahan, Ph.D., P.E.

MODULE 2: Definitions, Hardware, and Topologies

2.1 Introduction

This module begins by addressing the basic definitions used in computer networks. These include Local Area Networks (LAN) and Wide Area Networks (WAN), protocols, topologies, and data packets. Then a few essential pieces of networking equipment are covered. In the last part of this module we will cover the one thing all texts on networking include, the Open Systems Interconnect (OSI) reference model. The module will conclude with a description of how the OSI model relates to the real world of the Internet.

2.2 Background

A network represents the fundamental element of communication, which most of us have mastered the use of since 2 years old – that is word-of-mouth communication. In a conversation, ideas are communicated from one person to another. Using the telephone, we are able to do this communication over long distances.

Computer networks are simply extensions of this concept. They allow computers to remotely share information between themselves. Therefore, we will define a computer network as a system of computers and computer devices linked by cables and/or radio waves.

2.3 Definitions

2.3.1 LAN and WAN

The first factor used to classify networks is the physical relationship of the devices. If the computer network is of a local nature, such as within a single building, or perhaps the same floor of a building, than we can define this as a local area network, or LAN. Now if multiple LANs are interconnected within a metropolitan area, such as a company connecting computers of multiple offices together, we would call this a Metropolitan Area Network (MAN). Extending this even further, such as connecting LANs and MANs in multiple cities together, we would have what is known as a wide area network, or WAN. The most prominently known WAN is the Internet. The differences between LANs, MANs, and WANs can become difficult to see, and often the three terms run together. In fact, the term MAN is almost never used anymore, as most all networks are called either LANs or WANs. Typical LAN and WAN configurations are shown in Figures 1 and 2 respectively. Figure 2 indicates several LANs connected to each other through an Asynchronous Transfer Mode (ATM) switch. The term ATM refers to a protocol used by devices within a network and will be discussed later.

