CHAPTER 1

INTRODUCTION TO COMPUTER NETWORKS

After reading this chapter and completing the exercises, you will be able to:

Describe basic computer components and operations

Explain the fundamentals of network communication

Define common networking terms

Compare different network models

In only a few decades, computer networks have evolved from being a complex technology accessible to only the most tech-savvy users to being part of most people's everyday lives. Computer networks can be found in almost every business, school, and home. Their use is available to anyone with a mobile device or computer and a network connection, but installation and upkeep of all but the smallest networks still require considerable know-how. This chapter starts you on the path toward acquiring the skills to manage a large corporate network or simply configure a home network with a wireless router.

This chapter begins by discussing the computer and its role in a network to give you a foundation for the topics in this book. Next, you examine the components of a network and the fundamentals of communication between computers. Many new terms are introduced and defined, and the varied types of networks and network servers you might encounter are described.

About the Hands-On Activities

The hands-on projects in this book require setting up your lab environment so that it's ready to go, so make sure you read and follow the step-by-step instructions in the "Before You Begin" section of the Introduction, which help you set up your lab for all projects in this book.

The hands-on projects in this book contain information about how networks work that's best understood by hands-on experience. If you can't do some of the projects, you should at least read through each one to make sure you don't miss important information. Table 1-1 summarizes what you need for the hands-on projects in this chapter.

Table 1-1 Hands-on project requirements

Hands-on project	Requirements	Time required	Notes
Hands-On Project 1-1: Examining a Computer's Boot Procedure	Net-*XX*	10 minutes	A Windows 10 computer configured as described in "Before You Begin" The ability to access the firmware setup screen
Hands-On Project 1-2: Upgrading a Stand-alone Computer to a Networked Computer	Net-*XX*, a NIC, a patch cable, and a hub or switch	30 minutes	A lab computer set up as described in "Before You Begin"
Hands-On Project 1-3: Viewing Network Software Layers	Net-*XX*	10 minutes	
Hands-On Project 1-4: Using `ipconfig`, `ping`, and `arp`	Net-*XX*	15 minutes	
Hands-On Project 1-5: Exploring Peer-to-Peer Networking	Net-*XX*	15 minutes	
Hands-On Project 1-6: Creating a Shared Folder	Net-*XX*	15 minutes	
Hands-On Project 1-7: Transferring a Document to Another Computer	Net-*XX*	15 minutes	A share named NetDocs on the instructor's computer (Net-Instr)
Hands-On Project 1-8: Looking Up Computer and Networking Acronyms	A computer with Internet access	20 minutes	Internet access

An Overview of Computer Concepts

At the heart of a computer network is the computer. Networks were created to facilitate communication between computing devices, which ultimately facilitates communication between people. So, to better understand networks, how they work, and how to support them, you must have a solid understanding of computer operations. In fact, most of the devices you encounter when working with a network involve a computer. The most obvious are network servers and workstations that run operating systems, such as Windows, Linux, UNIX, and Mac OS X. Not as obvious are devices such as routers and switches, which move network data from computer to computer and network to network. These complex devices are also computers, although they're specialized computers for performing specific tasks. Other types of nontraditional computers include smartphones, smart watches, home assistants like Amazon Echo and Google Home, and smart "things" such as appliances, thermostats, and even lamps, which are collectively referred to as **Internet of Things (IoT)** devices. The next sections discuss the basic functions of a computer and its associated components, along with computer hardware, the boot procedure, and the basic functions of an operating system (OS). Networking is the focus of this book, but your grasp of the fundamentals of computer components and operations helps you understand networking components and operations.

Basic Functions of a Computer

A computer's functions and features can be broken down into the three basic tasks all computers perform: input, processing, and output. Information is input to a computer from a device such as a keyboard or from a storage device such as a hard drive; the central processing unit (CPU) processes the information, and then output is usually created. The following example illustrates this process:

- *Input*—A user running a word-processing program types the letter A on the keyboard, which results in sending a code representing the letter A to the computer.
- *Processing*—The computer's CPU determines what letter was typed by looking up the keyboard code in a table.
- *Output*—The CPU sends instructions to the graphics card to display the letter A, which is then sent to the computer monitor.

Some components of computers are designed to perform only one of these three functions; others are designed to perform two or all three functions. For example, a standard keyboard and mouse perform input functions, and storage devices, such as hard drives, perform both input (when files are read from the drive) and output (when files are written to the drive). Network cards can perform all three functions. A network card is an output device when data is sent from the computer to the network and an input device when data comes from the network to the computer. In addition, many

network cards have rudimentary processors that perform actions on incoming and outgoing data to help supplement the computer's main CPU.

Input Components

Before a computer can do any processing, it requires input, commonly from user-controlled devices, such as keyboards, microphones, Webcams, and scanners. External interfaces, such as serial, FireWire, and USB ports, can also be used to get input from external devices.

Input is also generated by storage devices, such as hard disks and CDs/DVDs that store programs and data files containing computer instructions and data. For example, a spreadsheet program, such as Microsoft Excel, might contain instructions for the CPU to calculate formulas for adding the values of two columns of data and a spreadsheet file called `MyBudget.xls` containing the numbers and formulas the spreadsheet program should use. Both the program (Microsoft Excel) and the data file (`MyBudget.xls`) are used as input to the CPU, which then processes the program instructions and data.

A spreadsheet program normally starts when a user double-clicks the spreadsheet program icon or the icon representing the spreadsheet data file. These actions are instigated by user input. Sometimes, however, your computer seems to start performing actions without user input. For example, you might have noticed that your hard drive sometimes shows activity without any obvious action from you to initiate it. Or, a notification might pop up on your screen reminding you of a calendar event. However, inputs to a computer can include timers that cause programs to run periodically and data arriving from network cards, for example, that cause a program or process to run. So, although it sometimes seems as though your computer has a mind of its own, computers don't actually do anything without first getting input to jolt them into action.

Processing Components

A computer's main processing component is the CPU, which executes instructions from computer programs, such as word-processing programs and Web browsers. It also runs the instructions making up the OS, which provides a user interface and the environment in which applications run. Aside from the CPU, computers usually include ancillary processors associated with input/output (I/O) devices, such as graphics cards. These processors are often referred to as "onboard processors." The processor on a graphics card, called a "graphics processing unit (GPU)," takes a high-level graphics instruction, such as "draw a circle," and performs the calculations needed to draw the circle on a display device. With an onboard GPU, the main CPU doesn't have to handle many of the complex calculations graphical applications require, thereby improving overall system performance. Other devices, such as network interface cards and disk controller cards, might also include onboard processors.

CPUs are usually composed of two or more processors, called **cores**, in one package. A **multicore CPU** is like a person with two brains. With only one brain, you

could add four numbers, but you would probably do it in three sequential summing operations: Add the first number to the second number, take the first sum and add it to the third number, and add that sum to the fourth number to arrive at the final sum. If you had two brains, you'd still need three summing operations, but two could be done simultaneously: The first brain adds the first two numbers while the second brain is adding the third and fourth numbers; then the second brain gives its results to the first brain, and the first brain sums the results of the first two summing operations. So, multicore CPUs enable computers to carry out multiple instructions simultaneously, which results in better overall performance when running demanding applications.

Output Components

Output components include monitors and printers, but they also include storage devices, network cards, and sound cards, to name a few. The external interfaces mentioned previously as input components can be used as output components, too. For example, a disk drive connected to a USB port allows reading files from the disk (input) and writing files to the disk (output).

Storage Components

Storage components are a major part of a computer's configuration. Generally speaking, the more storage a computer has, the better the performance is. As you saw in the previous section, most storage components are both input and output devices, allowing data to be saved (output) and then accessed again later (input). When most people think of storage, they think of disk drives, CD/DVD drives, and USB or flash drives. However, there are two main categories of storage: short-term storage and long-term storage.

RAM: Short-Term Storage

Short-term storage is the random access memory (RAM) on a computer. RAM is short-term storage because when power to the computer is turned off, RAM's contents are gone, just as though you erased a whiteboard. When power is restored, RAM has no data stored until the CPU begins to write data to it.

The amount of RAM, or memory, in a computer is crucial to the computer's capability to operate efficiently. RAM is also referred to as "working storage." Everything the CPU is currently processing must be available in RAM, including program instructions and the data the current application requires. So, to run a spreadsheet program, there must be enough RAM to load both the spreadsheet program and the data in the spreadsheet. If there's not enough available memory, the spreadsheet program won't run, or the computer uses the disk drive to supplement RAM temporarily.

Neither option is desirable. The reason temporary use of the disk drive isn't optimal is because RAM is thousands of times faster than the fastest disk drives. The time required to access data in RAM is measured in nanoseconds (billionths of a second), but access to data on a disk drive is measured in milliseconds (thousandths

of a second). So, if the disk drive must be used to supplement RAM while running an application, that application, and indeed the entire computer, slows down precipitously.

On current desktop computers, the amount of RAM installed is usually 4 GB or more. More is generally better, but the amount of RAM you actually need depends on how you use your computer. If you usually have only one or two typical business applications open at once, 2 GB might be enough. However, if you run complex graphics applications or games or have several applications open simultaneously, you'll likely benefit from having more RAM.

Long-Term Storage

Long-term storage maintains its data even when there's no power. Examples include hard disks, CDs/DVDs, solid-state drives (SSDs), and USB flash drives as well as other types of removable media. Long-term storage is used to store document and multimedia files as well as the files that make up applications and the OS. The amount of storage a computer needs depends on the type and quantity of files to be stored. In general, office documents, such as word-processing files, spreadsheets, and presentations, require comparatively little space. Multimedia files—pictures, music files, and videos—require much more space. Long-term storage is plentiful and extremely inexpensive. Hard drive specifications are in hundreds of gigabytes, with multi-terabyte (a terabyte is 1000 GB) drives quite commonplace. More details about hard disks are discussed later in "Personal Computer Hardware."

Data Is Stored in Bits

Whether storage is long term or short term, data on a computer is stored and processed as **binary digits** ("bits," for short). A **bit** holds a 1 or 0 value, which makes representing bits with electrical pulses easy. For example, a pulse of 5 volts of electricity can represent a 1 bit, and a pulse of 0 volts (or the absence of a pulse) can represent a 0 bit. Bits can also be stored as pulses of light, as with fiber-optic cable: A 1 bit is represented by the presence of light and a 0 bit as the absence of light.

Data in a computer, such as the letters in a word-processing document or the music played from an MP3 music file, is represented by collections of 8 bits, called a **byte**. You can look at each byte as a printable character in a document. For example, a single byte from an MP3 file plays about 1/17 thousandth of a second of music. To put it another way, one second of MP3 music takes more than 17,000 bytes.

Bits, Bytes, Megabytes, and Beyond

Some types of computer information are expressed in bits and others are expressed in bytes. For example, when we talk about how fast a network connection is, the speed is usually expressed in bits, as in 100 million bits per second or 100 Mbps. When we talk about how much data a hard disk can store, the capacity is expressed in bytes, as in 100 billion bytes or 100 GB. Notice that when expressing bits, a lowercase b is used, but when expressing bytes, an uppercase B is used. If you want to convert bits to bytes,

simply divide by 8; for example, 100 Mbps would be about 12.5 MBps. Conversely, to convert bytes to bits, multiply by 8. All of the prefixes used to express large numbers of bits or bytes can be confusing, so Table 1-2 is given as a reference. Notice that each prefix increases the previous prefix by a factor of 1000; for example, 1 megabyte is equal to 1000 kilobytes.

