CHAPTER 3

Network Hardware and Transmission Media

Men have become the tools of their tools.
— Henry David Thoreau

Most Internet users don't understand the hardware and media used to give them the freedom they enjoy on the WWW. There are a lot of different types of nodes that serve specific purposes, as well as different transmission media types that connect network nodes together. The average Internet user is mainly concerned that they are able to send that important e-mail and have it get there, or that they are able to download the new episode of *Survivor*. For the average user, the Internet simply is there, and that is fine for them.

The same holds true in today's workplace. Almost every business uses a network in some form and in some capacity. Even if a worker does not interface with a computer, they are probably working off a printout that was generated electronically and often from a database that connects to . . . you got it — a network. As long as they have what they need to perform the functions they need to do, they don't care what it takes to get the data passed from one point to the next.

The fact that you are reading this book means you have a reason for learning how data is transmitted. That means you need to know the information in this chapter intimately.[1] In later chapters, when we refer to a router, you need to recognize that name and know what it does.[2] This chapter provides an explanation for most of the network hardware that is in use in networks today. Network traffic and traffic patterns, as well as the cables (or lack of) used to pass the traffic, are also discussed. After reading this chapter, when

[1] This in no way implies that you don't need to know the rest of the information in this book.

[2] Besides that, if we kept saying ''node'' through this whole book, we would all get pretty bored and probably a little confused. Maybe that is why they got rid of the term ''network'' — people simple got bored and confused.

someone asks you to explain what *''10 half or 100 full''* means, you will be able to explain what they mean, define the difference between the two, and list a few pros and cons of each.

3.1 Stuff You Just Need to Know

There are a few things you need to have a basic understanding of before we jump into this chapter. First, you need to know what bits and bytes are. Even if you know what bits and bytes are, take a quick skim through this section. We also provide an overview of network addressing, encapsulation types, and other technologies we will be discussing throughout this chapter. If everything seems familiar to you, please feel free to skip to Section 3.2. If further discussion is required for any of the information in this section, it will be introduced when appropriate.[3] If you decide to skip to Section 3.2 and later get to a point in this chapter where you are not sure about something, check back to see if it was explained in this section.

ACRONYM ALERT

SNMPv3 — Simple Network Management Protocol version 3

3.1.1 Bits, Bytes, and Binary

A binary number is a system of numbering used in data communications. Sometimes referred to as the *base-2 number system*, the binary numeral system represents numeric values by a 0 or a 1. The numeral system that we are all most familiar with is the base-10 number system, often referred to as the *decimal numeral system*. The decimal numeral system represents numeric values by a 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9. Table 3-1 shows a comparison of the decimal and binary systems.

You can see that the decimal representation of the number ten is 10, whereas the binary representation is 1010. In the binary system, the numbers are counted just like they are in the decimal system. Numeric symbols count incrementally one at a time and when the highest symbol is reached (a 1 in binary, a 9 in decimal), the number resets to 0 and carries one to the left.

For example, if you count from zero through ten in decimal, it looks like this: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. When the highest symbol (9) is reached, the number carries over a 1 symbol to the left and then resets the first symbol to 0. If you count zero through ten in binary, it looks like this: 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010. In binary, when the highest symbol (1) is reached, it carries a number to the left and resets, just like in decimal.

[3] In fact, this is information you are probably familiar with. We won't dwell too much on this section; that way we can have more room to talk about the beefier hardware that moves data in any given network.

Table 3-2 shows some examples of converting decimal numbers to binary.

Table 3-1 Decimal Numbers and Their Binary Number Equivalents

DECIMAL	BINARY
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010

Table 3-2 Decimal/Binary Conversions

DECIMAL	128	64	32	16	8	4	2	1
BINARY	0	0	0	0	0	0	1	1

Starting from the right of the table, you can reference the decimal symbols with the binary symbol. The decimal number 3 is equal to (2+1). The binary symbols that correspond with the decimal symbols being referenced are then set to 1 and all others are set to 0.

DECIMAL	128	64	32	16	8	4	2	1
BINARY	1	0	0	0	1	0	0	1

Starting from the right of the table, you can reference the decimal symbols with the binary symbol. The decimal number 137 is equal to (128+8+1). The binary symbols that correspond with the decimal symbols being referenced are then set to 1 and all others are set to 0.

The symbols that are used in the binary system are known as *binary digits*, or *bits*. The single digit in the binary number is 1 bit (which is a 1 or a 0). For example, binary number 0100 is 4 bits long. The bit is the basic unit of information in data communication. It is much like a toggle switch with only two settings, on (1) or off (0). In data communications, the bit is set based on electrical levels. A 1 is set if voltage is received, and a 0 is set if there is no voltage.

There are other terms you will come across that you need to understand when referencing a group of bits. Eight bits are equal to 1 byte, 1,024 bits are equal to 1 kilobit (Kbit or Kb), 125,000 bytes are equal to 1 megabit (Mb), and so on (see Table 3-3).

Table 3-3 Grouping of Bits

SI NAME	BINARY VALUE IN BITS	BINARY NAME (IEC)
Kilobit (Kbit)	2^{10}	Kibibit (Kbit)
Megabit (Mbit)	2^{20}	Mebibit (Mibit)
Gigabit (Gbit)	2^{30}	Gibibit (Bibit)
Terabit (Tbit)	2^{40}	Tebibit (Tibit)
Petabit (Pbit)	2^{50}	Pebibit (Pibit)
Exabit (Ebit)	2^{60}	Exbibit (Ebit)
Zettabit (Zbit)	2^{70}	Zebibit (Zibit)
YottaBit (Ybit)	2^{80}	Yobibit (Yibit)

We have already determined that 8 bits are referred to as 1 byte. To continue, 1,024 *bytes* is equal to 1 *kilobyte* (*KB* or *kB*), 1,048,576 *bytes* is equal to 1 *megabyte* (*MB* or *Mbyte*), and so on (see Table 3-4).

3.1.2 Non-human Resources

There is a vast array of resources in use in a network. Anything that is used within the network to provide data to the end users (e.g., applications, operating systems, servers, memory, storage devices, etc.) is considered a network resource. All the hardware and media discussed throughout this chapter are network resources. In this section, we refer to the processing and storage resources used by the nodes in a network.

Table 3-4 Grouping of Bytes

SI NAME	BINARY VALUE IN BYTES	BINARY NAME (IEC)
Kilobyte (KB, kB)	2^{10}	Kibibyte (KiB)
Mebibyte (Mbyte)	2^{20}	Mebibyte (MiB)
Gigabyte (Gbyte)	2^{30}	Gibibyte (GiB)
Terabyte (Tbyte)	2^{40}	Tebibyte (TiB)
Petabyte (Pbyte)	2^{50}	Pebibyte (PiB)
Exabyte (Ebyte)	2^{60}	Exbibyte (EiB)
Zettabyte (Zbyte)	2^{70}	Zebibyte (ZiB)
Yottabyte (Ybyte)	2^{80}	Yobibyte (YiB)

Network resources can be classified as volatile or nonvolatile.

```
vol·a·tile[4]
adjective
1: readily vaporizable at a relatively low temperature
2: flying or having the power to fly
3: a: lighthearted
b: easily aroused <volatile suspicions>
c: tending to erupt into violence
4: a: unable to hold the attention fixed because of an inherent lightness
 or fickleness of disposition
b: characterized by or subject to rapid or unexpected change
5: difficult to capture or hold permanently
non·vol·a·tile[5]
1: not volatile:
a: not vaporizing readily
b: of a computer memory : retaining data when power is shut off
```

[4] volatile. (2008). In *Merriam-Webster Online Dictionary*. Retrieved May 14, 2008, from www.merriam-webster.com/dictionary/volatile

[5] nonvolatile. (2008). In *Merriam-Webster Online Dictionary*. Retrieved May 14, 2008, from www.merriam-webster.com/dictionary/nonvolatile

3.1.2.1 Volatile Memory

Data storage is performed by a storage device or memory that is set aside for the storage of data for a nonpermanent period of time. In other words, a device receives and reviews data, processes it, and then moves on to the next data process. It uses volatile memory or storage in order to perform this action. Once the data is no longer needed, it can be removed and new data can take its place. When power is removed, volatile memory does not retain its data.

POP QUIZ

The decimal number 211 is equal to what binary number?

3.1.2.1.1 Random Access Memory

Random access memory (RAM)[6] is the most well known form of memory in the data environments. It is called random access memory because it is memory that is available for data storage and access, regardless of the order in which it is stored. Information stored in RAM is accessible until it is cleared out or the device it is being used on is shut down.

RANDOM BONUS DEFINITION

data storage density — The quantity of data that can be stored within a data storage medium.

Computers store OS and system data in RAM when the computer boots up. The remaining space that is not used by the system software is utilized as programs are accessed and used on the computer. Data access is quicker with data that is stored in RAM than any of the other storage devices a computer may use.

3.1.2.1.2 Dynamic Random Access Memory

Dynamic random access memory (DRAM) is the type of RAM that is used as the main memory by most PCs. DRAM has to have a little jolt of electricity every couple of milliseconds in order to operate. DRAM uses a transistor and a capacitor for each storage cell it contains. Each received bit is stored in a cell. As the capacitor loses its charge, an electronic charge refreshes the capacitor.

[6] A lot of companies are working on a nonvolatile form of RAM. This will speed up the boot-up and shutdown times of a device, and will save energy as well. As more and more companies are releasing ‘‘green’’-friendly devices, this technology may debut soon (maybe even before this book is released).

DRAM is considered high density because it is able to store more data than other memory types. This is because each storage cell only requires one capacitor and transistor. Examples of DRAM modules include:

- Dual inline memory module (DIMM) — Designed for use in personal computers, miscellaneous workstations, and servers.
- Single inline memory module (SIMM) — Used in personal computers prior to the late 1990s.
- Single inline pin package (SIPP) — Used in older computers that had the Intel 80286 processor.
- Synchronous dynamic random access memory (SDRAM) — DRAM with a serial interface, which allows the memory to accept new instructions while it is still processing previous instructions. Used in computers, workstations, and servers.

3.1.2.1.3 Static Random Access Memory

Static random access memory (SRAM) uses electronic circuitry to store bits in memory. SRAM does not need to be charged, as there are no capacitors being used to store the bits. SRAM cells maintain one of two states, either a 0 or a 1. SRAM is most commonly used as the cache memory for most microprocessors, storing up to several MBs of data. Device system registers will also often use SRAM as the mode of memory.

POP QUIZ

The binary number 01011100 is equal to what decimal number?

3.1.2.2 Nonvolatile Memory

Memory that can retain data even when it is not receiving power is known as *nonvolatile memory*. Nonvolatile memory is used as a secondary storage device. This is where data that needs to be stored for long periods of time is located, such as configuration files, OS software, and systems software. For the most part, nonvolatile memory is slower in moving data than volatile memory. This is the main reason that nonvolatile memory is used for storage.

3.1.2.2.1 Magnetic Storage Media

You might use magnetic storage a lot more than you are aware of. Not only are computer hard disk drives and backup tape drives (and a few other storage devices) magnetized data storage devices, magnetic storage is used in the audio and video world as well. As a matter of fact, the strip on the back of your debit and credit cards is magnetic storage for identification data that communicates with the card reader used when you purchase something.[7]

Data stored on electronic media can be removed and the space that it was occupying can be reused for other data. Data is written onto the medium with electrical impulses that set a bit to either positive or negative polarity. When data is accessed, the polarity of the bit is read, and the setting of the bit (1 or 0) is determined.