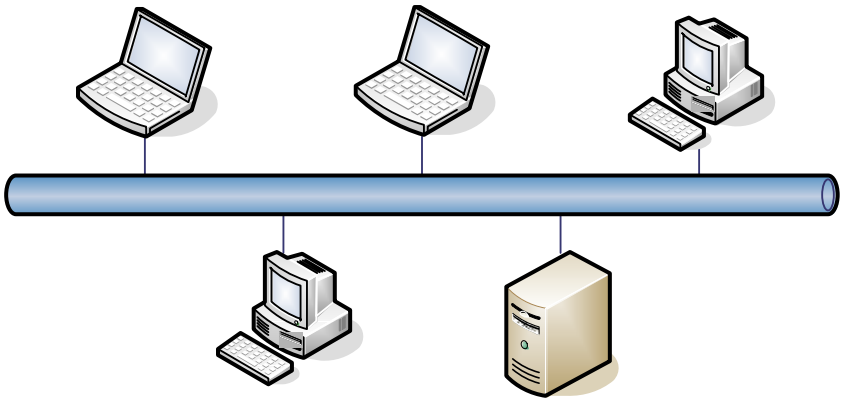

Figure 1. Local Area Network

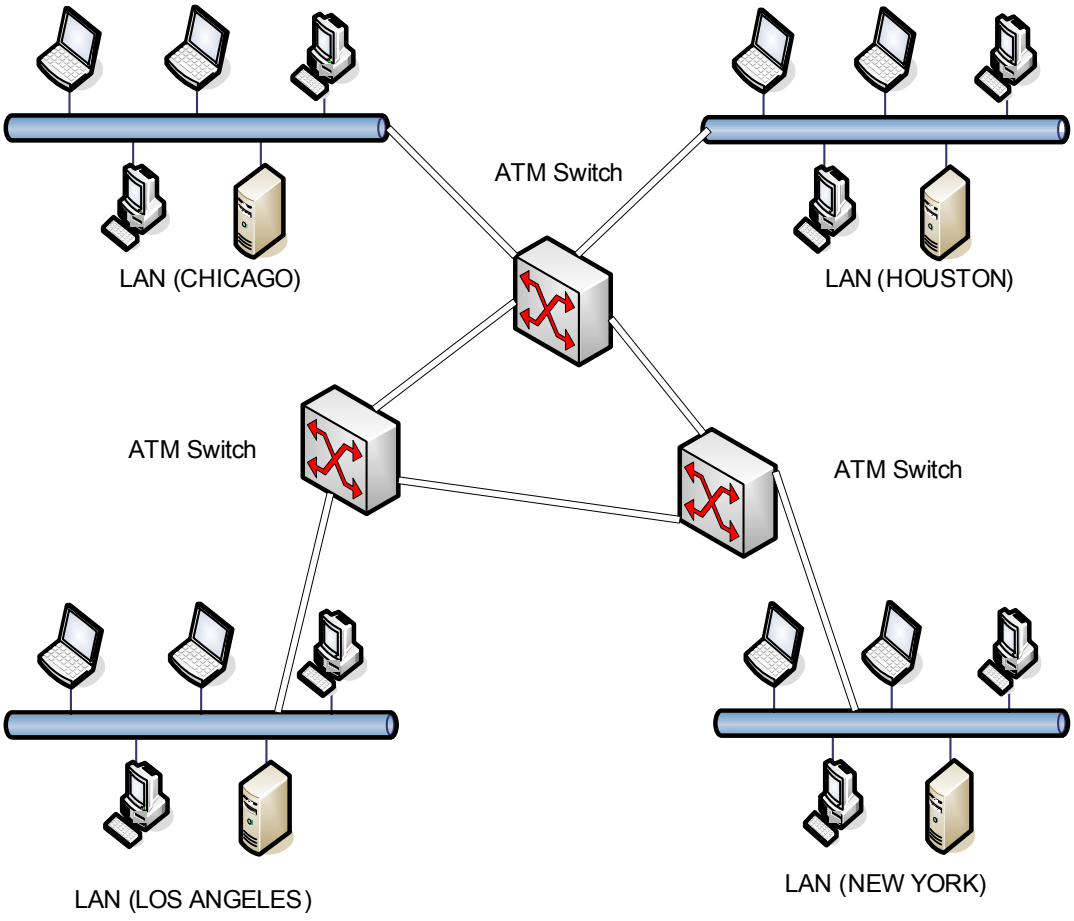

Figure 2. Wide Area Network

2.3.2 Protocols

A second factor used to classify computer networks is protocol. A protocol specifies how networks communicate, much like a language and set of customs for a group of people. The protocol defines the layout of the packets. A packet is a small piece of data that is formatted for transmission over a computer network. The way packets are put together in a computer network is defined by the protocol. Like addresses on an envelope that is being sent through the mail, computer data is put in a format that allows the messages to be sent over the networks and arrive at the correct destination.

For example, a letter written from a person in Russia to a Russian friend living in the United States might be written in their native Russian language. The Russian script is the native protocol that these two people understand. However, to get the letter to the correct address in the United States, the envelope would be addressed in English. Furthermore, as you well know, to get the letter to the correct destination the envelope must be addressed in a fashion that meets a specified standard. The "send-to" address must be in the middle and must contain the street name, city, state, and zip code. Then, the correct postage must be put in the top right hand corner. (All of the rules for getting the mail to the correct address are another protocol.) Now notice that we have placed a letter, which we will call the data, which is formatted by a certain protocol, in an envelope written to conform to yet another protocol. One protocol has to do with the data itself, while the other has the purpose of routing the letter to the correct location. This placing one protocol inside another is also common in computer networks. A model of this is demonstrated by the OSI model, which will be described later.

2.3.3 Topologies

A third property of LANs is the topology. Topology describes the way in which computers are tied together on a network – both the physical layout and the paths the packets travel. If topology is changed in a network, you have moved from one LAN to another. An example of this would be two floors of a building. One floor might be connected in a star fashion while the other is connected in a ring fashion. The interconnection between these two networks indicates the interconnection of two LANs, therefore making a MAN or a WAN. Special equipment is often needed to tie these LANs together.

The three basic topologies for LANs are bus, ring, and star. First, let us define a node and a station. A node and a station are terms that are often used interchangeably in networking. Both refer to devices on the network, such as a computer or a printer and other devices such as routers, which we will discuss later.