Table 1-2 Prefixes used for expressing bits and bytes

Prefix	Value
Kilo (K)	Thousand (10^3)
Mega (M)	Million (10^6)
Giga (G)	Billion (10^9)
Tera (T)	Trillion (10^{12})
Peta (P)	Quadrillion (10^{15})
Exa (E)	Quintillion (10^{18})
Zeta (Z)	Sextillion (10^{21})
Yotta (Y)	Septillion (10^{24})

Note

Table 1-2 isn't exactly right because computers do everything in binary, including how they count. So, a kilobyte is actually 1024 or 2^{10} bytes. A megabyte is 1000 kilobytes, which is actually 1,048,576 bytes, but it's much easier for us humans to work with round numbers like million and billion. So, when estimating storage capacity, we round 100 GB to 100 billion bytes instead of the more difficult 107,374,182,400 bytes.

Personal Computer Hardware

Most people are familiar with personal computer (PC) hardware. Other types of computers, such as minicomputers and mainframes, are usually locked away in a heavily air-conditioned room and privy only to the eyes of IT staff. The basic hardware used to build a PC or a mainframe differs only in the details. This section describes four major PC components housed in a computer case:

- Motherboard
- Storage device
- RAM
- Firmware

The Motherboard and Its Components

The motherboard is the nerve center of a computer, much like the spinal cord is the nerve center of the human body. It's a network of wires and controlling circuits that connects all computer components, including the CPU, RAM, disk drives, and I/O devices, such as network interface cards. Some key components of a motherboard are labeled in Figure 1-1 and explained in Table 1-3.

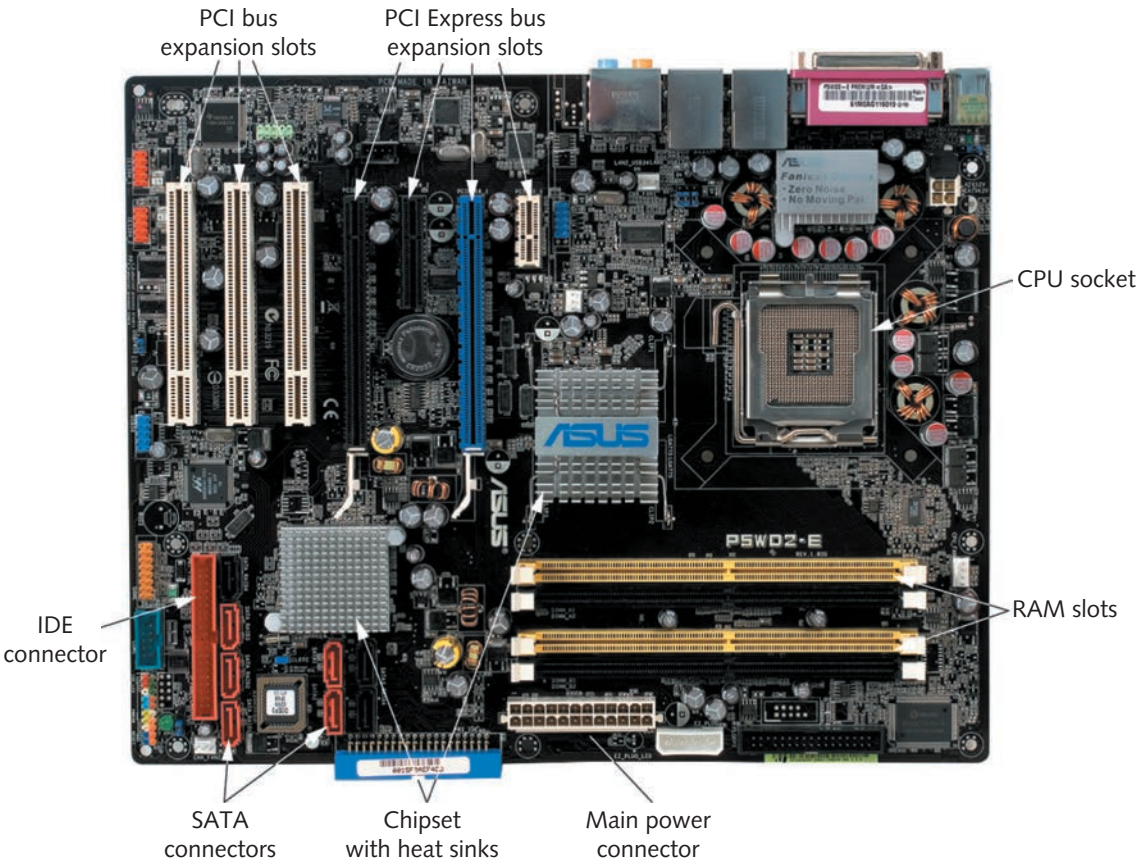

Figure 1-1 A PC motherboard

All data that goes into or comes out of a computer goes through the motherboard because all storage and I/O devices are connected to the motherboard, as is the CPU, which processes data going in and coming out of a computer.

Computer Bus Fundamentals

Table 1-3 mentions PCI Express bus expansion slots as a component of a motherboard. A **bus** is a collection of wires carrying data from one place to another on the computer. There are many bus designs and formats, each for a particular purpose. Although

Table 1-3 Key components of a motherboard

Component	Description
CPU socket	The CPU is installed in this socket.
PCI Express bus expansion slots	Used to add functionality to a PC by adding expansion cards that have a Peripheral Component Interconnect Express (PCIe) connector. The larger slots are suitable for high-performance expansion cards, such as graphics cards and disk controllers. The smaller slots are best suited to sound cards and network interface cards.
PCI bus expansion slots	This older expansion card standard is rarely found on new computers.
RAM slots	Slots for installing RAM on the motherboard.
Chipset with heat sinks	The **chipset** consists of two chips referred to as the Northbridge and the Southbridge. These chips control data transfers between memory, expansion slots, I/O devices, and the CPU. The heat sink sits on top of the chipset to prevent it from overheating.
SATA connectors	Used for connecting hard drives and CD/DVD drives that use the Serial AT Attachment (SATA) specification.
IDE connector	Used for connecting Integrated Drive Electronics (IDE) hard drives and CD/DVD-ROM drives. This older standard is rarely found on new computers.
Main power connector	This connector is where the motherboard receives power from the system power supply.

bus types come and go, it's safe to say that replacements for an older bus design will almost certainly be faster than their predecessor.

In a computer, there are buses between the CPU and RAM, between the CPU and disk drives, and between the CPU and expansion slots, among others. For the purposes of this book, you're most interested in the bus connecting expansion slots to the motherboard because you usually connect a network interface card (NIC) into one of these slots. NIC installation and expansion slot bus types are discussed in Chapter 2. What you need to know now is that not all motherboards come with all types of expansion slots, and the faster and busier your computer is, the faster its bus type needs to be.

Storage Device Fundamentals

Most desktop computers and laptops are likely to come with a hard drive as their primary long-term storage component. Hard drives consist of magnetic disks, called "platters," that store data in the form of magnetic pulses. These magnetic pulses are maintained even when power is turned off. Each pulse represents a single bit of data.

The platters spin at extremely fast speeds, with some faster disks having rotational speeds of 15,000 revolutions per minute (rpm). A read/write head is attached to an actuator arm that moves across the spinning platters in response to commands from the computer to read or write a file (see Figure 1-2). Generally, the faster the rotational speed,

the better the hard drive performance is. When a file is requested to be written or read, its location is determined, and then the read/write heads are moved over the corresponding spot on the platter. After the platter spins to the file's starting location, the read/write heads are activated to read or write the data. The average amount of time platters take to spin into position is called the "rotational delay" or "latency." The amount of time required to move read/write heads to the correct place is the seek time, and the time it takes to read or write data is the transfer time. The average amount of time between the request to read or write data and the time the action is performed is the access time.

Note

The terms used to measure hard drive performance aren't universal among manufacturers, but the terms used in the preceding paragraph represent most specifications.

Figure 1-2 Inside a hard drive

Courtesy of © 2010 Western Digital Technologies, Inc.

Hard disks store the documents you use with your computer as well as the applications that open these documents. In addition, the hard disk stores the OS your computer loads when it boots. As mentioned, the hard disk acts as an input device

when files are read. When the computer boots, the OS files are read from the disk, and instructions in these files are processed by the CPU. However, the files don't go directly from the hard disk to the CPU; first, they're transferred to short-term storage (RAM).

Solid-State Drives

Solid-state drives are used in place of hard drives in many systems because of their speed and reliability. An SSD uses a type of storage called "flash memory" that contains no moving parts and has faster access times than a mechanical hard drive. SSDs are more expensive than hard drives when you compare the price per gigabyte of storage, but their price continues to fall. SSDs are most often used in mobile devices (such as laptops, smartphones, and tablets) but are also found on high-performance desktops and servers, often supplementing, rather than replacing, hard drive storage.

RAM Fundamentals

RAM, the main short-term storage component on a computer, consists of capacitors to store data and transistors to control access to data. Capacitors require power to maintain the bits they store. Because RAM requires continuous power to store data, it's referred to as "**volatile memory**."

RAM has no moving parts, so as mentioned, accessing data in RAM is much faster than accessing data on a hard drive—there's no seek time or rotational delay. Because RAM is so much faster than a hard drive, any information the CPU processes should be in RAM. If data the CPU requires is located on the hard drive, it's loaded into RAM first, which takes considerable time. Therefore, the more RAM your system has, the more likely it is that all the data needed by running programs can be stored in RAM, making the system perform much faster.

Note

While SSDs have no moving parts, they are still considerably slower than RAM, so SSDs will not replace RAM in a system any time soon.

Firmware Fundamentals

A key component of every computer is its firmware. **Firmware** is a computer program stored in **nonvolatile memory**, such as ROM or flash memory. Firmware is located on the motherboard and is executed when the computer is first powered on. Nonvolatile memory is a type of storage that maintains its data after power is removed. The firmware on most PCs is called the **basic input/output system (BIOS)** or **Unified Extensible Firmware Interface (UEFI)**. A main function of the BIOS or UEFI is to tell the CPU to perform certain tasks when power is first applied to the computer, including initializing motherboard hardware, performing a power-on self-test (POST), and beginning the boot procedure.

Because of the complexity of motherboards, configuring some hardware components and tuning performance parameters are often necessary. When a computer begins to boot, the firmware program offers the user an opportunity to run the setup utility to perform this configuration. The configuration data the user enters is stored in **complementary metal oxide semiconductor (CMOS) memory**. It holds information such as possible boot devices, the status of hardware devices, and perhaps a system password, if needed. CMOS is a type of low-power memory that requires only a small battery to maintain its data.

Computer Boot Procedure

To take a computer from a powered-off state to running an OS, such as Windows or Linux, the following steps must take place:

1. Power is applied to the motherboard.
2. The CPU starts.
3. The CPU carries out the firmware startup routines, including the POST.
4. Boot devices, as specified in the firmware configuration, are searched for an OS.
5. The OS is loaded into RAM.
6. OS services are started.

These steps apply to almost every type of computer, including very small computing devices, such as smartphones and tablets. Probably the biggest difference between computers is what occurs in the last step. OS services are programs that are part of the OS rather than applications a user starts. The services an OS starts can vary greatly, depending on which OS is loaded and how it's configured. The number and type of services started on a system are what, at least in part, account for the time it takes a system to boot completely. Examples of common OS services include the user interface, the file system, and, of course, networking services.

Note

The projects in this book involving a Windows client OS use Windows 10 Education Edition. Other editions of Windows 10 can be used.