3.1.2.2.2 Read-Only Memory

Memory used to store information that is not intended to be modified is known as read-only memory (ROM). ROM is often referred to as *firmware*, which is the software required for hardware-specific operations. ROM chips can retain this data even without electricity applied to the device. There are arrays of different ROM chip types; among these are:

- **Read-only memory (ROM)** — Memory that is configured and set by the manufacturer. It contains device systems software necessary for the proper operation of the device.
- **Programmable read-only memory (PROM)** — A memory chip that can be written to only once. This will allow someone other than the manufacturer to write data onto the PROM. Just like ROM, the data is there forever. A device known as a PROM programmer (PROM burner) is used to write the data onto the chip.
- **Erasable programmable read-only memory (EPROM)** — A memory chip that can store data that may need to be overwritten at some point. The data on the EPROM is erased by UV light and can then be reprogrammed with a PROM burner.

ACRONYM ALERT

PCMCIA — Personal Computer Memory Card International Association

- **Electrically erasable programmable read-only memory (EEPROM)**[8] — A memory chip that can store data that may need to be overwritten at some point. The data on the EEPROM is erased by an electrical charge and can then be reprogrammed with a PROM burner.

[7] You can now ‘‘pay at the pump,’’ thanks to magnetic storage.
[8] Say that five times real fast!

3.1.2.2.3 Flash Memory

Flash memory is a form of EEPROM that is used by a device for specific storage purposes. Digital cameras, video gaming systems, laptops, many network devices, and PCs all use flash memory. Examples of flash memory are:

- Memory cards for cell phones
- Memory cards for digital cameras
- Memory cards for video game systems
- PCMCIA[9] type 1 memory cards (3.3 mm thick)
- PCMCIA type 2 memory cards (5.0 mm thick)
- PCMCIA type 3 memory cards (10.5 mm thick)
- Personal computer system BIOS chip

PC BIOS memory chips are the most commonly used fixed type of flash memory. The other types of flash memory are removable and can hold a lot of data. When feasible, flash memory is preferred over hard disk drive memory because it is faster, smaller, lighter, and does not have any moving parts. On the downside, flash memory is more expensive when comparing the cost of an equal amount of storage space on a hard drive.

POP QUIZ

What is the binary name for the binary value of 2^{50}?

3.1.3 Encapsulation

Encapsulation is the act of including data from an upper-layer protocol within a structure in order to transmit the data. As we discussed in Chapter 1, most applications use either TCP or UDP. If data is transmitted from the Application layer, the data that needs to be transmitted is passed to the Transport layer. Let's say that TCP is the protocol that is used. TCP adds a TCP header to the datagram and then the datagram is passed to the Network layer where it is encapsulated into an IP packet. The packet is then passed to the Data Link layer where it is encapsulated into a frame (Ethernet, Token ring, etc.) and then transmitted over the physical media to a destination. Figure 3-1 shows an example of this.

[9] Many people still refer to this type of memory card as a *PCMCIA card*. This is actually no longer the appropriate term. PCMCIA memory cards are now simply called PC cards.

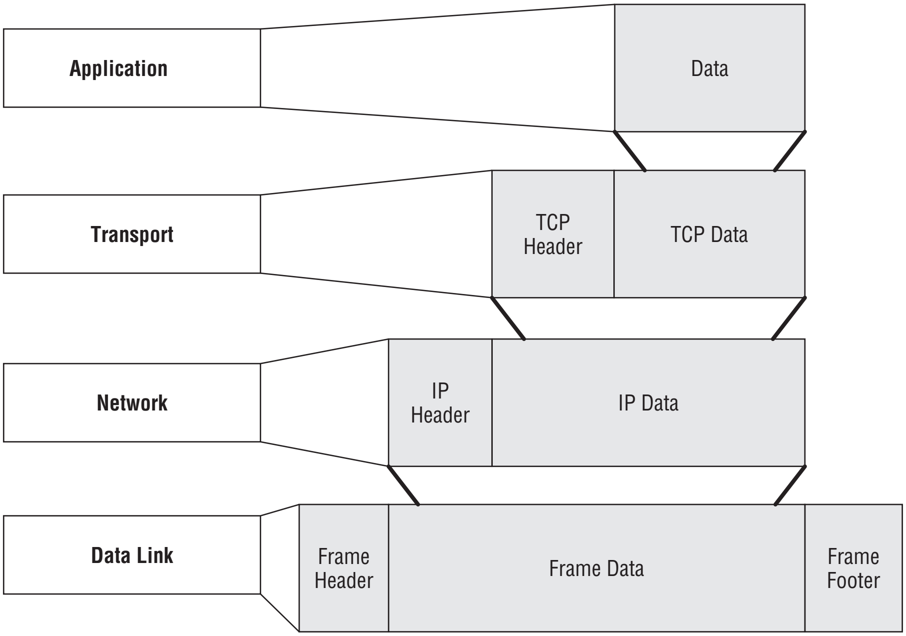

Figure 3-1 Encapsulation

Information passed from layer to layer is called service data units (SDUs) or protocol data units (PDUs). The difference between an SDU and a PDU is that the PDU specifies the data that is to be transmitted to the peer layer at the receiving end. The SDU can be considered the PDU payload. Recall from the paragraph above, data is transmitted from Layer 7 to Layer 4, from Layer 4 to Layer 3, and so on. The data that is put together to be passed from Layer 7 to Layer 4 is the PDU. The SDU is what it becomes when it is encapsulated into the PDU of the lower layer. Figure 3-2 shows an example of what PDU is used at each layer in the OSI reference model.

Each layer within the OSI reference model creates a PDU for any data that needs to be transmitted to the next lower level. In addition to the data in the PDU, each layer assigns a header to the PDU as well. Refer now to Figure 3-3. Data is being transmitted from Layer 7 to Layer 1, across a medium to the Physical layer on the opposite end, and then up each layer until it reaches Layer 7. Notice that each layer appears to communicate directly to the layer on the opposite end. When each layer passes data to the layer below it, the data (including the higher layer header) becomes an SDU. When the layer attaches its header to the SDU, it becomes the PDU that is transmitted to the next lower layer.

Layer	PDU
Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

Figure 3-2 PDUs used at each layer in the OSI reference model

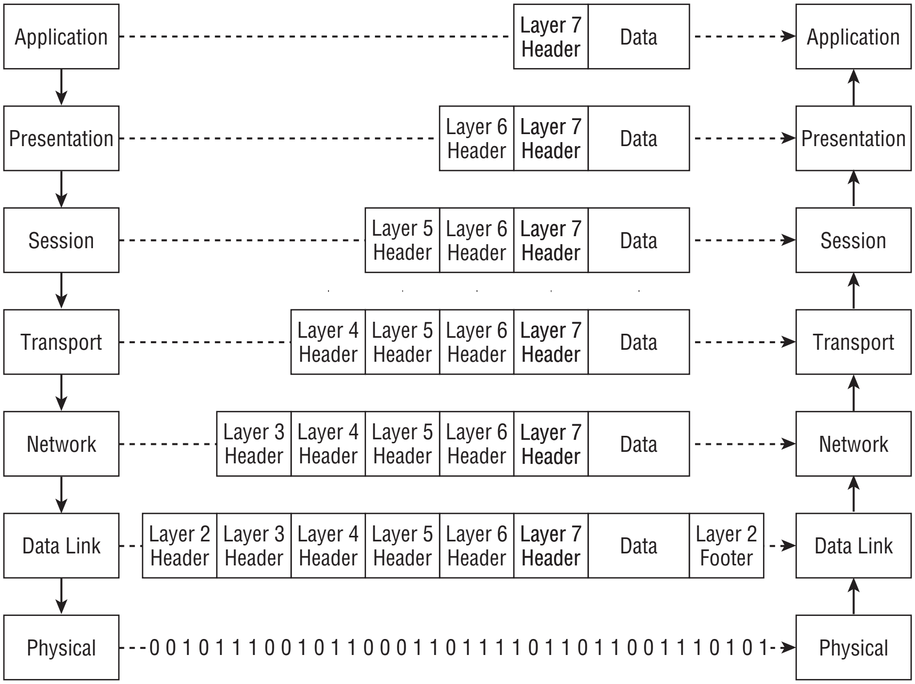

Figure 3-3 Layer-by-layer encapsulation

3.1.4 Data Communication Equipment and Data Terminal Equipment

Data communication predominately takes place between nodes that are known as either data communication equipment (DCE)[10] or data terminal equipment (DTE). In order for communication to take place between nodes, one end of the connection must be a DCE and the other a DTE. If you have to connect a DCE to a DCE or a DTE to a DTE, a null modem[11] or a crossover cable[12] must be used. The plug connector of a hub (see Section 3.3.4) or a modem would be an example of a DCE, whereas the plug connector on an NIC card (see Section 3.3.2.2) would be an example of a DTE.

RANDOM BONUS DEFINITION

straight-through cable — A twisted pair cable that is wired for normal DTE to DCE communications.
crossover cable — A twisted pair cable that is reverse-wired for DCE-to-DCE or DTE-to-DTE communications.

In data communications, synchronization between nodes is known as clocking. The DCE is responsible for providing the clock signal while the DTE is responsible for synchronizing its clock based on the signal received. The DCE uses what is called *internal clocking*, setting the clocking without any outside influence. The DTE uses *external clocking*, which requires a signal in order to set and synchronize its clocking.

3.1.5 All Your Base Are Belong to Us[13]

We don't want to jump into Ethernet signaling at this point (Chapter 6, ''Ethernet Concepts,'' will cover this in depth). We do want to introduce some terms that you will come across in this chapter (10BASE-T, 100BASE-TX, etc.), so you will understand what they mean.

Baseband simply refers to the way data is transported on the wire. A baseband signal is data that transported as digital data on an unmultiplexed channel over the transmission medium. The BASE in the term 10BASE-T stands for broadband. The number preceding BASE is the speed (for instance, 10BASE means that the transmission medium can support Ethernet transmission at a

[10] DCEs are also often called *data carrier equipment*.

[11] Serial cables that crosslink the transmit and receive wires. Also can be an adapter that is used to cross the signals.

[12] Normally a crossover cable is an Ethernet cable that is reverse-wired on each end. This will put all output signals on one end of the cable to be the input signals on the other, and vice versa. This is appropriate for other technologies, but is most common in Ethernet.

[13] If you are an Internet gamer, you are probably familiar with this slogan. This broken English translation appeared in a European release of the Japanese video game *Zero Wing*.

speed of 10 Mbps over baseband). All symbols following BASE identify either a distance of transmission or a medium type (5 for 500 meters, T for twisted pair, F for fiber optic).

3.1.6 Computer Buses[14]

Computers can be modified and any hardware that is added to the computer is known as a *peripheral*. New peripherals come with software, known as a *driver*, that is loaded on your PC and provides the instructions the computer will use to learn what it needs to communicate and coexist with the peripheral. Within the computer, there is a system that can logically connect multiple peripherals within the same set of wires. This system is known as the *computer bus*. Computer buses are also used to connect computer internal components (more on this in a minute[15]).

ACRONYM ALERT

PCI — Peripheral component interconnect

A computer bus can operate as both a *parallel* bus and a *serial* bus. What's the difference? Glad you asked. Parallel buses transmit several bits of data at the same time, in parallel on the bus, whereas serial buses transmit data one bit at a time, sequentially to the destination. The main types of computer buses are an *internal* bus and an *external* bus. The internal bus is the bus that is contained within the computer and connects internal components to the shared bus; an external bus is a bus that connects peripherals to the motherboard.

3.1.7 IP Addressing

Nodes in a TCP/IP network are assigned a numeric value, known as an *IP address*. We will be discussing IP addressing throughout this book, so this is a short overview. The IP address usually is unique and provides a network identify for the node. Although there are new versions of IP that are growing in popularity, currently[16] IP version four (IPv4) is still what the majority of networks are using.

An IPv4 address is a 32-bit number that is divided into four fields, called *octets*, separated by dots. Each octet represents 8 bits of the total 32-bit number. This is known as *dotted decimal notation*. An example of dotted decimal

[14] Not to be confused with a commuter bus.