The bus topology, shown in Figure 3, uses a cable connecting from one node to another. Like a chain, the entire operation of the system depends on every link being connected properly. A terminator is placed at both ends of the bus to signal the end of the chain. When the message gets sent out from one node on a bus, all nodes see the message as it passes. Each device on the network is responsible for determining if the data packets belong to it or another device. The terminator stops the packets, and prevents them from electrically being bounced off the end like an echo, since the network devices would see this as yet another set of data packets. While the

bus network is simple and cheap, it is only useful for small networks since it is difficult to isolate a problem if one of the connections is bad. (Imagine having 100+ machines and having to go check each connection to determine where the network problem originates.)

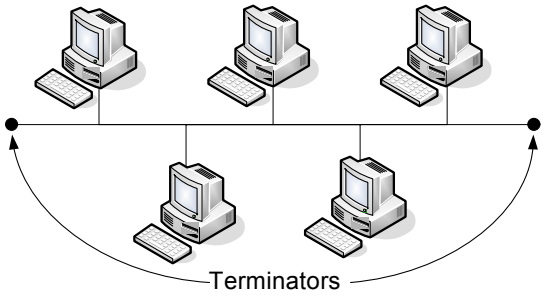

Figure 3. Bus topology

The ring topology, shown in Figure 4, provides a continuous path around the network, much like an interstate loop around major cities. Data traffic is put on the ring and sent from node to node. Each device looks at the intended address, and if the data belongs to this device it will accept it for processing. Either way, the data is sent to all nodes on the ring until it arrives back at the originating node.

A ring network provides fair access to each station and can cover a larger area as compared to other topologies. Each device on the ring acts as a repeater, which regenerates the received signal before transmission. While there are some advantages to a ring such as when it comes to finding a trouble spot, the ring is more expensive to implement than the bus because it will usually require more cable and special network equipment at the start. Telecommunications companies who put fiber rings around a city to carry a massive amount of telephone and data traffic often use this option. The great advantage to them here is that if someone cuts a cable in one spot, they can easily find the problem and there is still another path to get from point A to point B by sending the data in the other direction. In the bus topology, if a cable is cut between point A and B, there is no alternate path to communicate between these nodes.

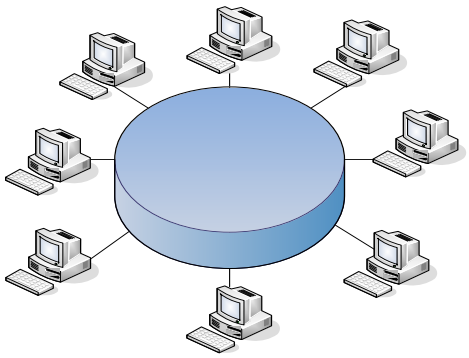

Figure 4. Ring topology

The star topology, shown in Figure 5, is by far the most popular today. (Ring and bus are only used for special cases.) Star uses a central point, or hub, to interconnect the nodes of a network. The telephone system was built on this concept, where each telephone user was connected back to their local central office over a pair of wires. Therefore, to talk to your next-door neighbor, the voice traffic went from your house, to the central office, then back to your neighbor's house. While the star topology was a bit more expensive than the bus topology for LANs, reduction in the costs of the hub devices have made this option one of the cheapest for anything other than a very small network. Furthermore, like the bus, it does not require a terminator. Like the ring, the star is easier to manage and troubleshoot. Each node has its own cable coming out of the hub, so damage to this one cable does not affect the other cables in the network.