Hands-On Project 1-1: Examining a Computer's Boot Procedure

Time Required: 10 minutes
Objective: Examine the computer boot procedure and firmware setup utility.
Required Tools and Equipment: Net-*XX* (a Windows computer configured as described in the "Before You Begin" section of the Introduction of this book)

Description: In this project, you examine the computer boot procedure from beginning to end, using a Windows computer. You also examine the firmware setup utility and view the configuration that specifies which devices the firmware should search for an OS. Because the firmware varies among computers, your instructor might have to assist with the keystrokes you enter to run the setup utility and view the boot order menu. This project uses a virtual machine and the setup utility in VMware Workstation. If you aren't using virtual machines for the projects in this book, the setup utility on most computers is similar.

Caution

Your computer must be turned off before you begin this project. Read the first step carefully before turning on the computer, as you need to act quickly to enter the setup utility.

1. Turn on your computer. Watch the screen carefully for a message telling you what key to press to activate the setup utility. On many systems, this key is F1, F2, or Delete. If you don't press the key in time, the OS boots normally. If this happens, shut down the computer and try again.
2. When you have entered the setup utility, your screen might look similar to Figure 1-3, but many setup screens look different. Before continuing, write down the steps of the boot procedure, listed earlier under "Computer Boot Procedure," that have taken place to this point:

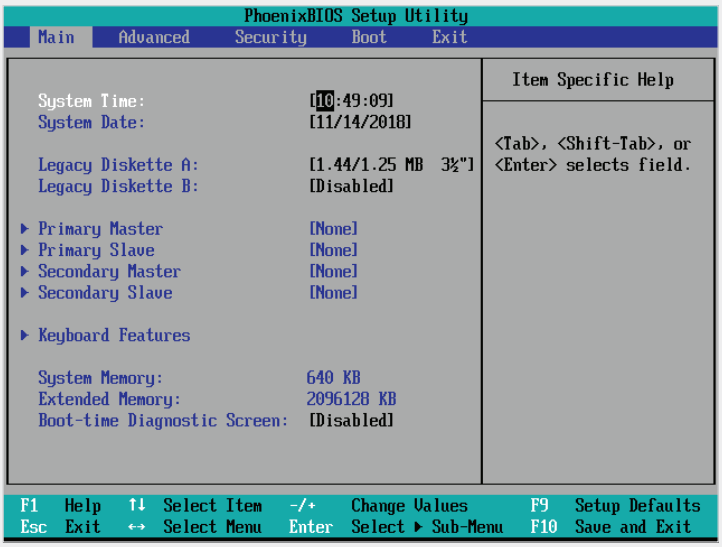

Figure 1-3 The setup utility

Source: Phoenix Technologies, Ltd

3. Navigate the setup utility until you find the boot order menu (see Figure 1-4). You can change the order in which the firmware looks for boot devices or exclude a device from the boot order. The firmware boots from the first device in which it finds an OS. You might need to change the boot order if, for example, you have an OS installed on the hard drive but want to boot from an installation CD/DVD to install a new OS. In this case, you move the CD/DVD device to the first entry in the boot order.

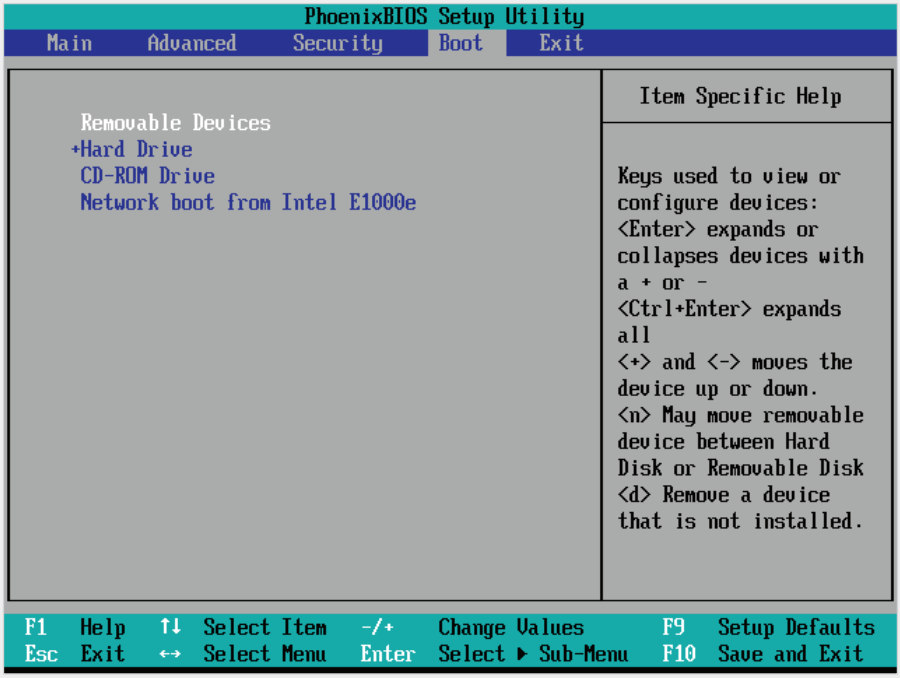

Figure 1-4 The boot order menu

Source: Phoenix Technologies, Ltd

4. For now, you can leave the boot order unchanged. To quit the setup utility, press the correct key (usually specified at the bottom of the screen). In Figure 1-4, you press Esc to exit without saving changes or F10 to save the changes before exiting. In either case, when you exit, the computer restarts. Press the key for exiting without saving changes.
5. Write the final steps of the boot procedure that occurred as Windows started:

_____

_____

_____

6. Shut down the computer for the next project.

The Fundamentals of Network Communication

A computer **network** consists of two or more computers connected by some kind of transmission medium, such as a cable or air waves. After they're connected, correctly configured computers can communicate with one another. The primary motivation for networking was the need for people to share resources, such as printers and hard drives, to share information such as word-processing files, and to communicate by using applications such as e-mail. These motivations remain, especially for businesses, but another motivating factor for both businesses and homes is to "get online"—to access the Internet. The Internet, with its wealth of information, disinformation, fun, and games, has had a tremendous impact on how and why networks are used. Indeed, many of the networking technologies used now that you learn about in this book were developed as a result of the Internet.

You might know how to use a network already; in particular, you probably know how to use programs that access the Internet, such as smartphone apps, Web browsers, and e-mail programs. To understand *how* networks work, however, you need to learn about the underlying technologies and processes used when you open a program that accesses the network. A good place to start is with the components that make a stand-alone computer a networked computer.

Network Components

Imagine a computer with no networking components—no networking hardware or software. It's hard to imagine in this age of seemingly everything being connected. However, not too long ago, when you bought a computer, its main purpose was to run applications such as word-processing and spreadsheet programs, not Web browsers and e-mail. In fact, a computer had neither the hardware nor the software needed for browsers and e-mail. These computers were called **stand-alone computers**. If you wanted to network this type of computer, you had to add these required components:

- *Network interface card*—A NIC is an add-on card that's plugged into a motherboard expansion slot and provides a connection between the computer and the network. Most computers have a NIC built into the motherboard, so no additional card is necessary. NICs are discussed in more detail in Chapter 2.
- *Network medium*—A cable that plugs into the NIC makes the connection between a computer and the rest of the network. In networks with just two computers, the other end of the cable can plug into the second computer's NIC. More likely, the other end of the cable plugs into an interconnecting device that accommodates several computer connections. Network media can also be the air waves, as in wireless networks. In this case, the connection is between the antenna on the NIC and the antenna on another NIC or interconnecting device. Network media are discussed in more detail in Chapter 4.
- *Interconnecting device*—Although this component isn't always necessary because two computers can be connected directly with a cable and small

wireless networks can be configured without an interconnecting device, most networks include one or several of these components. They allow computers to communicate on a network without having to be connected directly to one another. They include switches, hubs, routers, and wireless access points, as discussed in Chapters 2 and 8. A small network connected to a switch is shown in Figure 1-5.

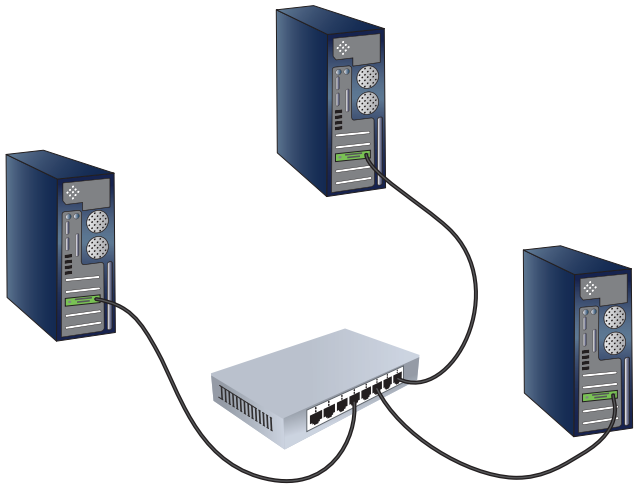

Figure 1-5 A network of computers connected to a switch

The previous list of components satisfies the hardware components needed to make a stand-alone computer a networked computer. The computer must also have the necessary software to interact with network hardware and communicate with other computers on the network. Network software transforms a stand-alone OS into a network OS. It's the software that allows a word-processing program to open a document on a server or knows how to request a Web page or send an e-mail. It's also the software that communicates between the OS and the network hardware. Network software can be divided into the following categories:

- *Network clients and servers*—**Network client software** requests information that's stored on another network computer or device. **Network server software** allows a computer to share its resources by fielding resource requests generated by network clients. Network client software can be an integral part of well-known applications, such as Web browsers and e-mail programs. A Web browser, for example, sends a request for a Web page to a Web server. Network client software can also run in the background, usually installed as

a networking service. In this case, it enables programs without built-in client software to access shared network resources on other computers. For example, Client for Microsoft Networks, which is installed automatically in Windows, allows a word-processing program to open a file that's shared on another Windows computer or print to a printer attached to another Windows computer. In this setup, the server software called File and Printer Sharing for Microsoft Networks receives the request from the client and provides access to the shared file or printer.

- *Protocols*—When clients and servers need to send information on the network, they must pass it to **network protocols**, which define the rules and formats a computer must use when sending information across the network. A network protocol can be likened to a human language. Just as two people who want to communicate must speak the same language, two computers that want to communicate must use the same protocol. An example of a network protocol is TCP/IP. Network protocols do all the behind-the-scenes tasks required to make networking work and handle most of the complexity in networking; they're discussed in depth in Chapter 5.

Note

The term "NIC device driver" is often shortened to simply "NIC driver," which is the term used throughout this book.

- *NIC driver*—After a network protocol has formatted a message correctly, it hands the data off to the NIC driver for transmission onto the network. NIC drivers receive data from protocols and then forward this data to the physical NIC, which transmits data onto the medium. The reverse is also true. When data arrives at the NIC from the medium, the NIC hands it off to the NIC driver, which then hands it off to network protocols. Every NIC installed in a computer must have an associated device driver installed in the OS. The device driver software manages the details of communicating with the NIC hardware to send and receive data to and from network media.

Figure 1-6 shows the Windows representation of a network connection. In the properties of the network connection, you can identify a network client and server, protocols, and the NIC driver. Each of these software components plays a role in the steps of network communication, as described in the next section.