[15] Disclaimer: This actually may take more or less than a minute. It depends on how fast you can read and how many breaks you take.

[16] IPv4 is popular at the time of this writing, although this may change in the near future, as a lot of new vendor implementations are using IPv6.

notation would be the IP address 192.168.1.1.[17] The meaning of the octet that is represented by each number depends upon what *network class* the IP address belongs to. The entire IP address is separated into two parts: the network part and the host part. Figure 3-4 shows an example of the difference in network classes.

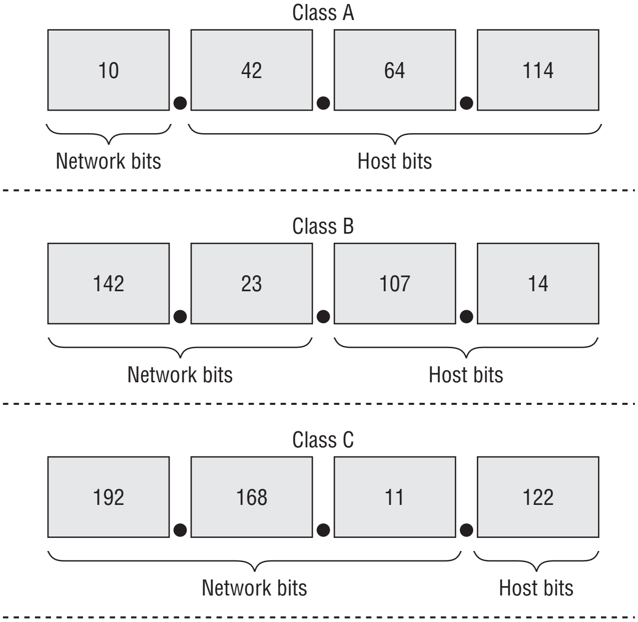

Figure 3-4 IP address network classes

The four[18] network classes are as follows:

- **Class A** — Class A addresses are identified by a number from 1 to 126 in the first octet. In Class A addresses, the first octet identifies the network and the remaining three octets identify the host. These addresses are normally assigned to larger networks.
- **Class B** — Class B addresses are identified by a number from 128 to 191 in the first octet. In Class B addresses, the first two octets identify the network and the last two identify the host. These addresses are normally assigned to medium-sized networks.
- **Class C** — Class C addresses are identified by a number from 192 to 223 in the first octet. In Class C addresses, the first three octets

[17] IP addresses are identified in decimal (dotted decimal notation, to be specific). If converted to binary, this number is 11000000.10101000.00000001.00000001 (note that there are 8 bits in each field).

[18] There is also a Class E network class, but it is not an approved standard and is experimental.

identify the network while the last octet identifies the host. These addresses are normally assigned to small to medium-sized networks

- **Class D** — Class D addresses are a little different than the other classes. Class D addresses are used for multicasting. These addresses always begin with the first 4 bits being 1110 and the remaining 28 bits identifying the network in which the multicast message is to be sent.

DID YOU JUST NOTICE THAT?

If you were paying attention during the previous discussion of IP network classes, you may have noticed that the number 127 is skipped in the transition from Class A (first octet containing 1–126) to Class B (first octet containing 128–191). This is because the number 127 in the first octet represents a special type of IP address called a loopback address. Used mainly for troubleshooting, the loopback IP simply loops datagrams back to the sender.

Some other special IP addresses include:

- **0.0.0.0 — Default network (where packets go when the router doesn't know where a host is)**
- **1.1.1.1 — Broadcast to all on a specified network**

3.2 Transmission Media

Transmission media refers to the modes and materials by which the data is transferred in a network. Network cables, light waves, and so on are all considered transmission media. (If you are referring to more than one medium, it is called media.[19]) Transmission media provide a way for data to be passed from one endpoint to another. The medium does not guarantee delivery nor is it concerned with what information is contained in the datagram; it simply provides the path for the data.

POP QUIZ

Define *RAM*.

In the United States, there are two forms of transmission media in data communications. The first type, *bounded* or *guided*, is a communication line (or any other type of solid medium) that transports waves from one endpoint to another. The second type, *unguided* or *wireless*, is where data is passed wirelessly from one access point (antenna) to another.

[19] Another one of those terms that is often misused but always understood.

3.2.1 Network Cabling

Wireless communication as a transmission medium is becoming more and more popular, but network cabling is still the backbone of any network. There are many different types of cabling, each serving a specific purpose to meet the needs of the network. Often you will find different types of cabling running side by side between nodes in the network. It's important to understand the cabling types that are in use on any network you configure and how to maintain them. The major cable types are:

- Twisted pair
- Coaxial
- Fiber optic

The type of cabling that is used depends on the network. Data traffic requirements, the size of the network, the topology of the network, the protocols in use, the nodes in place, cost considerations, and many other things need to be taken into account when designing and/or maintaining a network. In this section, we will discuss the more popular cable types and how they work.

TIPS FOR INSTALLING AND REPLACING CABLES

Whenever you need to replace cables, or are tasked with designing and implementing a cable run, there are a few hints you should be aware of that will save you headaches in the future.

1. **Use cable ties to keep cables grouped together. Do not use tape, staples, glue, rubber bands, etc. The cable ties are easy to work with and easy to remove when you need to.**
2. **Make sure to label the cables on each end of the link. It can be very time consuming to try to track down a problem if the cables are not labeled. Tape, glue, and even rubber bands work well for this task. Staples or tacks do not.**
3. **Keep the cable off the floor. If you do not have a choice, then make sure you cover the cable with a cable protector.**
4. **Stay away from anything that may cause electrical interference.**
5. **Cut your cables too long on purpose — leave some excess (on both ends) to work with in the future.**
6. **Make a detailed drawing of the cables that are installed in the building. The drawing needs to be easy to understand when tracking cable routes and endpoint connections.**

(continued)

TIPS FOR INSTALLING AND REPLACING CABLES *(continued)*

7. Implement a "hands-off" policy for end users. Make sure you know who is touching the cables and interfaces attaching end-user nodes to the network. This is especially important in coaxial runs. One glitch and all the users go down.

3.2.1.1 Twisted Pair Cable

Twisted pair cabling consists of two or more pairs of conductors that are twisted together within the cable. The conductors are wrapped in plastic and then all of the pairs are wrapped within the cable, making them less susceptible to outside electrical interference. Twisted pair cables are used primarily in areas with short to medium distances between nodes. Twisted pair is less expensive than coaxial cable or fiber cable, and is often used as a consideration in network design.

There are four pairs of twisted wires in a network Ethernet cable. These are color coded in blue, brown, green, and orange. Each twisted pair has one solid and one striped wire. Here is a list of the wires that are within a normal twisted pair cable:

- Blue
- Blue/white
- Brown
- Brown/white
- Green
- Green/white
- Orange
- Orange/white

POP QUIZ

Define *encapsulation*.

There are two main types of twisted pair cabling in use in LANs. Unshielded twisted pair (UTP) is the most popular copper cable type. Shielded twisted pair (STP) is the other type. Ethernet and Token Ring both use twisted pair cabling.

- **Unshielded twisted pair** — UTP cabling is the type of copper cabling that is used the most in networks today. UTP cables consist of two or more pairs of conductors that are grouped within an outer sleeve. Figure 3-5 shows an example of a UTP cable.

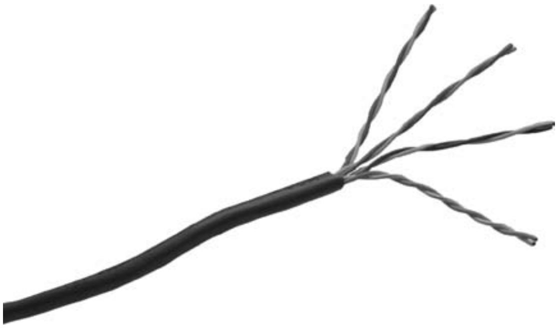

Figure 3-5 UTP cable

UTP cable is often referred to as *Ethernet cable*, because Ethernet is the predominate technology that uses UTP cable. UTP cabling is cheap, but does not offer protection from electrical interference. Additionally, bandwidth is limited with UTP in comparison with some of the other cable types.

- **Shielded twisted pair** — STP cabling is a type of copper cabling that is used in networks where fast data rates are required. STP cables consist of two or more pairs of conductors that are grouped together and then an additional metal shield wraps around the twisted pairs, forming an additional barrier to help protect the cabling. Finally, all of the cables are grouped together and a final outer sleeve is placed over the wiring. Figure 3-6 shows an example of an STP cable.

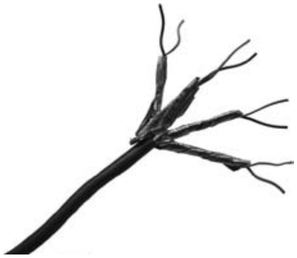

Figure 3-6 STP cable

STP cables are also referred to as Ethernet cables. STP cables provide additional protection to the internal copper, thus data rates are increased and more reliable. The conductors that are grouped together can be shielded as individual pairs (in other words, each pair will have its own shield), or all pairs can be shielded as a group.

The ANSI/TIA/EIA-568-B standard, *Commercial Building Telecommunications Standard*, is the standard that defines the requirements for installing and maintaining cabling systems, component, and data transmissions in commercial buildings. In the standard, the categories (Cat) of twisted pair cabling are outlined. As of the release of the ANSI/TIA/EIA-568-B standard, the only categories that are recognized by the standards are Cat 5e and above.[20] Table 3-5 lists all the categories, but you need only to know they exist. You should focus on Cat 5e and above, as this is the direction the data world is heading.

Table 3-5 ANSI/TIA/EIA-568-B Standard Categories

CATEGORY	ANSI/TIA/EIA-568-B STATUS	USED FOR	PERFORMANCE
Cat 1	Unrecognized	ISDN, ISDN basic rate interface (BRI), doorbell wiring, POTS voice communication	Less than or equal to 1 Mbps
Cat 2	Unrecognized	Token Ring	4 Mbps
Cat 3	Unrecognized	10BASE-T Ethernet	16 MHz
Cat 4	Unrecognized	Token Ring	20 Mbps
Cat 5	Unrecognized	100BASE-T Ethernet	Less than or equal to 100 MHz
Cat 5e	Recognized	100BASE-T and 1000BASE-T Ethernet	Less than or equal to 100 MHz
Cat 6	Recognized	Backward compatible to Cat 3, Cat 5, and Cat 5e cabling; 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet	Less than or equal to 250 MHz
Cat 6a	Recognized	10GBASE-T Ethernet	Less than or equal to 500 MHz
Cat 6e	Recognized	10GBASE-T Ethernet	Less than or equal to 625 MHz

Twisted pair cables can be hard-wired to endpoints or attached to a registered jack (RJ) connector. The most common connector is often referred to as an *RJ45 connector*. The RJ45 connector resembles the connector for land-based telephones, only larger. If you have plugged your PC into a network, then you plugged in an RJ45 (see Figure 3-7).

[20] This does not mean that other categories are no longer in use. They probably are and will be in networks that never change (which are rare). It simply means there are no plans to advance the category (and you can bet there are not a lot of vendors out there that will continue to build based on Cat 5 and below technology).

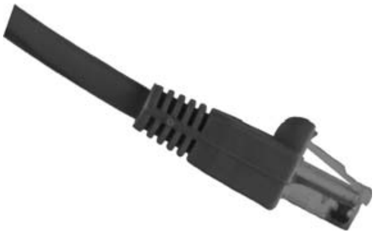

Figure 3-7 An 8P8C plug (RJ45)

STUFF YOU JUST HAVE TO KNOW

Let's take a moment to talk a little about registered jacks. A registered jack (the *RJ* in *RJ45*) is simply a standardized network interface. The pattern of the wiring, as well as the construction of the jack itself, is based on the standard for which the jack was developed. Although we have written mostly about the RJ45 in this chapter, this does not imply that the RJ45 is the only type of interface you will come across. So we have provided the following handy-dandy reference list for your information.