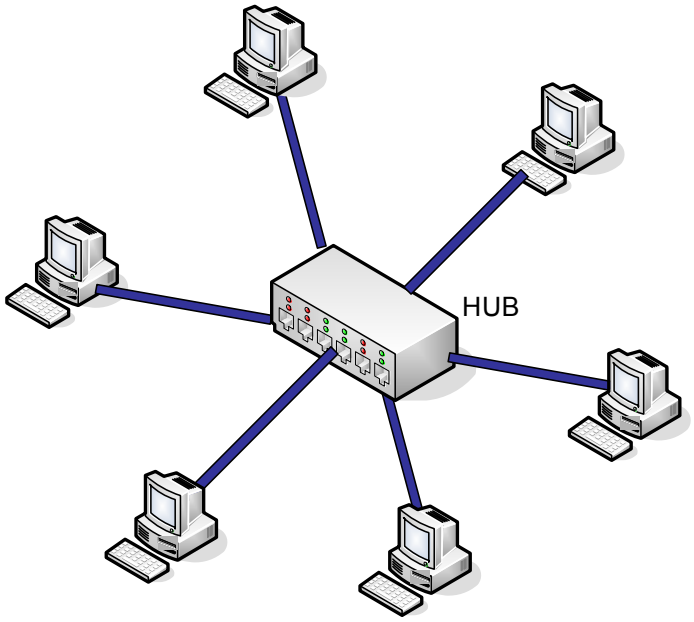

Figure 5. Star topology

2.3.4 Data Packets

A data packet is a collection of bits that will be sent over some medium, such as a cable. A collection of data bits into some orderly form would be called a packet. While the bits represent voltage levels, which in turn are used to represent ones and zeros, packets are used to provide a higher level of information. Packets will include information about network routing as well as the sending and receiving addresses of the data. Another term often used to present packets is frames. A frame is a collection of packets and its size varies based on the specific transmission conditions agreed between the communicating stations.

The way in which packets are put together to allow communication defines the protocol – much like the way people put together letters to make words defines a language. These protocols are agreed on standards that allow two computers to speak the same language and therefore communicate with each other.

2.4 Hardware

2.4.1 Introduction

Now that we have covered some basic concepts, let's go over the things we will actually be able to see in most any network – the media (or cables) and the cards that go in the computer. These media interfaces make up the most basic level of communication, what we will see later as providing the OSI model Layer 1 communication. The four major types of communication media are coaxial cables, twisted pair cables, fiber optic cables, and wireless. The most common among these is the twisted pair cable.

2.4.2 Media

Coaxial cables, usually called coax, are what most television cable companies use inside your house. Therefore, the cable connecting your TV to the cable company and your TV to your VCR are probably coax. The coax used for data communications and LANs is different from the coax on your television, therefore when you buy cable for LANs you need to avoid television cable. While you might be able to make it fit physically, TV coax offers more resistance to the flow of electric current than data coax, which makes it unsuitable for networking purposes. In the data world, coax comes in two varieties, thick and thin. Therefore we will often refer to a network as thicknet or a thinnet, depending on the type of coax used. If coax is used, it is probably the thin type. Figure 6 shows the construction of a typical coax cable.

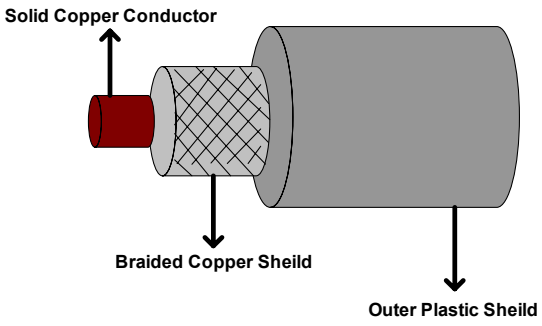

Figure 6. Coaxial cable

Thicknet cable is actually RG-8 (RG stands for radio grade) and is quite a bit thicker than the cable used for TV. The Institute of Electrical and Electronics Engineers (IEEE) standards state that the maximum distance a RG-8 cable can be run between repeaters (which regenerate the signal and has a similar function to an amplifier in the analog world) is 500 meters. Therefore, since the typical application of data networks is 10 Mbps (10 megabits per second, or 10 million bits per second) Ethernet, this thicknet cable is often referred to as 10Base5, where the 10 indicates a 10Mbps transmission rate and the 5 indicates the number of 100 meter lengths between repeaters. Ethernet will be covered in more detail in module 3.