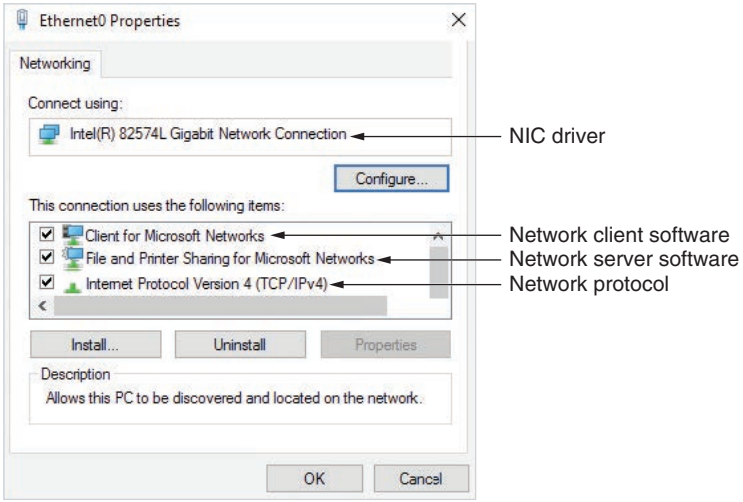

Figure 1-6 The properties of a network connection in Windows

Steps of Network Communication

Most network communication starts with a user needing to access a resource on another computer, such as a Web server or file server. A user's attempt to access network resources is summarized in these basic steps:

1. An application tries to access a network resource by attempting to send a message to it.
2. Network client software detects the attempt to access the network. Client software formats the message generated by the application and passes the message on to the network protocol.
3. The protocol packages the message in a format suitable for the network and sends it to the NIC driver.
4. The NIC driver sends the data in the request to the NIC, which converts it into the necessary signals to be transmitted across the network medium.

Remember that there are two sides to a communication session, and most of them involve a client trying to access network resources and a server providing those resources. The steps taken on the server side are essentially the reverse of those on the client side:

1. The NIC on the server receives signals from the network medium and converts them into message data, which is read by the NIC driver.
2. The NIC driver passes the message to the network protocol.
3. The network protocol determines which server software the message is targeting and passes the message to this designated software. Remember that a computer can have many clients and many servers running at the same time. For example, a computer running Windows Server might be acting as a mail server and a file server. Each server function requires different server software.

4. The server software receives the message and responds by sending the requested data to the client computer, using the four steps outlined previously.

Layers of the Network Communication Process

Each step of a client accessing network resources is often referred to as a "layer" in the network communication process. Each layer has a specific function to accomplish, and all the layers work together. Figure 1-7 depicts this process. Keep in mind that the steps outlined previously simplified the communication process, which is one reason the layered approach is so effective: Complex concepts can be described in simple steps. Chapter 7 discusses the layered approach to networking in more detail, and Chapter 5 explains the role of protocols in network communication.

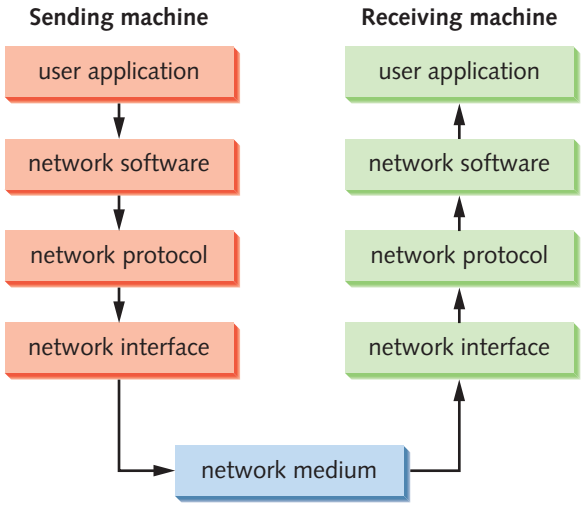

Figure 1-7 Layers of the network communication process

Note

The layers shown in Figure 1-7 and described in Table 1-4 are a simplified version of actual layered models such as the TCP/IP model and OSI model, both of which are discussed in later chapters.

As you'll see in Chapter 7 when the OSI model of networking is discussed, the layers are given different names and divided into additional pieces. What's important now is grasping the idea of a layered approach, in which a complex process is broken into manageable steps, each with a specific role to play. Table 1-4 maps the resource access steps listed previously to the four layers in Figure 1-7.

Table 1-4 Layers of the network communication process

Step	Description	Layer
1	An application tries to access a network resource.	User application
2	Client software detects the attempt to access the network and passes the message on to the network protocol.	Network client or server software
3	The protocol packages the message in a format suitable for the network and sends it to the NIC driver.	Network protocol
4	The NIC driver sends the data in the request to the NIC, which converts the data into the necessary signals to be transmitted across the network medium.	Network interface

How Two Computers Communicate on a LAN: Some Details

The layers of the network communication process give an overview of how network communication works. However, few details have been provided on what each layer accomplishes. This discussion focuses on computer addresses and how they're used during network communication.

In a network using a protocol such as TCP/IP (the most common network protocol), computers have two addresses: a logical address and a physical address. The logical address is the IP address, and the physical address is called the Media Access Control (MAC) address. You can look at these two addresses much like the addresses used to send mail through the postal system. When a letter is mailed in the United States, it requires a street address and a zip code. The zip code gets the letter to the correct region of the country, and the street address gets the letter to the correct home or business.

Note

The MAC address is stored as part of the physical NIC, which is why the MAC address is referred to as the "physical address."

You can liken the zip code to the logical or IP address and the street address to the physical or MAC address. When a message is sent on a network, the IP address is used to get the message to the correct network, and the MAC address gets the message to the correct computer on this network. If the sender and receiver are on the same network, the IP address in the message is used mainly as a means to ascertain the destination computer's MAC address.

For example, Figure 1-8 shows two computers connected to a switch. Computer A wants to communicate with Computer B. One of the simplest forms of communication is a ping. The `ping` command sends a message from one computer to another,

essentially asking the other computer whether it's listening on the network. If a computer receives a ping, it replies so that the sending computer knows the message was received. It's like the cell phone commercial with a person asking "Can you hear me now?" Here are the steps of this communication process:

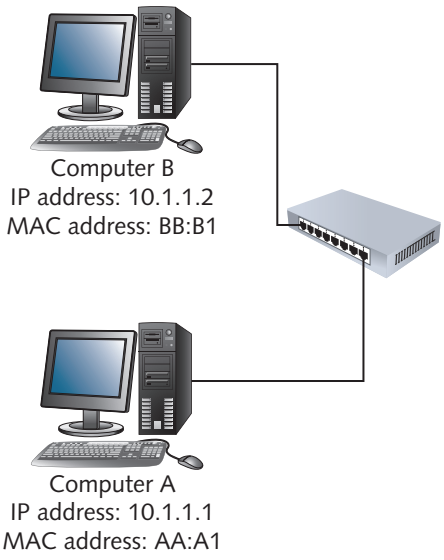

Figure 1-8 Communication between two computers

1. A user at Computer A types `ping 10.1.1.2` (the IP address of Computer B) at a command prompt.
2. The network software creates a ping message.
3. The network protocol packages the message by adding IP addresses of the sending and destination computers and acquires the destination computer's MAC address.
4. The network interface software adds MAC addresses of the sending and destination computers and sends the message to the network medium as bits.
5. Computer B receives the message, verifies that the addresses are correct, and then sends a reply to Computer A using Steps 2 through 4.

Users don't usually initiate network communication by using a computer's IP address; instead, they use the computer name. However, just as you can't mail a letter with only the recipient's name, you can't communicate over a network with only the computer's name. You certainly know the name of the person you're writing to, but you might have to look up his or her address in your address book before you can address the envelope. Similarly, computers use an address book of sorts, called a **name server**, to get a computer's IP address, given its name. TCP/IP provides name server functions through its Domain Name System (DNS, discussed in more detail in

Chapter 5). With this information in mind, the preceding steps can be expanded as follows:

1. A user at Computer A types `ping Computer B` at a command prompt.
2. A name lookup is done to retrieve Computer B's IP address.
3. The network software creates a ping message.
4. The network protocol packages the message by adding IP addresses of the sending and destination computer and acquires the destination computer's MAC address.
5. The network interface software adds MAC addresses of the sending and destination computers and sends the message to the network medium as bits.
6. Computer B receives the message, verifies that the addresses are correct, and then sends a reply to Computer A using Steps 3 through 5.

Quite a few details in these steps have been left out for now, but they're expanded on in the TCP/IP discussion in Chapter 5. Next, take a look at an example of using a network to save a word-processing document to a Windows server and see how the layers of the network communication process are used. Several components are involved in this task, as you see in Hands-On Project 1-3. In this example, shown in Table 1-5, a user at ClientA is running a word-processing program, such as Microsoft Word, and wants to save the file to a shared folder on another Windows computer named ServerX.

Table 1-5 Saving a file with the network communication process

Step	Description	Layer
1	The user on ClientA clicks Save in the word-processing program and chooses a shared folder on ServerX to save the file.	User application
2	Client for Microsoft Networks detects the attempt to access the network, formats the message, and passes the message to the network protocol.	Network software
3	The network protocol (in this case, TCP/IPv4) packages the message in a format suitable for the network interface and sends it to the NIC driver.	Network protocol
4	The NIC driver sends the data in the request to the NIC (in this case, Ethernet0), which converts it into signals to be transmitted across the network medium.	Network interface
5	ServerX's NIC receives the message from the network medium, processes it, and sends the data to TCP/IPv4.	Network interface
6	TCP/IPv4 on ServerX receives the message from the NIC, processes it, and sends the data to the network software (in this case, File and Printer Sharing for Microsoft Networks).	Network protocol
7	File and Printer Sharing for Microsoft Networks formats the message and requests that the OS save the file to the disk.	Network software

Note

In Table 1-5, there's no "User application" step on the server. When a server is involved, typically the last step is handled by network software, such as File and Printer Sharing for Microsoft Networks, a Web server, or other server software.

Now that you have a solid idea of how network communication takes place and how networks are depicted in drawings, you can learn some common terms for describing networks and network components in the next section. Along the way, you see more figures of different types of networks.

Hands-On Project 1-2: Upgrading a Stand-alone Computer to a Networked Computer

Time Required: 30 minutes
Objective: Upgrade a stand-alone computer to a networked computer.
Required Tools and Equipment: Lab computer (as specified in the book's lab setup instructions), a NIC, a patch cable, and a hub or switch
Description: In this project, you install a NIC and connect it to an interconnecting device with a cable. This project can be done in groups or as an instructor demonstration. It's intended only to familiarize you with the hardware components needed to make a stand-alone computer a networked computer.

1. Install the NIC, following the steps your instructor provides. This process might involve opening the computer case or simply plugging a USB NIC into a USB slot.
2. Turn on the computer. If necessary, insert a disk containing the NIC driver and follow the instructions for installing it.
3. Using the supplied cable, plug one end into the NIC and the other end into the interconnecting device, which should be a hub or a switch.
4. Examine the indicator lights on the NIC and the hub or switch. There might be one or two lights on each port of the device, depending on its features. There's at least one indicator on the NIC and on each port of the hub or switch that's usually referred to as a "link light." The link light glows when a data connection has been made between the NIC and the hub or switch. Your instructor can supply more details about the indicator lights available on your hub or switch. List the status of indicators on the NIC and the hub or switch port into which the NIC is plugged:

   _____

5. Shut down the computer and unplug and put away the cables.

Hands-On Project 1-3: Viewing Network Software Layers

Time Required: 10 minutes
Objective: View the properties of your computer's network connection and identify the layers of the network communication process.
Required Tools and Equipment: Net-*XX*
Description: In this project, you view the properties of your computer's local area connection and identify the layers of the network communication process. Each network connection in Windows contains the software responsible for the steps of the network communication process.