- **RJ11 — Used for telephone wires. If you pick up a phone (land line, of course) and look at the wire that plugs into the phone, you are most likely looking at an RJ11 connector.**
- **RJ14 — Same as above, but for two lines instead of one.**
- **RJ25 — For three lines.**
- **RJ61 — For four lines.**
- **RJ48 — Tor T1 and ISDN lines.**
- **RJ49 — Tor ISDN BRI lines.**
- **RJ61 — For twisted pair cables.**

The term *RJ45* refers to what is normally attached to any 8 Position 8 Contact (8P8C) jacks and plugs, but the true RJ45 standard defines the mechanics of the interface as well as a wiring scheme that does not match the ANSI/TIA/EIA-568-B standard. There are two parts to the 8P8C: the plug and the jack. The plug is what was referred to in

ACRONYM ALERT

HDLC — High-Level Data Link Control

Figure 3-7 and is often called the *male connector* or *male plug*. The *jack* is the interface that the plug goes into and is called the *female connector* or *female jack*.

There are eight pins, numbered 1 through 8 in an RJ45 connector. Sometimes these are labeled on the plug. If they are not labeled, you can identify the pin numbers by holding the connector in your hand with connector pins facing upward and outward. The pin that is closest to you will be pin number 1 and then they are sequentially numbered through pin number 8. (See Figure 3-8.)

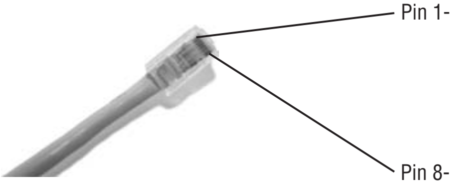

Figure 3-8 RJ45 pin numbering

ANSI/TIA/EIA-568-B defines the pin to twisted pair definitions for pin assignments when connecting the twisted pair to the 8P8C connector. The definition of the pin/pair assignment[21] is named T568A and T568B.[22] The standard to use depends on the 8-pin cabling system that is in use. T568A and T568B define the order in which twisted pairs should be attached to the 8P8C adapter. Table 3-6 shows an example of the cable pin-outs for a T568A straight-through cable.

The difference between the T568B pin-out definitions and the T568A pin-out definitions is that the green pair and the orange pair are reversed. Table 3-7 shows the pin-outs for T568B.

3.2.1.2 Coaxial Cable

Coaxial cabling is not as popular as twisted pair cabling, but there still are some networks that use it.[23] Figure 3-9 shows an example of a coaxial cable. Within the cable, there is either a single inner conductor or group of conductors that are twisted together to form one. The conductor is then wrapped in a plastic sleeve, which is wrapped in a metallic conducting shield. Finally, these are all wrapped in an insulating sleeve. There may be a slight variation between cable vendors, but the functions of the coaxial cable remain the same.

[21] The pin/pair assignment is often referred to as the *cable pin-outs*.

[22] T568B is not to be confused with the standard ANSI/TIA/EIA-568-B.

[23] Most of these were networks that were built in the late 1980s and early 1990s. Most new deployments use twisted pair.

Table 3-6 T568A Straight-Through Pin-Outs

8P8C PIN NUMBER	WIRE COLOR	10BASE-T 100BASE-T SIGNALING	1000BASE-T SIGNALING
1	Green/white	Transmit+	Bidirectional data A+ (BI_DA+)
2	Green	Transmit−	Bidirectional data A− (BI_DA−)
3	Orange/white	Receive+	Bidirectional data B+ (BI_DB+)
4	Blue	Not used	Bidirectional data C+ (BI_DC+)
5	Blue/white	Not used	Bidirectional data C− (BI_DC−)
6	Orange	Receive−	Bidirectional data B− (BI_DB−)
7	Brown/white	Not used	Bidirectional data D+ (BI_DD+)
8	Brown	Not used	Bidirectional data D− (BI_DD−)

Table 3-7 T568B Straight-Through Pin-Outs

8P8C PIN NUMBER	WIRE COLOR	10BASE-T 10BASE-T SIGNALING	100BASE-T SIGNALING
1	Orange/white	Transmit+	(BI_DA+)
2	Orange	Transmit−	(BI_DA−)
3	Green/white	Receive+	(BI_DB+)
4	Blue	Not used	(BI_DC+)
5	Blue/white	Not used	(BI_DC−)
6	Green	Receive−	(BI_DB−)
7	Brown/white	Not used	(BI_DD+)
8	Brown	Not used	(BI_DD−)

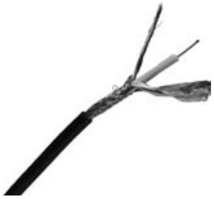

Figure 3-9 An example of coaxial cable

The inner conductor and the conducting shield work on the same *axis* and work together to pass data — hence the name *co* (cooperative) and *axial* (running on the same axis). Data is transmitted in the space between the inner conductor and the outer conducting shield. Coaxial cables are best suited for high-frequency or broadband signaling.

The connectors that are used to connect coaxial cable runs are known as *bayonet Neill-Concelman (BNC) connectors*. There are two main types of coaxial cabling, *thin coaxial* and *thick coaxial*, often referred to as *thinnet* and *thicknet*. When used for Ethernet, they are called *thin Ethernet* (10BASE2) and *thick Ethernet* (10BASE5).

Thin coaxial cabling, known as *RG-58*, is used for connections that use a low power signal. In Ethernet, the maximum distance that data can be transmitted is 185 meters. A node must be placed within that distance, or data corruption and deletion may occur. Thick coaxial cabling, known as *RG-8*, is used for connections that require a higher power signal. The maximum travel distance between nodes using thick coaxial cables is 500 meters.

3.2.1.3 Fiber Optic Cable

When used in data networking, fiber optic cables are groups of thin strands of glass or transparent plastic that is able to carry data for long distances. The fibers are grouped together to form the *core* of the cable. The core is wrapped in a *cladding*, which is denser glass material that reflects light back to the core. Surrounding the cladding is a buffer. Finally, there is an outer wrap called a *jacket* that helps protect the core from damage. Fiber optic cable has helped make a lot of the advances in networking over the last few years. The use of fiber cables provides for an increase in the distance data can travel between nodes, as well as speeds that are, well, as fast as light.[24] Optical signaling is not hampered by electronic interference, so data loss is not seen as often as with twisted pair or coaxial.

Fiber optic cabling works by sending reflections of light from one endpoint to another. The light travels between the core and the cladding and back again. The cladding reflects the light back to the core, much like a mirror does if you shine a light into it. This is known as *total internal reflection* (see Figure 3-10).

[24] Light signals can be transmitted at speeds of up to 40 Gbps.

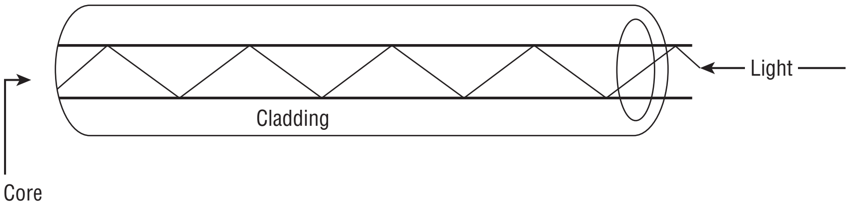

Figure 3-10 Total internal reflection in a fiber optic cable

Fiber optic cables are advantageous as a transmission medium for fast data exchange over long distances. Fiber optic cabling can also save space in a LAN as it requires less space than copper cables. There are two main types, or modes, of fiber optic cabling used for data communications: *single-mode fiber* (SMF) and *multi-mode fiber* (MMF).

- **Single-mode fiber optical cabling** — SMF cables are thinner than MMF cables. This is because SMF cables are designed to carry a single beam of light. Because there are not multiple beams involved, the SMF cable is more reliable and supports a much higher bandwidth and longer distances than MMF cables. The bulk cost of SMF cabling is much less expensive than MMF cabling. Figure 3-11 shows an example of an SMF cable.

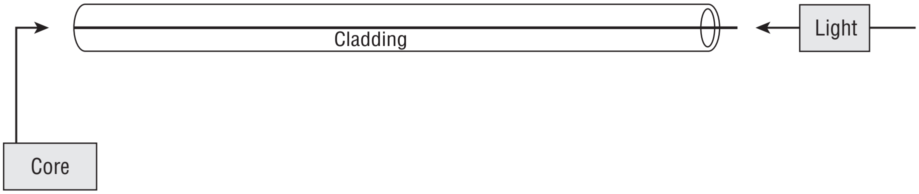

Figure 3-11 Single-mode signaling

POP QUIZ

What is IEEE Standard 802.11?

- **Multi-mode fiber optical cabling** — MMF cabling is made for shorter distances. Unlike SMF, there are multiple beams of light, so the distance and speed are less. Granted, supporting data rates of up to 10 Gbps for distances as far as 300 meters is nothing to sneeze at. Because of the additional modes, MMF cabling is able to carry much more data at any given time. Figure 3-12 shows an example of MMF cabling.

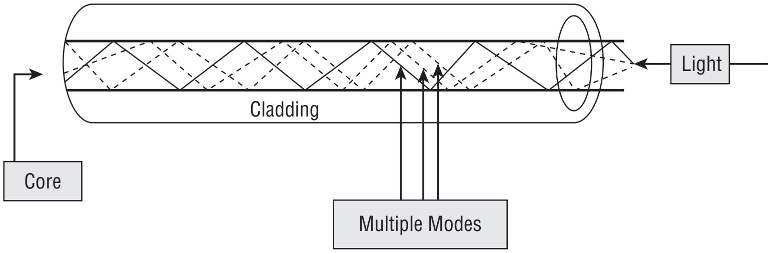

Figure 3-12 Multi-mode signaling

3.2.2 Wireless Communication

Wireless communication has really grown in the past few years. Many businesses, universities, and even some cities have now implemented wireless access for anyone to use. There is nothing like being able to sit in a bookstore or a coffee shop and being able to connect to the Internet and all that it offers. Signals in wireless communication are sent via antennas, microwave stations, satellite, or infrared light.

Wireless communication enables data to be transferred through the air via a communication signal. Communication is normally handled by infrared light or high-frequency radio waves. Infrared communication normally takes place between nodes. The wireless signal between a PDA and a PC is an example of nodes that use an infrared signal. Data communications, radio, and cellular phones are all examples of nodes that use radio waves for data communication. Section 3.3.3.9.3 covers the hardware that makes wireless communication as a transmission medium a reality.

3.3 Network Hardware

A lot of different types of network hardware work together[25] to issue, pass, respond, receive, and otherwise transmit data in a network. Network hardware performs the operations necessary to receive and forward data that it is responsible for. Not all network hardware is created equal. Keep in mind, however, the hardware is built to support the available standards that the particular node should be able to support. Most of the hardware in networks is nothing more than a big paperweight without the software loaded on the device to teach it what to do and sometimes how to do it. To take this a bit further, the hardware and software are useless without someone to configure

[25] There are also times when the network hardware does not work well together, but we will save that discussion until Chapter 16, ''Troubleshooting.''

it. Until computers are able to think for themselves, it is always going to take human intervention to get a node to operate correctly in a LAN.

The following sections list network hardware common in networks today. Not all the devices listed are in place in every network. They are available to anyone who needs the device in order to support implemented or planned standards within a network.