Thin coax cable is known as RG-58A/U, or simply 10Base2. (Can you guess what the 2 means?) Being much thinner and more flexible, it is easier to work with and less expensive. Thin coax is what many people used to have running in their office or their homes as the simple way to interconnect two or three computers. (Rarely seen now.) The connectors on thin coax are known as BNC, for bayonet nut connector. The BNC is connected to a computer's Network Interface Card (NIC) using a BNC T-connector. The T-connector allows the cable to be connected to the computer and then continue on to the next computer. In this fashion, the thin coax is usually used in a simple bus topology, where one cable is sent from one computer to another until the last computer on the line has been reached. At the end of the line, a terminator must be used, as we discussed in the section on topologies. Figure 7 shows these BNC type connectors.

Figure 7. BNC Connector, Terminator, and T-Connector
Courtesy of Homestead [1]

The most popular cable is the twisted pair. It is popular since it is flexible, can be run up to 100 Mbps, and is easier to use in a star network. A twisted pair cable is the same type of cable that has been used to transmit telephone calls for years. In fact, the telephone cable coming into your house is probably a 4-wire twisted pair cable. The modular connector you use to plug your telephone into the jack is called Registered Jack-11 (RJ-11). In contrast, the cable used for computer networks has 8 twisted wires and the connectors used are RJ-45, which are slightly larger than the RJ-11. Figure 8 shows a RJ-45 cable with the cable connections.

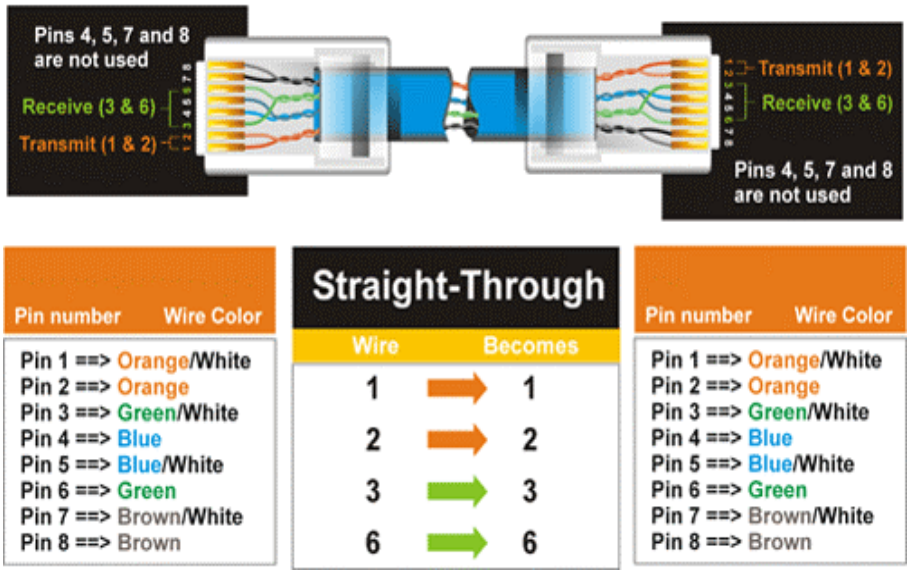

Figure 8. RJ-45 with Pin Cable Connections
Courtesy of Linksys [2]

The twisting of the wires together helps to reduce ElectroMagnetic Interference (EMI) and Radio Frequency Interference (RFI). The coax cables have a metal shielding which provides an even better source of protection against EMI and RFI. Therefore, if you have an environment with lots of high power electrical devices, such as motors, you might need to use a coax for better protection. Twisted pair can also be bought with a shield, which is known as shielded twisted pair, or STP. The normal variety is unshielded twisted pair, or UTP. The typical UTP cable is known as 10Base-T, because it is used for 10 Mbps transmission over twisted pair. The 10 Base-T cable is also called Category 3 cable, or simply Cat 3. Cat 4 cable would allow you to go to speeds of 20 Mbps, and Cat 5 to 100 Mbps. Because of the move to fast Ethernet, which transmits at 100 Mbps, most people are using Cat 5 cable for all normal cable installations. Figure 9 shows a typical twisted pair cable.