1. Start your computer, and log on as **NetAdmin**.
2. Open the Network Connections dialog box by right-clicking **Start** and clicking **Network Connections**.
3. Right-click **Ethernet0** and click **Properties** to open the Ethernet0 Properties dialog box (see Figure 1-9).

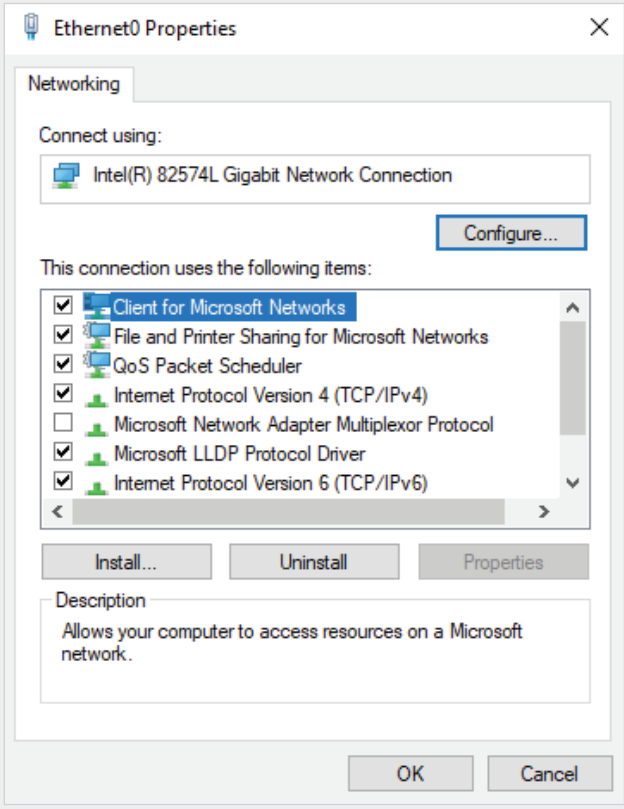

Figure 1-9 The Ethernet0 Properties dialog box

4. The "Connect using" text box displays the NIC. In the list box under it, you see several items. Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks, and Internet Protocol Version 4 are the items you're most interested in right now, as they're the most necessary software components to make network communication work.
5. Assume a user is running a word-processing program and saves a file to a Windows server. Use the information you learned in this chapter to match the appropriate layer of the network communication process with each of the following components. Note that some layers can be used more than once.
   - Word-processing program: _____
   - NIC displayed in the "Connect using" text box: _____
   - Client for Microsoft Networks: _____
   - File and Printer Sharing for Microsoft Networks: _____
   - Internet Protocol Version 4 (TCP/IPv4): _____
6. Close all open windows, but leave your computer running for the next project.

Hands-On Project 1-4: Using `ipconfig`, `ping`, and `arp`

Time Required: 15 minutes
Objective: Use `ipconfig`, `ping`, and `arp` to view and test network addresses and connectivity.
Required Tools and Equipment: Net-*XX*
Description: In this project, you select a partner, use command-line tools to view your network configuration, and test your computer's capability to communicate with other computers. The `ipconfig` command displays the IP address configuration of network interfaces. The `ping` command sends a message to a computer to verify the capability to communicate with it, and `arp` displays the MAC (physical) addresses your computer has discovered.

1. Start your computer, and log on as **NetAdmin**, if necessary.
2. Right-click **Start** and click **Command Prompt** to open a command prompt window. At the command prompt, type **`ipconfig`** and press **Enter**. You should see a screen similar to Figure 1-10, although the numbers you see will vary. The `ipconfig` command lists the IP address configuration for network interfaces as well as other network settings.
3. To see more details about your network configuration, type **`ipconfig /all`** and press **Enter**. You can scroll up the command prompt window to see all the output. Under the heading "Ethernet adapter Ethernet0," find the row labeled Physical Address (see Figure 1-11). The number you see in this row is the MAC address, a 12-digit hexadecimal value. Also, find the IP address in the IPv4 Address row. Write down these two addresses:

_____

_____

```
C:\Users\NetAdmin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : yc-cnt.edu
   Link-local IPv6 Address . . . . . : fe80::90e7:d59d:958:4de3%3
   IPv4 Address. . . . . . . . . . . : 172.31.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.31.1.250

Tunnel adapter isatap.yc-cnt.edu:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : yc-cnt.edu

C:\Users\NetAdmin>
```

Figure 1-10 The `ipconfig` command output

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : yc-cnt.edu
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-F4-62-18
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::90e7:d59d:958:4de3%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Thursday, January 29, 2015 11:21:51 AM
   Lease Expires . . . . . . . . . . : Friday, January 30, 2015 11:21:51 AM
   Default Gateway . . . . . . . . . : 172.31.1.250
   DHCP Server . . . . . . . . . . . : 172.31.1.205
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-5A-EF-95-00-0C-29-F4-62-18
   DNS Servers . . . . . . . . . . . : 172.31.1.205
                                       172.31.1.206
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.yc-cnt.edu:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : yc-cnt.edu
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\NetAdmin>
```

Figure 1-11 Using `ipconfig /all` to list physical (MAC) and IP addresses

4. Tell your partner what your IP address is and make a note of your partner's IP address. At the command prompt, type **`ping IPaddress`** and press **Enter** (replacing *`IPaddress`* with your partner's IP address). You should see output similar to Figure 1-12.

```
C:\Users\NetAdmin>ping 172.31.1.205

Pinging 172.31.1.205 with 32 bytes of data:
Reply from 172.31.1.205: bytes=32 time=1ms TTL=128
Reply from 172.31.1.205: bytes=32 time<1ms TTL=128
Reply from 172.31.1.205: bytes=32 time<1ms TTL=128
Reply from 172.31.1.205: bytes=32 time<1ms TTL=128

Ping statistics for 172.31.1.205:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAdmin>
```

Figure 1-12 Results of the `ping` command

5. Remember that your computer needs both the destination IP address and MAC address to communicate with another computer. You supplied the IP address by typing it at the command prompt. Your computer discovered the MAC address of your partner's computer by using Address Resolution Protocol (ARP). To see this address, type **`arp -a`** and press **Enter**. The output should be similar to Figure 1-13. You might see more lines of output, depending on what other devices your computer has been communicating with. ARP is discussed in more detail in Chapter 5, but for now, just know that it works automatically without user intervention.