3.3.1 End-User Interface Hardware Types

A network exists to serve the needs of the end users. The network administrator (head honcho, big daddy, C-3PO, or whatever else the person is called) plans very carefully to ensure that the right equipment is purchased and brought into the network. The hardware has to be able to support data traffic needs as well as the necessary standards and protocols. Look at it this way: it wouldn't do you any good to buy a cell phone from one vendor and then order the cell phone plan from another vendor. Most likely, the cell phone would never work.[26]

The end users interface with some specific hardware devices that they need to do their job. In Figure 3-13, you can see an example of some of the many hardware devices that an end user may actually interface with. At the very least, an Internet user will have a PC or laptop and an adapter of some sort that will allow the PC to connect to a network. In many office environments, multiple users will share the services of a printer, fax machine, or copy machine. The network is what allows them to do this. For the purposes of this chapter, we will not discuss the end-user direct access hardware. It would be information that you are most likely familiar with.

3.3.2 Connecting End Users

Although there are many different user interface types out there, we are going to focus on the PC or laptop as the user interface type for the remainder of this book. If we enter into discussions of other user network interfaces, we will define these as they come up.

RANDOM BONUS DEFINITION

wireless fidelity (Wi-Fi) — A term that describes certain types of 802.11 WLANs.

[26] Jim heard on the news the other day that a cell phone vendor out there claims its service will work with any other vendor's plan. Looks like maybe we can all get along.

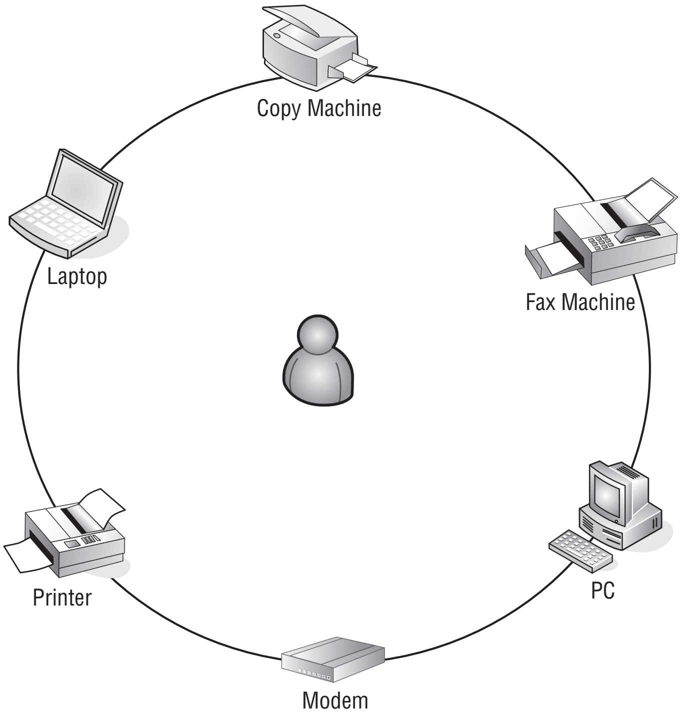

Figure 3-13 End-user hardware types

The user interface is the device, software application, software program, or other tool the user uses to complete a network transmission. The network interface is the physical interface that allows the network node to connect to the network.

It's important to note the distinction between a network interface and a user interface. Take a look at Figure 3-14. Really, you couldn't tell a user to go interface with a router and send an e-mail to 192.168.2.2. Now look at Figure 3-15. The opposite holds true, as well: you can't tell a router to send an e-mail to your brother Joel in Abilene.

End users interface with cell phones, telephones, PDAs, PCs, e-mail programs, word processing programs, and a variety of other software and hardware tools. They may go as far as installing a network adapter so they can connect to the network, but the adapter really is not a user interface; it's a way for a PC (or other node) to pass and receive data to and from a network.

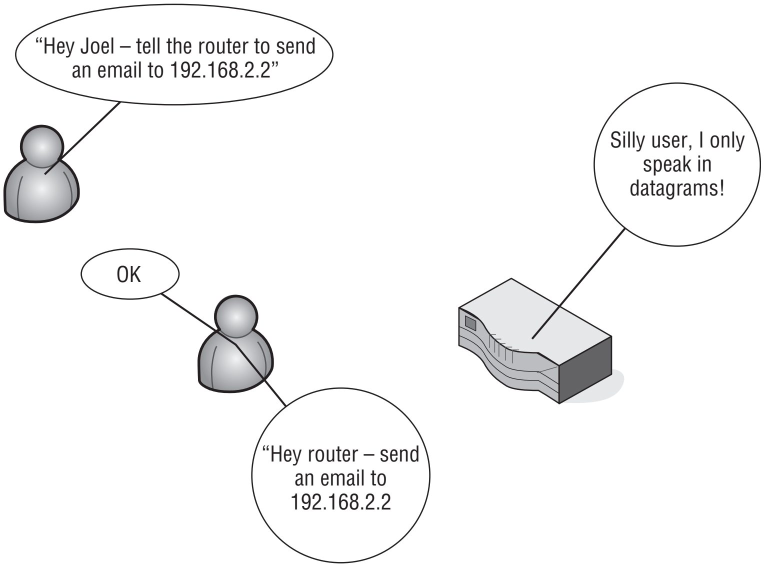
"Hey Joel – tell the router to send an email to 192.168.2.2"
OK
Silly user, I only speak in datagrams!
"Hey router – send an email to 192.168.2.2

Figure 3-14 A user trying to interface with a router

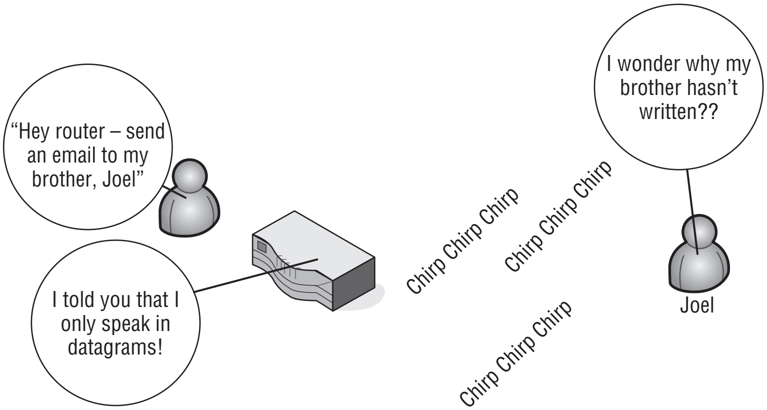
"Hey router – send an email to my brother, Joel"
I told you that I only speak in datagrams!
Chirp Chirp Chirp
Chirp Chirp Chirp
Chirp Chirp Chirp
I wonder why my brother hasn't written??
Joel

Figure 3-15 A router trying to send an email to a user

3.3.2.1 Network Interfaces and Adapters

Like many other things in networking, the terms *interface* and *adapter* can have various meanings (and sometimes they mean the same thing).

We already discussed user interfaces and the types that are associated in that group. We are now going to discuss network interfaces and network adapters. Before we do that, take a look at how Merriam-Webster defines an interface and an adapter.

RANDOM BONUS DEFINITION

Worldwide Interoperability for Microwave Access (WiMAX [IEEE 802.16]) — A task force responsible for the IEEE 802.16 standards for broadband wireless access (BWA) networks

in·ter·face[27]
noun
1: a surface forming a common boundary of two bodies, spaces, or phases (an oil-water interface)
2 a: the place at which independent and often unrelated systems meet and act on or communicate with each other (the man-machine interface)
b: the means by which interaction or communication is achieved at an interface transitive verb
1: to connect by means of an interface (interface a machine with a computer)
2: to serve as an interface for
adapt·or[28]
also adap·ter
noun
1: one that adapts
2 a: a device for connecting two parts (as of different diameters) of an apparatus
b: an attachment for adapting apparatus for uses not originally intended

A network interface is any device or method that serves as an access point to a data path among various network nodes within a network. A network interface is also the point that connects users with a network that is outside the boundaries of their LAN. Network interfaces provide a way for a node to speak to other nodes, regardless of the standards that are in place along the data path.

There is more to a network interface than simply installing it and then plugging in a cable. The network interface is also able to convert data from proprietary or noncommon standards to one that is shared, thus allowing nodes to communicate with another one even if they don't have the same protocols implemented. A network interface connects end-user devices to a network. The network interface controller (NIC) that is in a standard desktop computer is a type of network interface. The point at the boundary of a LAN,

[27] *Merriam-Webster Online Dictionary*. Retrieved May 9, 2008, from `www.merriam-webster.com/dictionary/interface`.
[28] *Merriam-Webster Online Dictionary*. Retrieved May 9, 2008, from `www.merriam-webster.com/dictionary/interface`.

which connects the LAN to an outside network, is another type of network interface. In Layer 3 environments, *interface* is often the term used to describe a network connection and really isn't considered hardware.

Network adapter is usually the term given to the hardware interface to the network. Previously we said that an NIC card is a network interface that a computer uses. An NIC card is also referred to as a network adapter.[29] The NIC card adapts to the computer, allowing it to have an interface to the network. Confused yet? Wait — there's more. There is also what is known as a *virtual network adapter*, which is an application that assists a computer to connect to the Internet without a physical adapter. This is usually done over WiFi or WiMAX.

We really shouldn't dwell on this much longer. With practice, you will learn how to *adapt* to your fellow networking gurus and can *interface* with one another while talking about how great this book is and how much you enjoyed reading it.[30] You will get a better feel for adapters and interfaces throughout the remainder of this book. It's not as difficult as it may seem, we promise.

3.3.2.2 Network Interface Controllers

The network interface controller (NIC)[31] is a hardware card that allows a PC to participate in passing and receiving data on a network. An NIC is commonly referred to as an *NIC card*, *LAN card*, *LAN adapter*, *network card*, *network adapter*, *Ethernet adapter*, and a few other names. Often the name may be a reference to technology the NIC is supporting (i.e., an Ethernet card). All are entirely acceptable and, regardless of what term you use, generally understood by whoever is participating in the discussion.[32] Figure 3-16 shows an example of an NIC card.

NIC cards operate at Layers 1 and 2 of the OSI reference model. Because NIC is a physical connecting device, providing a user with network access, it is a Layer 1 device. However, because it uses a system for addressing nodes, it is also a Layer 2 device. NIC cards[33] have a 48-bit serial number assigned to them, which is the MAC address. NIC cards normally take one of two forms; they can be an expansion card that has to be physically inserted into the bus on the PC motherboard or they can be integrated into the motherboard. You may also have interfaces that have a difference connector type, such as a USB interface.

[29] A good portion of the time if someone says ''network adapter,'' they are talking about an NIC card. Or the adapter at the end of a cable (serial adapter, Ethernet adapter, etc.).

[30] It seemed like a good time for a shameless plug.

[31] Some people assume that NIC stands for network interface card. This is not correct, although the term NIC card is accepted by most. If NIC were network interface card, then an NIC card would be a network interface card card.

[32] If you are ever unsure, just ask someone.

[33] Okay. We said that it was a funny term, but it's one we are comfortable with. It is less awkward to ask someone, ''Who do you buy the NIC card from?'' than ''Where did you get that NIC?''

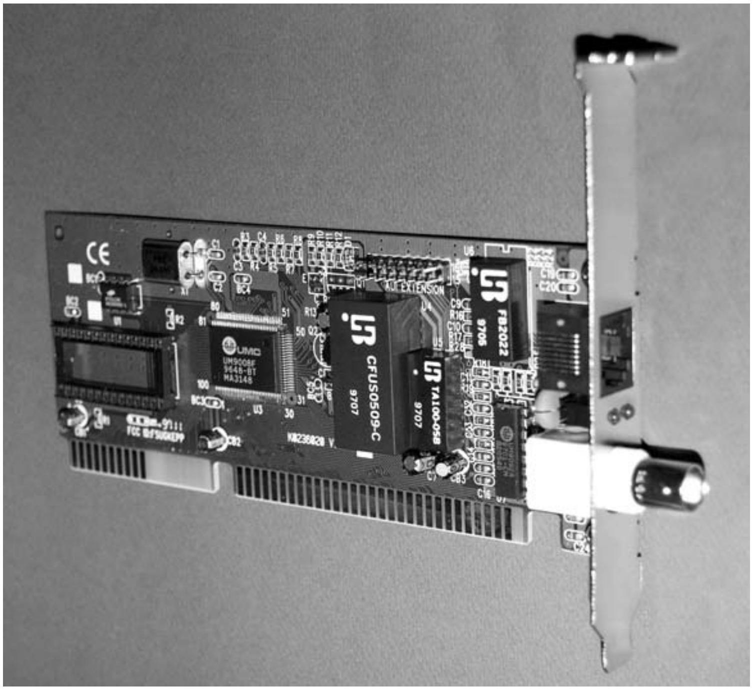

Figure 3-16 An NIC card

3.3.3 To Boldly Go Where Data Needs to Flow (or, How Does that E-mail Get to Brother Joel?)

We have our cables, computers, NIC cards, buses, and all the things we need to get our bits to hit the NIC card and travel across our UTP to a destination on the other side of the LAN. As you can see in Figure 3-17, our bits just are not going to go very far. The application sends the data to our NIC card, who forwards it on to the medium, who just cannot figure out where the bits should go.