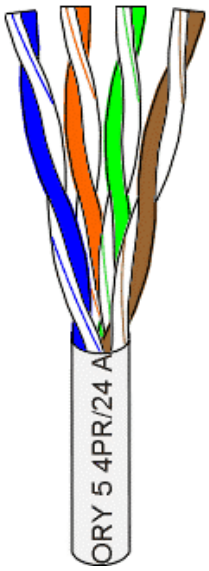

Figure 9. Twisted pair cable
Courtesy of Helmig [3]

Fiber optic cable, while not very popular today for basic LANs, has been used for years for high bandwidth traffic. It allows the use of up to (and over) 1 Gbps (1 gigabit per second, or 1 billion bits per second) speeds, and therefore is often used to carry the entire traffic of a building or a floor from one LAN to another.

Recently the use of radio waves as the media has become popular in wireless LANs. The advantage of such media is obvious, no cables to string out over rooms. However, each device on the network must have an antenna that communicates back to the central hub. While wireless LANs are not always the best solution, in certain situations it is the most feasible solution. One such case is in doctor's offices, where a doctor might go from room to room and want to be able to carry a laptop to see each patient. Using a wireless LAN, the doctor may stay connected to the network at all times and still have complete intra-office mobility. Shown in Figure 10 is a Linksys Wireless Access Point, which provides the central connection for multiple wireless devices.

Figure 10. Linksys Wireless Access Point
Courtesy of Linksys [2]

2.4.3 Network Interface Card

The cables or radio antenna just discussed must be connected to the workstation. By workstation, we are referring to any PC or Unix computer. (Although all are similar in regard to LAN connectivity, we will refer to them as either PCs or workstations.) To allow the cable to be connected to the PC, a special circuit card must be in the PC that usually has a connection point coming out of the back. This card is referred to as a network interface card.

The NIC contains both the hardware and software that will be needed to allow the workstation to communicate with the network. On the hardware side, the card first must fit into the workstation (on a PC you would have either an Industry Standard Architecture (ISA) or Peripheral Component Interconnect (PCI) bus card), and then the NIC has the appropriate connections on the back for the network cable. For typical PC installations, we would want an ISA or PCI Ethernet combo card. The ISA and PCI refer to the pin connections going into the PC, which we will not cover here. The Ethernet refers to the networking protocol being used, of which Ethernet is the most common, and the combo tells us that the card allows thin coax BNC connections and twisted pair RJ-45 connections (But not both!). If you have another type of network, such as token ring or Fiber Distributed Data Interface (FDDI), then your NIC will be different. Figure 11 shows a typical NIC being used today – a PCI based RJ-45 Ethernet card. If you by a new computer, the NIC is often build onto the motherboard of the computer, so all you will see if a RJ-45 jack on the back of the computer. Notebook computers will also have a NIC, which is usually built into the computer.

Figure 11. NIC
Courtesy of Linksys [2]

Another type of NIC is the wireless NIC, usually called a wireless adapter. If will look just like that of figure 11 except it will have an antenna. Many notebooks computers sold today will have the wireless adapter built into the system.

2.5 OSI Model

One thing we run into quickly with networking is complexity. Many things must happen at many different levels to allow two devices to communicate. For example, we said protocols are used when two people talk to one another. Therefore, when we talk to someone on the telephone we understand that a normal protocol of saying "hello" when we answer the telephone is expected. We do not just pick up the ringing phone and listen for the calling person to start speaking. This approach would work fine, but it just is not the way in which we are accustomed. However, on a deeper level, many other protocols had to be used to even get the other person to answer. These protocols take care of how the electrical signals travel down the wires and how by dialing a number we end up with a particular telephone at a particular address. Actually making a simple telephone call involves many complex protocols. In order to put some organization to these protocols a model was developed. Depending on the intended purpose of the network the selected protocols may differ, but the model for organizing them remains.

2.5.1 Layers

The OSI model is used to break the many protocols into up to seven functional layers. The three bottom layers (1-4) are focused on the technical network details of getting two devices (or people in our example) to communicate. These details include the electrical signals going down the wires as well as the wires themselves. In contrast, the top layers (5-7) deal with the issues of applications. In our example, this is the actual conversation, and the expectation that a ringing phone is answered with a "hello."