```
C:\Users\NetAdmin>arp -a

Interface: 172.31.1.11 --- 0x3
  Internet Address      Physical Address      Type
  172.31.1.205          00-15-5d-01-01-1b     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\NetAdmin>
```

Figure 1-13 The `arp -a` command displays MAC addresses

6. Use the **`ping`** command to communicate with other computers and devices on your network, and use **`ipconfig /all`** to find the addresses of your default gateway (a router in your network) and your DNS servers. Write the MAC addresses of your default gateway and DNS servers:
   - Default gateway: _____
   - DNS servers: _____
7. Close all open windows, but leave your computer running for the next project.

Network Terms Explained

Certification

98-366	Understanding network infrastructures:
	Understand the concepts of Internet, intranet, and extranet
	Understand local area networks (LANs)
	Understand wide area networks (WANs)

Every profession has its own language with its own unique terms and acronyms. Learning this language is half the battle of becoming proficient in a profession, and it's no different in computer and networking technology. The following sections explain some common terms used in discussing computer networks. Because some of these terms are associated with network diagrams, a number of figures are included in the following sections to show different ways of depicting networks.

LANs, Internetworks, WANs, and MANs

A small network that is limited to a single collection of machines and connected by one or more interconnecting devices in a small geographic area is called a **local area network (LAN)**. LANs also form the building blocks for constructing larger networks called "internetworks." In Figure 1-14, the computers in a LAN are interconnected by a switch, and Figure 1-15 shows a wireless LAN.

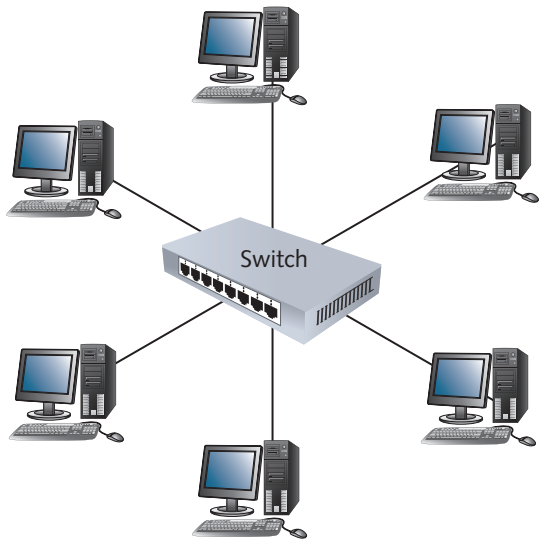

Figure 1-14 A LAN with computers interconnected by a switch

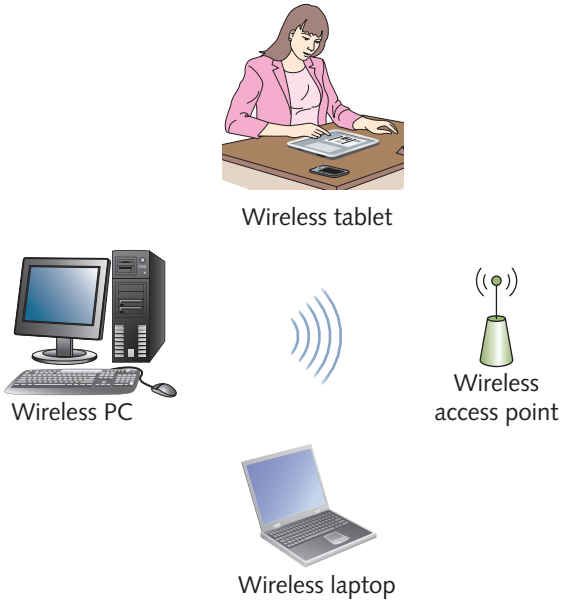

Figure 1-15 A wireless LAN

LANs are represented in other ways, as shown in Figure 1-16; note the different symbols for a hub and a switch. Figure 1-17 shows a logical depiction of the same network; a logical depiction leaves out details such as interconnecting devices, showing only the computers that make up the network.

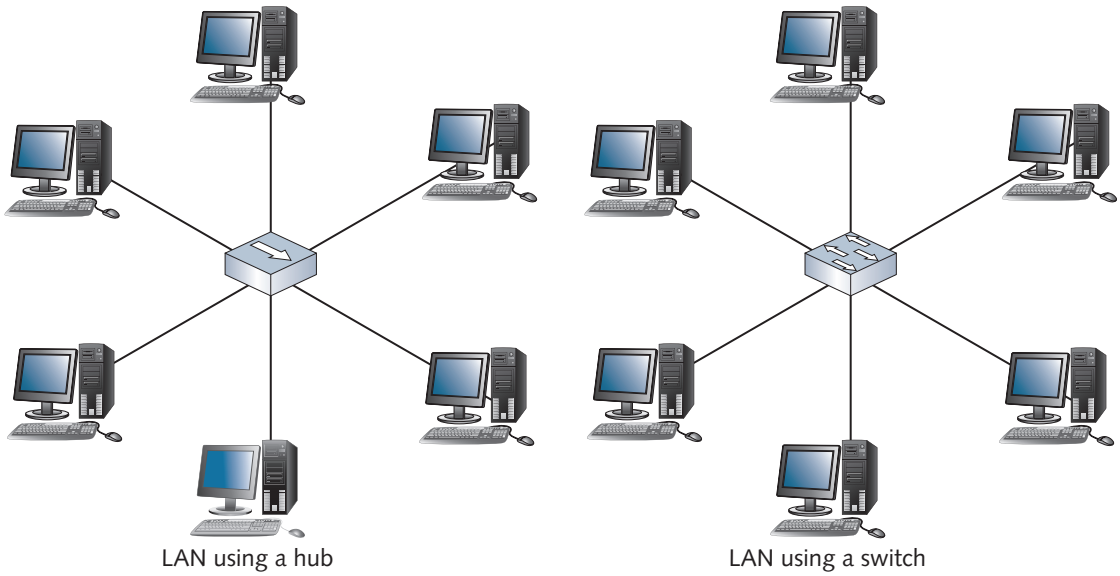

Figure 1-16 A LAN with a symbolic hub (left) and a symbolic switch (right)

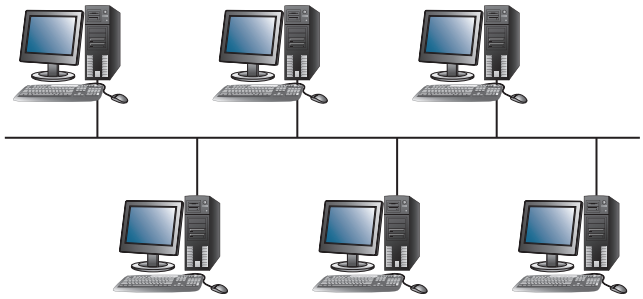

Figure 1-17 A logical depiction of a LAN

An **internetwork** is a networked collection of LANs tied together by devices such as routers, as discussed in Chapters 2 and 8. Figure 1-18 shows two LANs interconnected by a router (represented by the standard symbol). Internetworks are usually created for these reasons:

- Two or more groups of users and their computers should be logically separated on the network yet still be able to communicate. For example, in a school, you might want to logically separate the LAN containing student computers from the LAN containing faculty computers. Routers provide this logical separation but still allow communication between groups, as you see in Chapter 2.

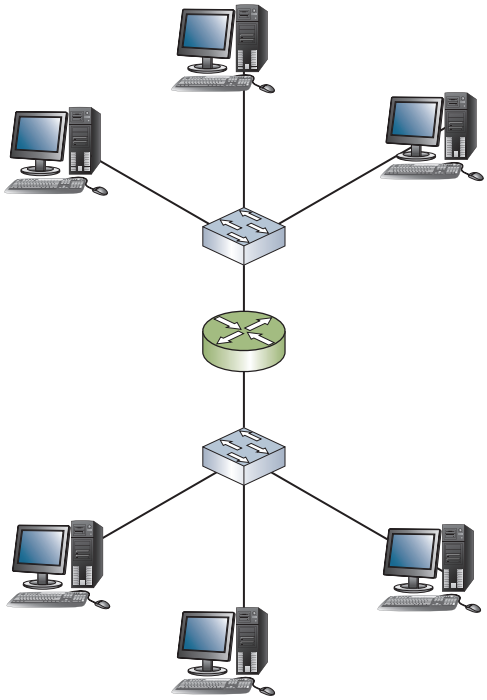

Figure 1-18 An internetwork with two LANs connected by a router

- The number of computers in a single LAN has grown to the point that network communication is no longer efficient. The nature of certain network protocols and devices makes network communication increasingly less efficient as the number of computers on a LAN grows. Routers can be used to separate the computers into two or more smaller LANs, thereby increasing communication efficiency.
- The distance between two groups of computers exceeds the capabilities of most LAN devices, such as hubs and switches. This problem can happen, for example, when a company has multiple buildings or multiple floors in a building. Routers are often used to communicate between groups of computers that are separated geographically.

You might not realize it, but the computer you have at home is probably part of an internetwork. Every time you go online to browse the Web or check your e-mail, your computer (or LAN, if you have a home network) becomes part of the largest internetwork in the world: the Internet.

As a network's scope expands to encompass LANs in geographically dispersed locations, internetworks become classified as **wide area networks (WANs)**. A WAN spans distances measured in miles and links separate LANs. WANs use the services of third-party communication providers, such as phone companies, to carry network traffic from one location to another. So, although both internetworks and WANs connect LANs, the difference lies mainly in the LANs' proximity to each other and the technologies used to communicate between LANs. Therefore, the Internet is both an internetwork and, because it spans the globe, a very large WAN.

Occasionally, you might encounter a network type called a **metropolitan area network (MAN)**. MANs use WAN technologies to interconnect LANs in a specific geographic region, such as a county or city. It's not uncommon to find large, complex networks that use all four network types: LANs and internetworks for purely local access, MANs for regional or citywide access, and WANs for access to remote sites elsewhere in the country or around the world. Take, for example, a nationwide bank. The main branch in a large city has a building with multiple floors and hundreds of computers. Each floor constitutes a LAN, and these LANs are connected to form an internetwork. The internetwork at the main branch is then connected to other branches throughout the city to form a MAN. In addition, the main branch is connected to other branches in other cities and states to form a WAN.

In network drawings, WANs are often shown with a jagged or thunderbolt-shaped line representing the connection between two devices, usually routers, and the Internet is usually represented as a cloud. A cloud is used to obscure the details of a large network, as if to say, "There's some collection of networks and network devices, but the details aren't important." Figure 1-19 shows a WAN connection between two routers with a connection to the Internet. A grouping of three computers is often used to represent multiple computers on a LAN when the exact number doesn't matter.

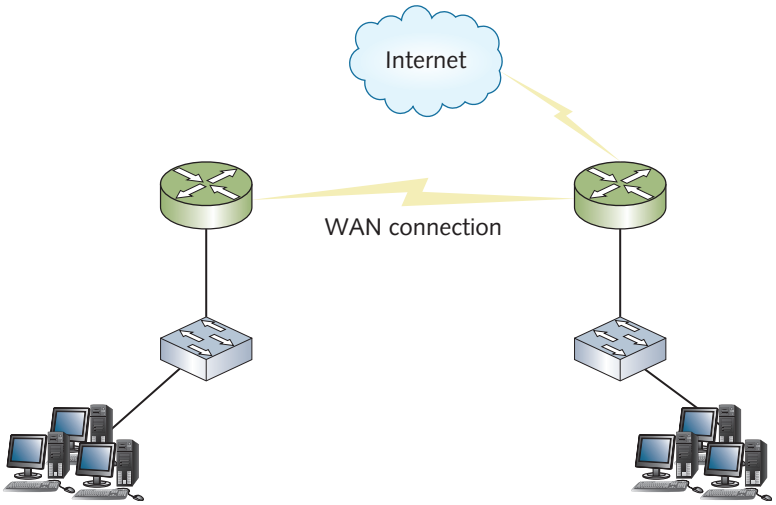

Figure 1-19 A WAN with a connection to the Internet

Internet, Intranet, and Extranet

The **Internet** is a worldwide public internetwork that uses standard protocols, such as TCP/IP, DNS, HTTP, and others, to transfer and view information. It's a public network because the devices such as routers and Web servers that make up much of the network are accessible directly through an IP address. An **intranet**, on the other hand, is a private network, such as a school or company network, in which the devices and servers are available only to users connected to the internal network. Many of the same protocols and technologies used on the Internet are used to access information on an intranet. An **extranet** sits somewhere between the Internet and an intranet. It allows limited and controlled access to internal network resources by outside users. It's used when two organizations need to share resources, so controls are put in place to allow this sharing without making resources available to the wider Internet.

Packets and Frames

When computers transfer information across a network, they do so in short bursts of about 1500 bytes of data. Each burst, or chunk, of data has the same basic structure; specifically, each chunk of data contains the MAC addresses and IP addresses of both the sending (source) and receiving (destination) computers. So, to transfer a small word-processing file, only one burst of data transfer might be needed, but large photo or music files are first divided into several hundred or even thousands of chunks before they're transferred. After each chunk of data is sent, the computer pauses momentarily. Data is transferred in this way for a number of reasons:

- The pause between bursts might be necessary to allow other computers to transfer data during pauses.

- The pause allows the receiving computer to process received data, such as writing it to disk.
- The pause allows the receiving computer to receive data from other computers at the same time.
- The pause gives the sending computer an opportunity to receive data from other computers and perform other processing tasks.
- If an error occurs during transmission of a large file, only the chunks of data involved in the error have to be sent again, not the entire file.

To use another analogy, you can look at chunks of data as sentences people use when speaking. Pauses in conversation give listeners an opportunity to register what has been said and possibly get a word in themselves.

Tip

To get an idea of how many chunks of data are involved in transferring a typical file, a 3-minute music file is about 3 million bytes (3 MB) of data, which takes about 2000 chunks of data.

Packets

The chunks of data sent across the network are usually called "packets" or "frames." **Packet**, the more well-known term, is often used generically to mean a chunk of data sent over the network. However, this term does have a particular meaning: It's a chunk of data with source and destination IP addresses (as well as other IP protocol information) added to it. Figure 1-20 shows a representation of the original data to be transferred, and Figure 1-21 shows the packets created after the data has been broken into chunks and IP addresses added.

Using the U.S. mail analogy, you can look at a packet as an envelope with the zip code added but not the street address. In relation to the layers of the network communication process, packets are generated by and processed by the network protocol. You learn more details about this process in Chapters 5 and 6.

Frames

A **frame** is a packet with the source and destination MAC addresses added to it. In addition, frames have an error-checking code added to the back end of the packet, so the packet is "framed" by MAC addresses (and other network interface information) on one end and an error-checking code on the other. A frame is like a letter that's been addressed and stamped and is ready to deliver.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.

Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.

Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.

Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.

Figure 1-20 Original data

Dest: IP: 172.16.1.2, Source IP: 172.16.1.1	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies.
Dest: IP: 172.16.1.2, Source IP: 172.16.1.1	purus lectus malesuada libero, sit amet commodo magna eros quis urna. Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.
Dest: IP: 172.16.1.2, Source IP: 172.16.1.1	Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci
Dest: IP: 172.16.1.2, Source IP: 172.16.1.1	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies
Dest: IP: 172.16.1.2, Source IP: 172.16.1.1	Pellentesque habitant tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.

Figure 1-21 Data divided into several packets

Frames are essentially the final state of data before it's placed on the network medium as bits. The network interface is the layer of the network communication process that works with frames. Figure 1-22 shows what the packets from Figure 1-21 look like after the frame information is added.

The process of adding IP addresses and then MAC addresses to chunks of data is called **encapsulation**. Information added at the front of data is called a **header**, and information added at the end of data is called a **trailer**. Data is encapsulated several times as it works its way down from the sending application until it reaches the network interface as a frame. When the destination computer receives the frame, the

Dest MAC, Source MAC	Dest IP, Source IP	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies,	Error check
Dest MAC, Source MAC	Dest IP, Source IP	purus lectus malesuada libero, sit amet commodo magna eros quis urna. Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.	Error check
Dest MAC, Source MAC	Dest IP, Source IP	Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci	Error check
Dest MAC, Source MAC	Dest IP, Source IP	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies	Error check
Dest MAC, Source MAC	Dest IP, Source IP	Pellentesque habitant tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.	Error check

Figure 1-22 The packets are now frames and ready for delivery

process is reversed as the network interface deencapsulates the frame (has the header and trailer removed) so that it becomes a packet again. This process continues until the packet arrives at the receiving application or service as the original data. This process is all part of the layered approach to networking.

Clients and Servers

You've already learned about the role of client network software and server network software. Unfortunately, the world of networking sometimes uses the same terms to discuss two different things. The following sections clarify what "client" and "server" mean and how their meanings can differ depending on how they're used.

Client

A **client**, in networking terms, can be a workstation running a client OS, such as Windows 10, or the network software on a computer that requests network resources from a server. In addition, you can refer to a physical computer as a client computer. What the term "client" means, therefore, depends on the context in which it's used. To clarify, it's typically used in these three contexts:

- *Client operating system*—The OS installed on a computer is designed mainly to access network resources, even though it might be capable of sharing its own resources. Windows 10 and Mac OS X fit this description, for example, as do certain distributions of Linux. A client OS is also often referred to as a "desktop OS."
- *Client computer*—This computer's primary role in a network is to run user applications and access network resources. Most computers in a network fit this description.

- *Client software*—This is the software that requests network resources from server software running on another computer. For example, a Web browser, an e-mail client (such as the Gmail app), and Client for Microsoft Networks fit into this category.

Server

When most people hear the word "server," they conjure up visions of a large tower computer with lots of hard drives and memory. This image is merely a computer hardware configuration that may or may not be used as a server, however. In short, a computer becomes a **server** when software is installed on it that provides a network service to client computers. In other words, you can install certain software on an inexpensive laptop computer and make it act as a server. By the same token, a huge tower computer with six hard drives and 256 GB of RAM can be used as a workstation for a single user. So, although some hardware configurations are packaged to function as a server, and others are packaged as client or desktop computers, what makes a computer a server is the software installed on it. Just as there are three contexts in which the term "client" is used, so it is with the term "server":

- *Server operating system*—This term is used when the OS installed on a computer is designed mainly to share network resources and provide other network services. A server OS is tuned to be able to share files efficiently and perform network operations in response to client requests, even though the OS might also be able to run user applications and client software. Windows Server, Mac OS X Server, UNIX, and many Linux distributions fit this description.
- *Server computer*—This term is used when a computer's primary role in the network is to give client computers access to network resources and services. The computers that most often fit this description are usually in the IT room or locked away in a closet.