We all know that the example in the preceding paragraph is simplistic, but if you think about it, that is about all we have covered so far. Well, folks, it's time now for us to talk about the nodes in the network. Some of these nodes you may not ever come across in real life, and others you will become very familiar with. There are a lot of different nodes in a network, and often equipment from many different vendors of node types is implemented within the same network.[34] When designing a network, it is important to put the right node in place to perform the right job. You really don't need a router

[34] Don't put all of your eggs in one basket.

in a bridged network, nor would you try to use a repeater to connect to your Internet service provider (ISP).

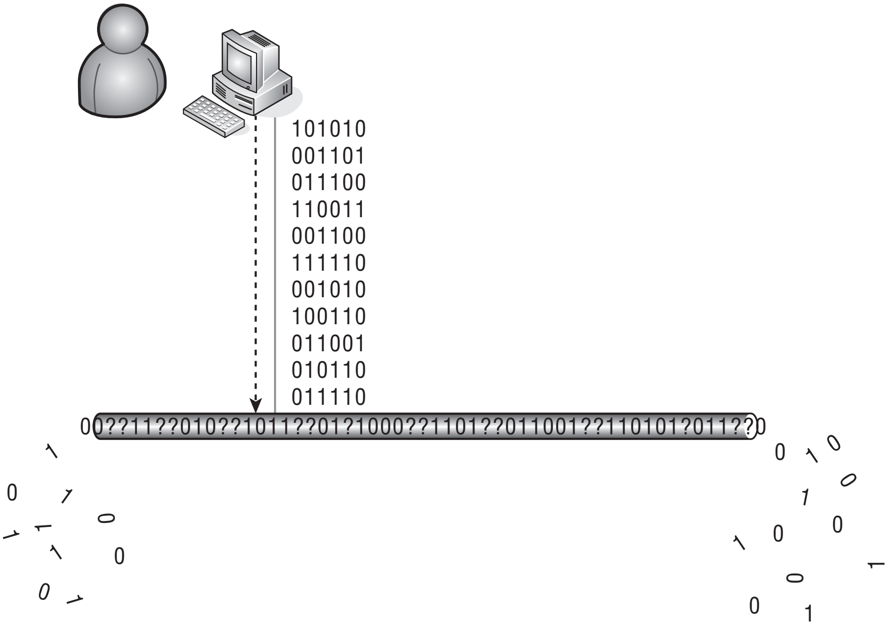

Figure 3-17 Sending data to the pseudo-net

This section does not provide an in-depth discussion of the standards involved with and the modus operandi of any individual node. Most of these will be covered in upcoming chapters. This section is more of an introduction to networking hardware. Where does the data go when it leaves your computer? What other nodes might you be using and not even realize it? These are the types of questions you will be able to answer when you are done with this section. The next time you hear someone say, ‘‘Hey, what’s all the hubbub?’’ you may be able to come up with a witty quip in response.

3.3.3.1 Concentrators

A network *concentrator* is a node that is able to multiplex signals and then transmit them over a single transmission medium. Most concentrators support multiple asynchronous[35] channels and one high-speed synchronous channel. The term *concentrator* is often used generically when referring to some nodes

[35] In data communication, an *asynchronous* process is one that does not require a clocking mechanism in order to work. A *synchronous* process does require clocking — in other words, it has to be synchronized in order to work.

known as hubs (see next section). A concentrator usually provides *point of presence (POP)* access for remote users, as well as performing other functions.[36]

3.3.3.2 Hubs

Hubs are commonly used to connect devices within network segments[37] to one another. Figure 3-18 shows an example of a typical hub deployment in a network segment. Notice in the figure, the hub actually supports data rates of both 10 Mbps and 100 Mbps. There are a lot of different types of hubs, with varying numbers of hosts supported. Some support multiple data rates while some only support a single data rate. The hub that is appropriate for your environment should be chosen based on the needs of the network and the end users.

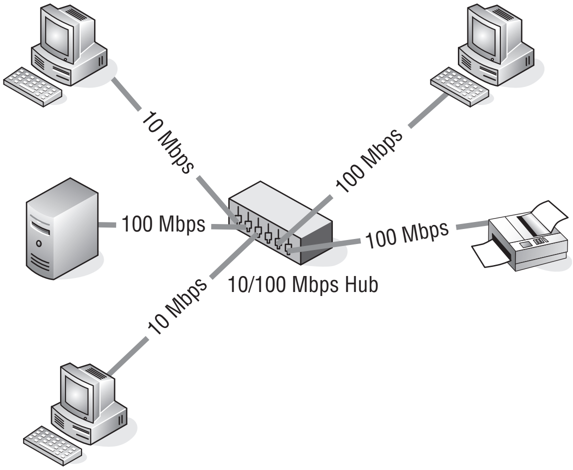

Figure 3-18 Hub deployment

When data is received by a hub, the hub forwards the received data to all the nodes that connect to it. All ports see datagrams received on any other ports within the hub. Hubs are considered *shared media*, as there are multiple hosts sharing a common transmission medium. If a hub is made aware of a collision (data that collides when two or more hosts try to pass data at the same time), it will signal the other ports to stop transmitting until the collision is resolved. Hubs also

ACRONYM ALERT

FPGA — Field-programmable gate array

[36] Some concentrators are also able to perform high-layer functions, such as routing.

[37] Segments are areas of a LAN that are contained within a boundary with the boundary termination node being a router, switch, or a bridge.

typically determine if one of the ports is having problems (excessive collisions, corrupted data, etc.). If so, the hub can react and shut the port off from the rest of the shared media. Hubs are considered Layer 1 nodes.

Hubs have largely been replaced in recent years, due to the popularity and cost reduction of network switches, though they are still in use for many home and small business networks. Additionally, hubs can be used to copy datagrams that are sent to or received by a specific node and have that information forwarded to one or more network monitoring connections.

3.3.3.3 Media Access Units

Media access units (MAUs), also referred to as *multi-station access units*,[38] function similarly to hubs, but for Token Ring networks. Data flows through the MAU in a logical ring topology, although the physical topology is a star topology configuration. The MAU can recognize any hosts that are inactive and disable the port the host is on so as not to disrupt the operation of the logical ring. MAUs are considered Layer 1 nodes.

Take a look at Figure 3-19. You see that all hosts are physically connected to the MAU in a star topology, while communication between the hosts is still performed as if the hosts were physically connected in a ring.

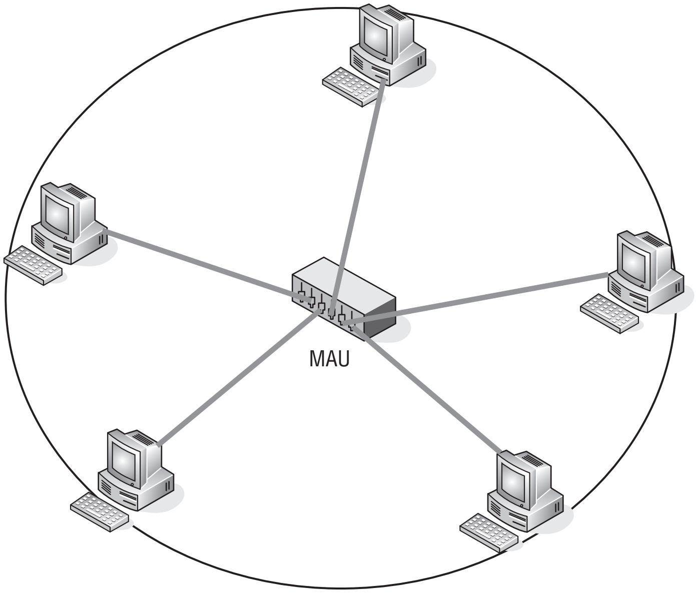

Figure 3-19 An MAU — physical star, logical ring

[38] There are two acronyms that are common when referring to the multi-service access unit, MAU and MSAU.

3.3.3.4 Repeaters

POP QUIZ

What does MAU stand for?

Repeaters are used to give data the extra push it needs to reach an endpoint. Transmission media has distance limitations before the signal experiences degradation, known as *attenuation* or *signal loss*. When the distance limit has been reached, instead of placing another switch, hub, or router in the path, a repeater is used.

The role of the repeater is simple: it accepts data and then retransmits it to the other side. Copper and fiber optic cabling are both supported by repeaters geared for the cabling type. Additionally, there are repeaters available for networks that use wireless as a transmission medium.

3.3.3.5 Bridges and Switches

Functionally, bridges and switches are pretty much interchangeable. Both are Layer 2 devices that support and perform the same basic function of joining network segments within the LAN (see Figure 3-20). Bridges traditionally were very small (some had only two port interfaces). When sold on the market, some bridges fetched a very expensive price, especially if they could support data rates that matched the rates supported by the transmission media in place.

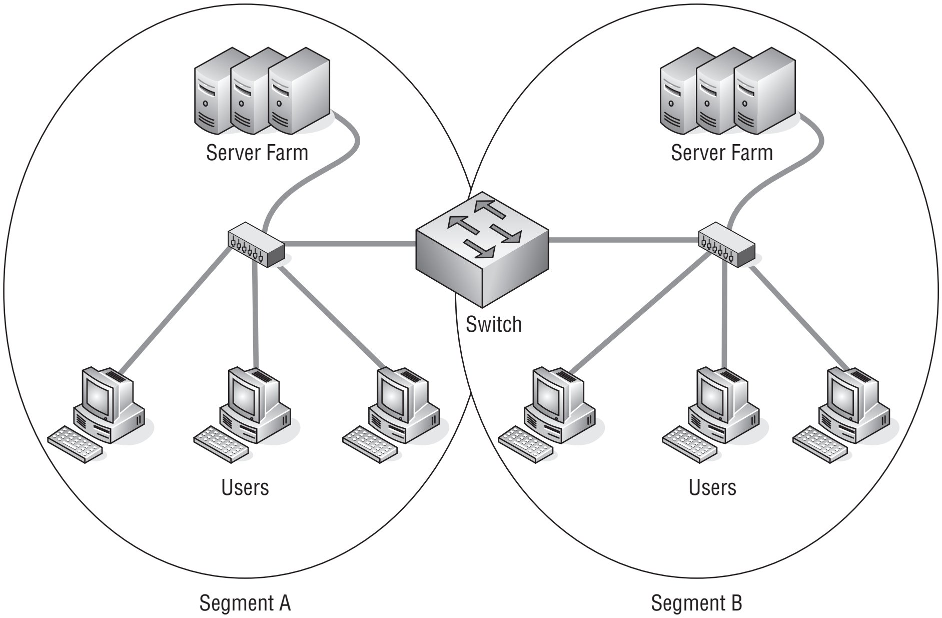

Figure 3-20 An example of a switch bridging two LAN segments to one another

In the late 1980s and the early 1990s, the demand started growing for faster systems and faster networks. LANs were expanding to the point where a shared media network was no longer able to handle the demand. Advancements in technology paved the way for system resource (processor and memory) advancements, which allowed vendors to build nodes with more flexibility in the number of ports than traditional bridges could support, all at the speed supported by the connected transmission medium. These nodes were termed *switches*, but their functions remained the same as what a bridge did — the switch just was able to do more of it. The term *switch* is more of a marketing term, used to separate the legacy nodes from the new and improved version.[39] For the most part, a bridge is a switch and a switch is a bridge and both do more than a hub.