The OSI model is shown in Table 1, with an idea of how our telephone call fits into the model.

OSI Model	**Telephone Call**
7 – Application Layer	Conversation
6 – Presentation Layer	Language
5 – Session Layer	Dialogue control
4 – Transport Layer	Voice circuit setup
3 – Network Layer	Routing
2 – Link Layer	Error Detection
1 – Physical Layer	Wires and electrical voltages

Table 1. OSI Model and Telephone Call

Physical Layer

Appropriately named this layer is concerned with the actual physical devices that connect the network together. The physical layer defines whether guided or unguided media should be used

as the transmission medium. Electrical wires and optical fibers are examples of guided media while the atmosphere is an example of unguided media. Unguided media uses a transmitting and receiving antenna for transferring data between communicating stations. Unguided media vary based on the type of frequency used and will not be covered here.

Link Layer

Added on top of the physical layer, the link layer deals with error detection and retransmission of lost or garbled messages. This layer provides a reliable facility for transmitting a serial bit stream between pieces of equipment. In our example, if one phone has been disconnected, this layer determines that the physical layer is not sufficient to complete the call and returns this information to the originating caller.

Network Layer

The network layer determines the address or routing information (phone number) required to complete the call in addition to establishing a particular path to that address. It insures the path is clear and available for use. A call from New York to Los Angeles will have many alternative paths, determination of which one to use is partly accomplished at this level.

Transport Layer

The transport layer serves as an interface between the network dependent layers (1-3) and the higher application layers (5-7). Layer 4 provides a complete voice path between the two callers while hiding the underlying network facilities. The network layer makes sure that the call reaches the destination network and the transport layer ensures end-to-end connectivity and reliability of service between the two calling stations.

Session Layer

The session layer sets up a dialogue session between the two callers. It manages the exchange of data (or voice) during the call after the connection is established. In our example, both people can be talking and hearing at the same time.

Presentation Layer

The language used here is critical. For example, if both people are speaking English then they understand each other. If, however, one is speaking Spanish and the other English, then an interpreter will be needed at this layer to make the call useful.

Application Layer

The conversation between the two people makes up the application layer. Everything below this layer was established in order that this application (or conversation) could take place.

2.5.2 OSI and the Internet

The example of the telephone conversation between two people simplifies the OSI model into something with which we are all familiar. Now let us look at Table 2, which indicates how the various *Internet* parts fit into the OSI model. The model is complicated only by the fact that the various parts (protocols) have unfamiliar names. If you get confused, look back at the telephone example (Table 1) to see how that part of the Internet mimics something more familiar.

OSI Model	**Internet**
7 – Application Layer	MS Outlook, Internet Explorer
6 – Presentation Layer	Telnet, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP)
5 – Session Layer	
4 – Transport Layer	Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
3 – Network Layer	Internet Protocol (IP)
2 – Link Layer	NIC: Ethernet, Token ring, Asynchronous Transfer Mode (ATM), etc.
1 – Physical Layer	Twisted pair, coax, fiber, wireless

Table 2. OSI Model and Internet

Notice that layer 1 is very similar to the telephone model we did before. Layer 1 is just the media used to connect us to the network. However, layer 2 involves the NIC. While the NIC itself might be considered part of layer 1, since it is physical hardware, the software on the NIC provides the layer 2 functions. Notice Ethernet is at layer 2. Ethernet is the most common of all of the LAN protocols. Then we see layers 3 and 4 make up the Transmission Control Protocol (TCP) and the Internet Protocol (IP), collectively known as TCP/IP. The UDP is a similar protocol.

Now the top three layers get a little fuzzy. Two of the most common of these protocols are Simple Mail Transport Protocol (SMTP), which is used to send and receive email, and HyperText Transport Protocol (HTTP), which is used to browse web pages. Notice these protocols do not fit perfectly into the definition of the OSI, and are often shown going between layers 5 to 7. However, we are showing them going between layers 5 to 6 here so we can show that the actual application software should sit at layer 7.

All types of networks make use of the OSI model. While the model does not fit perfectly into any of the networking situations, it helps to provide a layered picture of a complex system, and therefore proves very useful in the understanding of networking.