- *Server software*—This is the software that responds to requests for network resources from client software running on another computer. A Web server (such as Internet Information Services), an e-mail server (such as Microsoft Exchange), and File and Printer Sharing for Microsoft Networks fit into this category.

Note

Microsoft refers to server software components as "services." Other OSs use other terms; for example, in Linux/UNIX, server software components are referred to as "daemons."

As you can see, the lines between a client computer and a server computer are often blurred because OSs are designed as network operating systems, and most computers can take on the roles of both server and client. As you're learning, however, the language of networking is often imprecise, and you must pay attention to the

context in which networking terms are used to grasp their meaning. As you get more comfortable with all the terms and better understand how networks work, the nuances of the terminology will fall into place.

Network Models

A **network model** defines how and where resources are shared and how access to these resources is regulated. Network models fall into two major types: peer-to-peer and server-based (also called client/server). This discussion of network models addresses the role that computers play on the network and how these roles interact. Server-based networks are the most common in business settings, but understanding both types is essential, especially as they compare with each other.

Note

Peer-to-peer networks running Windows OSs are referred to as "workgroup networks," and server-based networks running Windows Server are called "domain-based networks."

In a **peer-to-peer network**, most computers function as clients or servers, as circumstances dictate. For example, a computer can act as a server by sharing a printer it's connected to and simultaneously act as a client by accessing a file shared by another computer on the network. In this type of network, there's no centralized control over who has access to network resources; each user maintains control over his or her own shared resources. The computers in peer-to-peer networks usually run desktop or client OSs.

In a **server-based network**, certain computers take on specialized roles and function mainly as servers, and ordinary users' machines tend to function mainly as clients. Windows Server, Red Hat Enterprise Linux, and UNIX are OSs designed primarily for server use. In these networks, servers have centralized authority over who has access to network resources.

Peer-to-Peer/Workgroup Model

As you have learned, computers on a peer-to-peer network can take both client and server roles. Because all computers on this type of network are peers, these networks impose no centralized control or security over shared resources. Any user can share resources on his or her computer with any other user's computer, and each user can determine what level of access other users have to his or her shared resources. Physically, a peer-to-peer network looks just like a server-based network; mainly, location and control over resources differentiate the two.

In a peer-to-peer network, every user must act as the administrator of his or her computer's resources. Users can give everyone else unlimited access to their resources or grant restricted (or no) access to other users on the network. To grant access, users must create user accounts and passwords for each user who will access shared resources on their computers. The username and password for accessing a computer are called **credentials**. If you have five computers in a peer-to-peer network, each user might have to remember as many as five different sets of credentials. Because of the lack of centralized authority over resources, controlled chaos is the norm for all but the smallest peer-to-peer networks, and security can be a major concern because not all users might be educated in creating secure passwords.

On a Windows-based peer-to-peer network, computers are members of a workgroup, but a workgroup is simply an identifier and doesn't constitute a network security boundary. In other words, users on computers in Workgroup A can access resources on computers in Workgroup B as long as they have the correct credentials.

Although this system can work on small networks, things can become unworkable as the number of users and computers grows—not because the network doesn't operate correctly, but because users can't cope with having to remember multiple sets of credentials to access resources spread out over several computers. This limitation is in contrast to a server-based network, in which security of all resources is administered centrally.

Most peer-to-peer networks consist of collections of desktop PCs linked by a common network medium and connectivity device, such as a switch. The machines and the OS installed on them aren't tuned to provide network services as efficiently as dedicated network servers configured with server OSs. They can bog down easily under increasing loads, as more users try to access resources from a particular machine. The user whose machine is being accessed across the network has to endure a performance reduction while his or her machine is busy handling network information requests. For example, if a user's machine has a network-accessible printer attached, the machine slows down every time someone sends a job to that printer. In addition, if a user restarts the machine while someone is accessing a resource on it, the network user's access fails or, even worse, data loss can occur.

Another issue that affects peer-to-peer networks is data organization. If every machine can be a server, how can users keep track of what information is stored on which machine? If five users are responsible for a collection of documents, any of those users might have to search through files on all five machines to find a document. The decentralized nature of peer-to-peer networks makes locating resources more difficult as the number of peers increases. Likewise, decentralization makes backup much trickier: Instead of backing up a single server that holds the shared documents, each machine must be backed up to protect shared data.

Given these issues and complexities, peer-to-peer networks might not seem worth using. However, they offer some advantages, particularly for small organizations. Peer-to-peer networks are the easiest and most inexpensive to install. Most require only

a client OS on desktop computers, along with cabling and connectivity devices. After computers are connected and configured correctly, users can begin sharing information immediately. Desktop computers and client OSs cost considerably less than their server counterparts.

Peer-to-peer networks are also well suited to small organizations, which tend to have small networks and small operating budgets. They're easy to use and don't require extensive staff training or a dedicated network administrator. With no centralized control, the loss of a machine means only the loss of access to the resources on it; otherwise, a peer-to-peer network continues to function when one computer fails. However, because managing resources and their security is difficult on a peer-to-peer network, even small networks of a few computers sometimes opt to use the server or domain network model.

Server/Domain-Based Model

Server-based networks allow centralized control over network resources, mainly by providing an environment in which users log on to the network with a single set of credentials maintained by one or more servers running a server OS. Server OSs are designed to handle many simultaneous user logons and requests for shared resources efficiently. In most cases, servers are dedicated to running network services and shouldn't be used to run user applications. You want to reserve servers' CPU power, memory, and network performance for user access to network services.

When you're using Windows Server OSs in a server-based network with centralized logons, you're running a Windows domain. A **domain** is a collection of users and computers whose accounts are managed by Windows servers called **domain controllers**. Users and computers in a domain are subject to network access and security policies defined by a network administrator and enforced by domain controllers. The software managing centralized access and security is a **directory service**. On Windows servers, the directory service software is **Active Directory**, and it's what makes a Windows server a domain controller.

The Linux OS supports a centralized logon service called Network Information Service (NIS), but more often Linux administrators use a service compatible with Active Directory, called Lightweight Directory Access Protocol (LDAP), if they want to use a directory service. A directory service is one of several network services usually found only on server OSs running in a server-based network. Others include the following:

- *Naming services*—Translate computer names to their addresses.
- *E-mail services*—Manage incoming and outgoing e-mail from client e-mail programs.
- *Application services*—Grant client computers access to complex applications that run on the server.
- *Communication services*—Give remote users access to an organization's network.
- *Web services*—Provide comprehensive Web-based application services.

Unlike peer-to-peer networks, server-based networks are easier to expand. Peer-to-peer networks should be limited to 10 or fewer users, but server-based networks can handle anywhere from a handful to thousands of users. In addition, multiple servers can be configured to work together, which enables administrators to add more servers to share the load when an application's performance wanes or to provide fault tolerance if a server's hardware malfunctions.

Like peer-to-peer networks, server-based networks have some disadvantages. The most obvious is the additional overhead of operating a server-based network. Server-based networks require one or more dedicated computers to run the server OS. Computers sold as servers usually have features that improve reliability and performance and cost more than desktop computers. In addition, these networks usually require at least part-time support from a person skilled in managing server OSs. Acquiring the skills to manage a server-based network or hiring a trained network administrator adds quite a bit to operating costs.

Housing all your network resources and services on a single server makes administration of resources easier in the long run, but it also creates a single point of failure. Fortunately, most server OSs now have redundancy features that allow taking a single server offline while other machines assume that server's duties. Naturally, having redundant hardware is costly. You must carefully weigh the costs of lost productivity if a server fails against the additional hardware and software costs of redundancy features.

Table 1-6 summarizes the strengths and weaknesses of peer-to-peer and server-based networks.

Table 1-6 Peer-to-peer versus server-based networks

Network attribute	Peer-to-peer network	Server-based network
Resource access	Distributed among many desktop/client computers; makes access to resources more complex	Centralized on one or more servers; streamlines access to resources
Security	Users control their own shared resources and might have several sets of credentials to access resources; not ideal when tight security is essential	Security is managed centrally, and users have a single set of credentials for all shared resources; best when a secure environment is necessary
Performance	Desktop OS not tuned for resource sharing; access to shared resources can be hindered by users running applications	Server OS tuned for resource sharing; servers are usually dedicated to providing network services
Cost	No dedicated hardware or server OS required, making initial costs lower; lost productivity caused by increasing complexity can raise costs in the long run	Higher upfront costs because of dedicated hardware and server OSs; additional ongoing costs for administrative support

Both peer-to-peer networks and server-based networks have advantages. For this reason, using a combination of the two models isn't uncommon. For example, a user might want to share a printer with a group of users in close proximity or a document folder with a department colleague. With this arrangement, a user is in control of a shared resource yet can still assign permissions to this resource by using accounts from the central user database on the server. Although sharing the resource is decentralized, the logon credentials to access the resource are still centralized.

Hands-On Project 1-5: Exploring Peer-to-Peer Networking

Time Required: 15 minutes
Objective: View other computers and shared resources on a peer-to-peer network.
Required Tools and Equipment: Net-*XX*
Description: In this project, you view other computers and shared resources in a peer-to-peer network. Your instructor should have a computer named Net-Instr available on the network with a share named NetDocs. You also view and, if necessary, change the type of network (public or private) to which you're connected.

Note

All students should use the same username and password.

1. Start your computer, and log on as **NetAdmin**, if necessary.
2. In the search bar next to Start, type **system** and click the search result that shows System with Control panel underneath it, as in Figure 1-23. In the "Computer name, domain, and workgroup settings" section, examine the current settings. Does your computer belong to a workgroup or a domain? Is this computer operating in a peer-to-peer or server-based environment? Write your answers on the following lines:

   _____

   _____

3. Your computer name should be NET-*XX* (with *XX* representing your student number) and your workgroup should be NETESS. Verify with your instructor whether they're the right settings for your environment. If the computer name is already set with your student number and the workgroup name NETESS, skip to the next step. Otherwise, click **Change settings**. In the System Properties dialog box, click **Change**. Type **NET-*XX*** in the "Computer name" text box (replacing *XX* with your student number), type **NETESS** in the Workgroup text box, and click **OK**. Click **OK** in the message box welcoming you to the NETESS workgroup, and then click **OK** in the message box stating that you must restart your computer. Click **Close**, and then click **Restart Now** to restart your computer. When the computer restarts, log on.

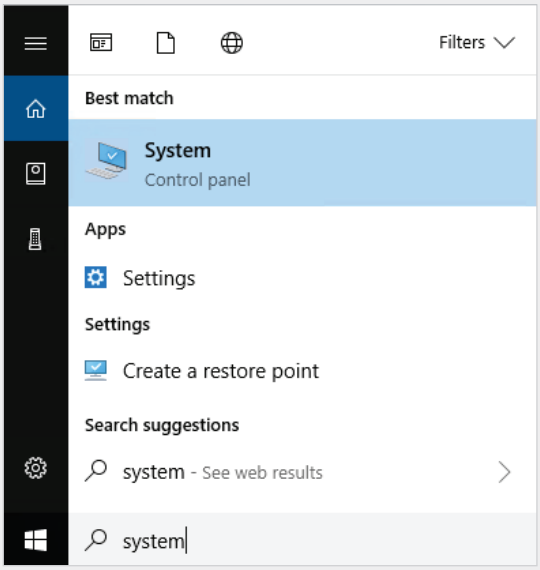

Figure 1-23 Opening the System control panel

4. To see other computers on the network and share files, you need to verify that certain network settings are correct. Open the Network and Sharing Center by clicking the computer icon on the right side of the taskbar and clicking **Network and Internet settings** (or just **Network settings** depending on your version of Windows 10). Next, click **Network and Sharing Center**.
5. Click **Change advanced sharing settings** to open the Advanced sharing settings dialog box (see Figure 1-24).
6. Under Network discovery, click the **Turn on network discovery** option button, if necessary. Under File and printer sharing, click the **Turn on file and printer sharing** option button, if necessary. If you had to make any changes, click the **Save changes** button; otherwise, click **Cancel**. Close all open windows.
7. In the Search box, type **cmd** and press **Enter** to open a command prompt.
8. At the command prompt, type **`net view`** and press **Enter**. You should see a list of computers in your workgroup, similar to Figure 1-25.
9. To view shared resources on a computer, you use the `net view computername` command. For example, to see whether there are any shared folders or printers on the instructor's computer, type **`net view net-instr`** and press **Enter**. You should see a screen similar to Figure 1-26, in which the share name is listed as NetDocs and the type is listed as Disk.
10. Close the command prompt window, but leave your computer running for the next project.

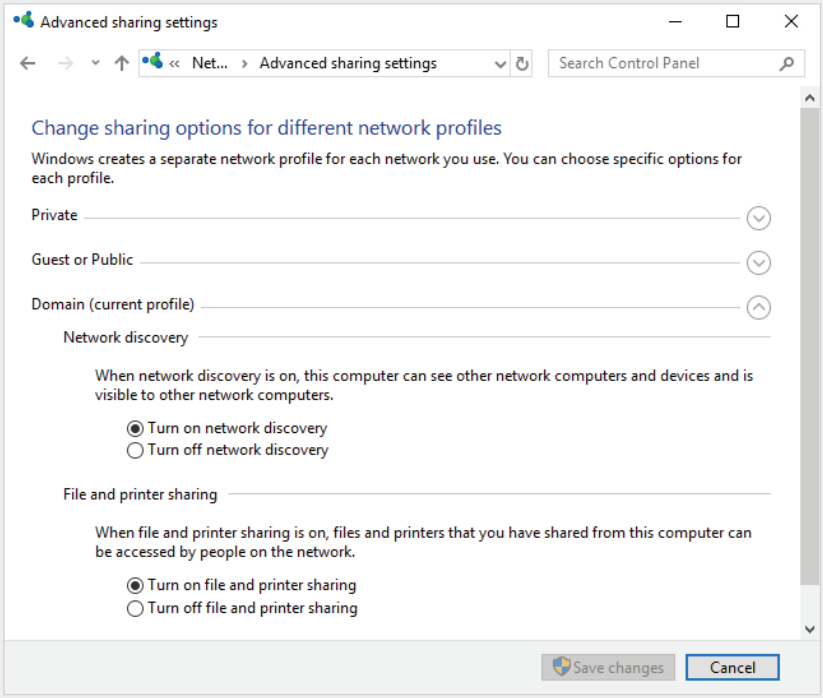

Figure 1-24 The Advanced sharing settings dialog box