AN UNRELATED MOMENT OF PAUSE

Too bad they didn't think of these:

- **AMIGA — A Merely Insignificant Game Addiction**
- **BASIC — Bill's Attempt to Seize Industry Control**
- **CD-ROM — Consumer Device, Rendered Obsolete in Months**
- **COBOL — Completely Obsolete Business-Oriented Language**
- **DOS — Defective Operating System**
- **ISDN — It Still Does Nothing**
- **LISP — Lots of Infuriating and Silly Parentheses**
- **MIPS — Meaningless Indication of Processor Speed**
- **PCMCIA — People Can't Memorize Computer Industry Acronyms**
- **PENTIUM — Produces Erroneous Numbers Through Incorrect Understanding of Mathematics**
- **SCSI — System Can't See It**
- **WWW — World Wide Wait**

Switches have almost completely replaced hubs in today's networks. The prices of switches and hubs are fairly close when taking into account the number of supported hosts. Some reasons why switches are preferred over hubs are that switches are configurable, support more hosts within a single node, and perform faster and more reliably than a hub.

[39] The sales and marketing folks continue to do this today. In Sections 3.3.3.7 and 3.3.3.8, we will discuss upper-layer switching (Layer 3 switching, web switching, application switching, etc.), which is nothing like traditional switching, but it sounds good and it sells.

RANDOM BONUS DEFINITION

buffer — A block of memory used to store data temporarily.

Switches are deployed in various locations in a network. Switches are able to determine the best path to a network segment through the use of the *Spanning Tree Protocol (STP)*. STP allows a network to be designed to include redundant links, which ensures that data gets to its destination if the primary link fails. STP also ensures that there are no loops in the network, which might be introduced with the addition of the redundant links. Spanning Tree has had many improvements made in the past few years. We will discuss the Spanning Tree Protocol further in Chapter 11, ''The Data Link Layer.''

Switches are also capable of being configured with multiple *virtual LANs (VLANs)*, which allow nodes to communicate as if they were all connected within the same LAN segment, regardless of where the nodes physically reside. In a VLAN environment, broadcast messages are only sent to the interfaces that are members of the VLAN, leaving the remainder of the switch the opportunity to serve other areas. Figure 3-21 shows an example of the logical topology of a fully meshed switched network.

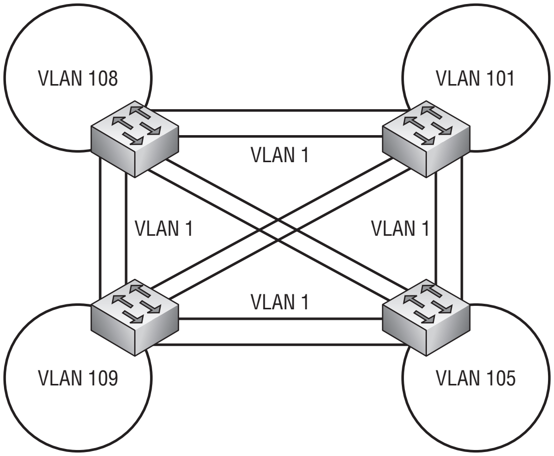

Figure 3-21 LAN switch deployment

Take note of all the available links and let's take a moment to discuss what problems may occur if there were no way to control the flow of data. Keep in mind that switches forward data in the direction of the node that knows where the MAC address of the destination is. In the example, if a host in VLAN 108 needs to get data to a host in VLAN 105, and there is nothing configured on the switch to assist in forwarding decisions, which path would the data take?

Each switch would flood the data out all other switches and would continue to do so at an alarming rate. Keep in mind that there are other nodes in other VLANs doing the same thing. A basic example, but enough for you to see that there are problems. That is what makes switches special — all the tools available today to address these issues and many more that may arise. We will discuss switching in more detail in Chapter 11.

3.3.3.6 Routers

Routers make it possible for our e-mails to make it to their destination. They make the decisions that are necessary to get data from one user to another. It would be virtually impossible to meet the demands of users today without a router in the mix, helping make decisions on how to get data from point A to point B.

Routers are advanced network nodes that connect networks of different types. Routers are intelligent enough to know how to get data from a Token Ring subnet to an Ethernet subnet, without data corruption of any kind. Routers support many protocols and standards that allow much more flexibility in their deployment. A router can be placed in the network to join two or more LANs together, two or more WANs, a LAN to an ISP, and so on. Figure 3-22 shows a router joining two networks to one another and joining both of them to the Internet.

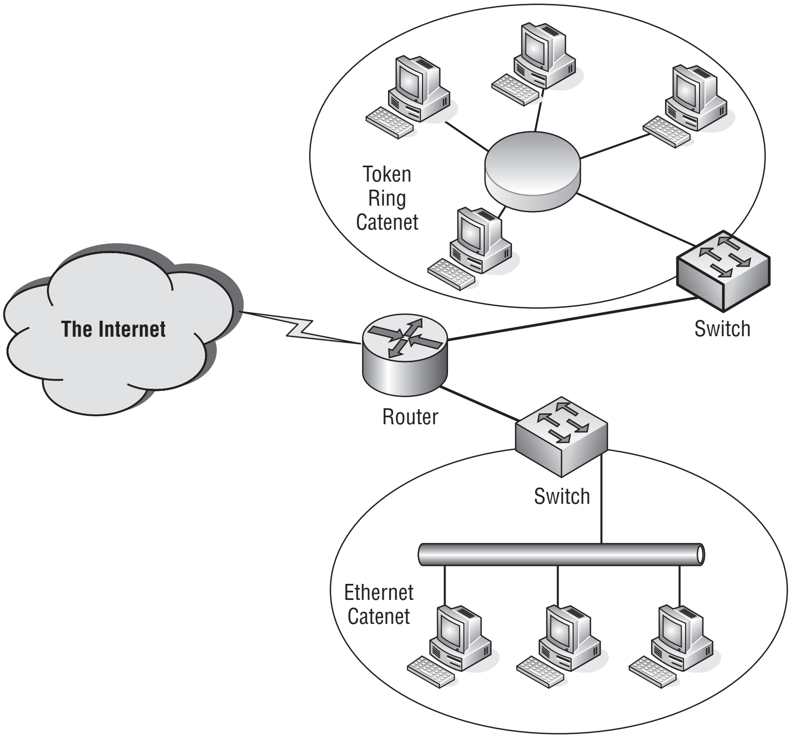

Figure 3-22 An example of a router deployment

POP QUIZ

At which layer of the OSI model does a switch operate?

Routers operate at Layer 3 of the OSI reference model and use IP addresses for data delivery. Routers also are able to communicate with other routers and share path information, so when a packet is received, it can be sent toward its destination over the best path possible. Routers run algorithms to assist in determining the best path, and they share information with one another, so every router can be on the same page. Routers ensure that data gets to where it is supposed to go.

Routers maintain routing tables that help determine where the best path is to a destination. The routing table includes information that shows what subnets the router has learned and the path to the next node (next hop) that leads to the destination IP address. The routing table is able to place a metric or cost to a destination to assist in routing decisions. The entries in the routing table can be configured (static) or learned via a routing protocol such as RIP or OSPF. Following is an example of a routing table:

```
Active Routes:
Network Destination Netmask Gateway Interface Metric
 0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.104 1
 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
 192.168.1.0 255.255.255.0 192.168.1.104 192.168.1.104 1
 192.168.1.104 255.255.255.255 127.0.0.1 127.0.0.1 1
 192.168.1.255 255.255.255.255 192.168.1.104 192.168.1.104 1
 224.0.0.0 224.0.0.0 192.168.1.104 192.168.1.104 1
 255.255.255.255 255.255.255.255 192.168.1.104 192.168.1.104 1
Default Gateway: 192.168.1.1
```

In the example, you can see that the routing table has information on the destination addresses that it is aware of, the subnet mask that is assigned to the destination IP address, the *gateway* (next hop to destination), the interface through which the data needs to go in order to reach the gateway, and the metric assigned to the destination. The metric is the number of hops to a destination. If there is only one route, the metric is ignored. If there are multiple routes to a destination, the one with the lowest metric is used.

Routers can be as simple as a router in a home office to as complex as an Internet backbone router. Routers support multiple protocols and interfaces, which allows them to be operated and translate data coming from multiple network types. Routers are discussed in greater detail in Chapter 10, ''The Network Layer.''

3.3.3.7 Layer 3 Switches

RANDOM BONUS DEFINITION

bit — A unit of data that is either a 0 or a 1.

Section 3.3.3.5 discussed traditional Layer 2 switches and the functions they perform. Layer 3 switches can operate at Layer 2, as well as function like a router. Layer 3 switches can be configured to make routing decisions to send data to a destination. Routers use software to perform logic decisions for operation and use a microprocessor to perform packet switching. Layer 3 switches have replaced the need for software logic decisions and some hardware that routers rely on with integrated circuitry to perform these tasks. The circuitry that is used is known as *application-specific integrated circuits (ASICs)*.

Layer 3 switches combine the wire speed technologies used by Layer 2 switches and the tools necessary to route packets as a router. Layer 3 switches make routing decisions based on the same routing table information as a traditional router does. As far as the hardware design, a Layer 3 switch and a router look a lot alike in many cases. Both are configurable and the higher end ones have slots where different types of modules can be inserted, increasing the protocols that are supported by the node.

Layer 3 switches are predominately developed for larger corporate LANs. The Internet still utilizes routers in the core to get data to a destination. Most Layer 3 switches are not able to support the WAN interfaces required for routing Internet data. Layer 3 switches are often referred to as *routing switches* or *Ethernet routing switches*.

Layer 3 switches also have the ability to control the flow of data by implementing what is known as *class of service* (CoS), which provides for packet queuing into classes of service to ensure that data with a higher priority is attended to before data with a lower priority.

3.3.3.8 Upper-Layer Switch Types

There are nodes that perform functions at Layer 4 and above of the OSI reference model. The term *switch* is more of a marketing term, as these nodes are nothing like traditional Layer 2 switches. Some of the terms that are assigned to switches that fall in the upper-layer category include:

- Multilayer switches
- Server load balancer switches
- Web switches
- Layer 7 switches
- Application switches
- Layer 3 switches
- Layer 4 switches

- Layer 4–7 switches
- Content switches

POP QUIZ

At which layer of the OSI model does a router operate?

The previous section discussed the Layer 3 switch. The Layer 3 switch is able to route data much like a router at wire speed, as well as function as traditional Layer 2 switches. Layer 3 switches are also sometimes referred to as multilayer switches.

A Layer 4 switch operates at the Transport layer and expands the functions that are performed by Layer 2 and Layer 3 switches. Layer 4 switches prioritize data based on applications that are in use. A Layer 4 switch provides for CoS to be deployed throughout the LAN (not just within the switch). An example of providing priority for applications would be in a LAN where e-mail traffic takes precedence over Telnet traffic. These parameters can be configured so if there are some users who need Telnet more than e-mail, it can be configured to allow for this. Layer 4 switches are also referred to as multilayer switches.

Server load balancers (SLBs) distribute traffic destined for a server. They share the load for requests between multiple servers, without the end user even being aware that there is any node between them and the server. Figure 3-23 shows an example of a switch performing load balancing for HTTP requested to a website.

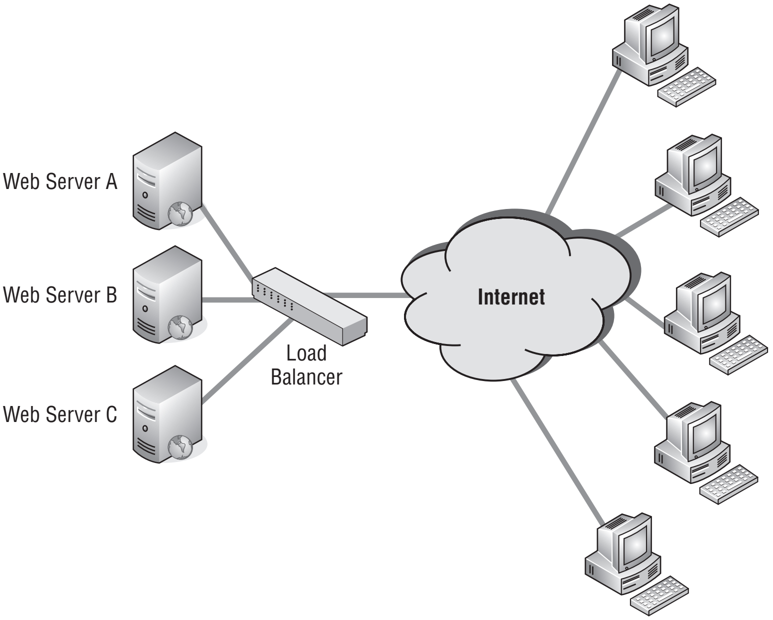

Figure 3-23 Deployment of a server load balancer

Load balancers also spoof the IP address of the server, which helps secure the servers from attack. Load balancers divide requests destined for the server among all the servers that are attached to the load balancer. If a load balancing solution is not in place, all traffic hits the same server, which could potentially cause latency and rejecting of requests to the server.

Some of the upper-layer switches are also able to cache data for speedy access. These functions are known as *data acceleration*. Some also support cryptographic protocols — for instance, Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Load balancing, data acceleration, cryptographic protocols, and many more things.[40] Who could ask for anything more?[41]

3.3.3.9 Remote Access

Network nodes that are used to provide remote users the capability of accessing a computer or network from a remote location are known as *remote access nodes*. Many corporate LANs utilize VPN technology to allow users into the LAN from any location, as long as they have access to the Internet. Some users may not have access to the Internet, and in those cases, they can use a modem to connect to the remote location.

Home users also have modems that allow them to connect to the service provider. Once connected, the users can digitally travel to almost anywhere in the world. They can also use VPN client software to connect to the VPN server (or rather, to the node that is running the server software). Remote access technology, like many other networking technologies, has grown by leaps and bounds in the last decade. Remote access (with the necessary applications) allows people to telecommute and work from remote locations as often as necessary.[42] Additionally, remote access gives small offices the capability to connect to the corporate LAN to conduct business. This is a much cheaper option than what was provided in the 1980s to early 1990s.

RANDOM BONUS DEFINITION

modulation — The process of manipulating a waveform to create a signal that sends a message. In data communications, modulation is performed by a node that converts a digital signal to an analog signal, in order to be communicated over a phone line.

[40] That's what Layer 4–7 switches are made of.

[41] We assure you: someone is always asking for more.

[42] Or as long as the boss will allow them to do so.

Remote access gives clients, vendors, and partners the capability to connect to the corporate LAN. The system administrator controls who gets to go where once they are on the LAN. In this section, we discuss the hardware nodes that provide an avenue for these technologies to exist.

3.3.3.9.1 Modems

The term *modem* is derived from its two main functions. A modem modulates and demodulates. This means that a modem converts digital data to an analog signal and then converts it back again when the data reaches the modem that is connected to the destination node. Figure 3-24 is an example of remote users accessing a corporate network segment via a modem.

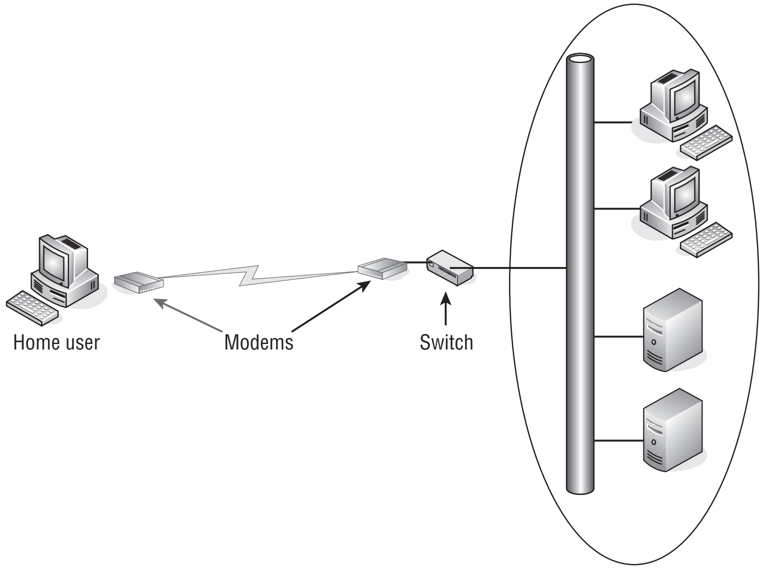

Figure 3-24 Modem remote access

Data that is sent and received by a modem is measured in *bits per second (bps)* or by its *baud rate*. Bps is a measure of the amount of data (number of bits) that can be sent in one second. Baud rate is determined by the type of modulation used and represents the number of times that a signal is changed in one second. The baud rate and the bps rate are not the same number.

Modems that connect a user's PC to a phone line are called dialup modems. Dialup modems are not the only modem type that is available. Internet access is now available to most people in the United States and other parts of the world at very high data rate speeds. There are different types of modems available to the average user as well as businesses and other organizational types. Here is a list of a few of these:

- Cable modem
- Asymmetric digital subscriber line (ADSL) modem
- Digital subscriber line (DSL)
- Microwave modem
- Optical modem
- Wi-Fi modem

The type of modem to use really depends on the needs of the user(s). A person who plays video games online would be much happier with a cable or DSL modem over the traditional dialup modem. Someone who goes online to send and receive e-mail once a week can probably survive with a dialup modem.[43]

3.3.3.9.2 VPNs

VPN technology provides a way for a remote user or branch office to connect virtually to a remote LAN over the Internet. A VPN supporting node has three main functions:

- Provide remote access for individual users
- Provide remote access for a branch office or other LAN
- Ensure that only authorized individuals are able to access the LAN

There are many different types of nodes that support VPN technology. Some are called *VPN routers*, *VPN switches*, *extranet routers*, and *extranet switches*. As long as the node in question's predominate jobs are remote access, authentication, and encryption, the node is VPN-compatible. VPN hardware supports enhanced security, load-balancing methodologies, and the capability to support an increased number of clients that can be connected at the same time, based on the processing power of the node.

POP QUIZ

What is the common name for a modulator/demodulator?

[43] But good luck with opening some of those attachments.

3.3.3.9.3 Wireless

Wireless remote access is a growing technology. Many business and companies are providing access to the Internet and/or the LAN for their customers and employees. There are two main nodes that are needed for wireless remote access. You need to have an end user with a wireless NIC (WNIC) and an access point for them to connect to. The end user is known as the wireless client. Access points are the boundary nodes for the network. A wireless client would be any node that is used to connect to the network without a solid communication path. Figure 3-25 shows an example of wireless remote access.

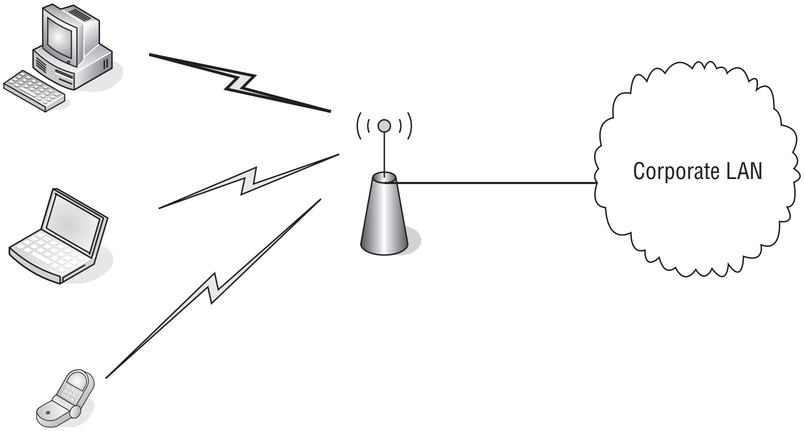

Figure 3-25 Wireless remote access

Some examples of these client node types would be:

- Cellular phones
- IP phones
- Laptops
- Workstations
- Computers

Notice that a wireless client does not have to be a portable device. It can be a stationary device as well, as long as it has an interface that supports wireless technology. There are many access point nodes; some are integrated into other network node types. Within networks that are completely wireless there are wireless bridges, switches, routers, and so on, just as there would be in any wired LAN.

3.3.3.10 Servers

Network servers are nodes that manage the resources available to the users of the network. There are many different types of servers, normally named for the function they perform. A few examples include:

- **Print servers** — Manage traffic destined to a network printer.
- **File servers** — Store files for network users.
- **Network servers** — Manage the traffic on the network.
- **FTP servers** — Manage file transfer.
- **Mail servers** — Manage e-mail traffic.
- **Fax servers** — Manage incoming and outgoing fax messages.
- **List servers** — Manage mailing lists.
- **Proxy servers** — A node that resides between a client and a server, whose purpose is to manage requests destined to the server. Proxy servers allow for shared connections and free the server up so the performance of the server from a end-user perspective is greatly improved.

Network servers are nodes that are dedicated to the technology they are configured to support. These nodes have nothing else to worry about but that specific function. Some servers can have multiple applications running and therefore have the resources necessary to support each of those. Even if the node is running multiple applications, the application itself is the server and is still referenced by the function it is set to do.

RANDOM BONUS DEFINITION

AppleTalk — A protocol suite developed by Apple Computer.

3.4 Chapter Exercises

1. Explain what ''10 half or 100 full?''[44] means to you, what the difference is between 10 half and 100 full, and list pros and cons of each.
2. List three types of interfaces and three types of adapters.
3. Why is an NIC card considered both an interface and an adapter?

[44] We told you that someone would ask this someday.

4. List three examples of flash memory.
5. List the PDU for each of the OSI layers:

Layer	**PDU**
Application	__________
Presentation	__________
Session	__________
Transport	__________
Network	__________
Data Link	__________
Physical	__________

6. What is the difference between volatile and nonvolatile memory?
7. What is the difference between STP and UTP cabling?
8. Explain when you would want to use MMF cables instead of SMF cables. Next, explain in what instances SMF cabling would be preferred over MMF cabling.
9. Define *modulation*.
10. What is the main difference between a Layer 3 switch and a router?

3.5 Pop Quiz Answers

1. The decimal number 211 is equal to what binary number?

   11010011

2. The binary number 01011100 is equal to what decimal number?

   92

3. What is the binary name for the binary value of 2^{50}?

   Pebibit (Pibit)

4. Define *RAM*.

   Volatile memory that is available for data storage and access, regardless of the order in which it was received.

5. Define *encapsulation*.

   Encapsulation is the act of including data from an upper-layer protocol within a structure in order to transmit the data.

6. What is IEEE Standard 802.11?

   IEEE 802.11 is the standard that is maintained by the IEEE outlining WLAN communications. Sometimes, IEEE802.11 is also referred to as Wi-Fi, although traditional Wi-Fi standards are not included in IEEE 802.11.

7. What does MAU stand for?

   Media access unit

8. At which layer of the OSI model does a switch operate?

   Layer 2

9. At which layer of the OSI model does a router operate?

   Layer 3

10. What is the common name for a modulator/demodulator?

    Modem