```
C:\Users\NetAdmin>net view
Server Name            Remark

-------------------------------------------------------------------------------
\\NET-01
\\NET-INSTR
The command completed successfully.

C:\Users\NetAdmin>
```

Figure 1-25 Using the `net view` command to list computers in a workgroup

```
C:\Users\NetAdmin>net view net-instr
Shared resources at net-instr


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
NetDocs     Disk
The command completed successfully.

C:\Users\NetAdmin>
```

Figure 1-26 Viewing shared resources with the `net view` command

Hands-On Project 1-6: Creating a Shared Folder

Time Required: 15 minutes
Objective: Create a folder on your computer and share it with the rest of the network.
Required Tools and Equipment: Net-*XX*
Description: In this project, you create a folder and then share it so that other users can add files to the folder via the network. Your instructor might assign you a partner.

1. Start your computer, and log on as **NetAdmin**, if necessary.
2. Right-click **Start** and click **File Explorer**. Double-click the **D** drive (or another drive specified by your instructor). Right-click in the right pane, point to **New**, and click **Folder**. Type **MyData**, and press **Enter** to name the folder.
3. Right-click **MyData** and click **Properties**. In the Properties dialog box, click the **Sharing** tab.
4. Click **Share**. In the File Sharing dialog box, click the list arrow and click **Everyone**. Click **Add**. Notice that the default permission level is Read. Click the **Read** list arrow, and then click the **Read/Write** permission level. Notice that the account you used to create the share has the permission level Owner, which grants the user full access to the share, including the ability to change its permissions.
5. Click **Share** to finish sharing the folder. In the confirmation dialog box shown in Figure 1-27, notice the notation under the share name: \\NET-*XX*\MyData. This is the network path to the share that users on other computers can use to access the shared folder. This notation is the Universal Naming Convention (UNC) path, which you learn more about in Chapter 9. Click **Done**, and then click **Close**.

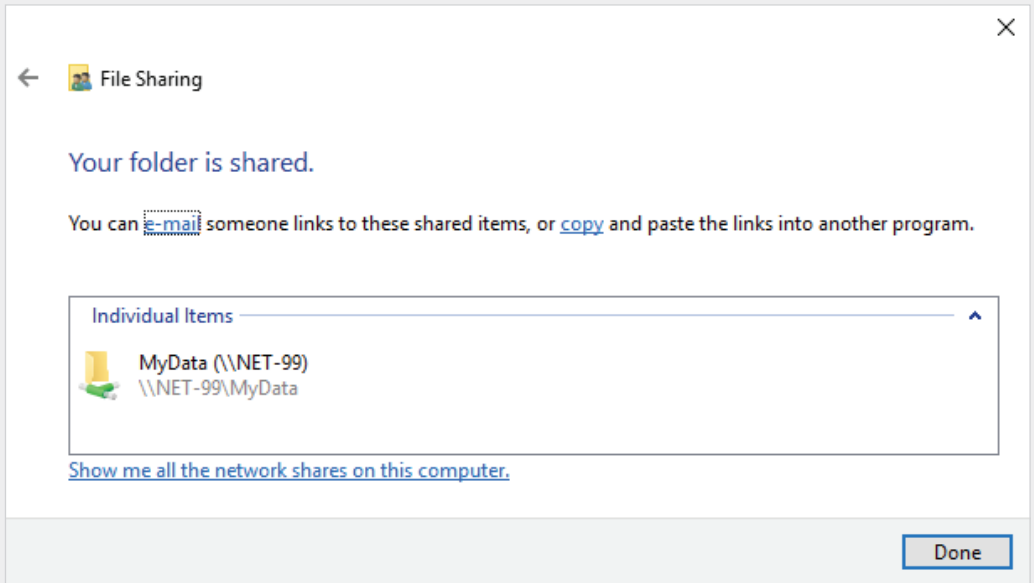

Figure 1-27 The confirmation dialog box displayed after creating a share

6. Try opening another student's shared folder by right-clicking **Start**, clicking **Run**, typing **NET-*XX*\MyData** (substituting your partner's student number for *XX*), and pressing **Enter**. A File Explorer window should open. To create a new file, right-click the File Explorer window, point to **New**, and click **Text Document**. Type your initials and press **Enter** to name the file.
7. To verify that your partner created a folder in your MyData share, open File Explorer, and then double-click the **D** drive and the **MyData** folder. If your partner finished Step 6, a new file should be there.
8. Close all open windows. You just performed some basic tasks associated with maintaining a network: creating shared folders and assigning permissions. You assigned Read/Write permissions to the Everyone group, which is a special group in Windows. All user accounts created on your computer belong to the Everyone group automatically, and you can't change this setting. You were able to access your partner's shared folder because you were both logged on to your computers with the same username and password, so you had the correct credentials.
9. Write down which network model you think was used in this activity:

_____

10. Close all open windows, but leave your computer running for the next project.

Hands-On Project 1-7: Transferring a Document to Another Computer

Time Required: 15 minutes
Objective: Create a document and copy it to your instructor's computer.
Required Tools and Equipment: Net-*XX*
Description: This project requires some setup by your instructor, so verify that the setup has been finished before continuing. In this project, you write a memo to your instructor containing the information specified in the following steps. Then you copy the file you created to a file share on your instructor's computer (or some other computer your instructor designates).

1. Start your computer, and log on as **NetAdmin**, if necessary.
2. Start Microsoft Word or another word-processing program; even a simple text editor, such as Notepad, will do. Write a letter to your instructor that includes the following:
   - The reason you're taking this class
   - What you hope to get out of this class
   - How much time you expect to put into this class each week outside classroom hours
   - Whether you expect to take more computer and networking classes

_____

_____

_____

_____

3. Save the document in your **Documents** folder (or a folder your instructor designates), naming it ***yourname***. For example, if your name is Bill Smith, name the document **billsmith**.
4. Start File Explorer and navigate to the folder where you saved the letter. Right-click the document you created and click **Copy**.
5. To paste the document to the instructor's shared folder, use the UNC path of your instructor's computer, which should be \\Net-Instr\NetDocs, unless your instructor specifies otherwise. In the search box, type **Net-Instr****NetDocs**, and press **Enter**.
6. Click **OK**. You should see a File Explorer window open. (The folder might contain documents if some of your classmates have already completed the activity.) Right-click a blank space in the right pane and click **Paste**. Your document should now be available on your instructor's computer.
7. Close all open windows, but leave your computer running for the next project.

Hands-On Project 1-8: Looking Up Computer and Networking Acronyms

Time Required: 20 minutes
Objective: Do online research to learn the meaning of common computer and networking acronyms.
Required Tools and Equipment: Any computer with Internet access
Description: This project requires access to the Internet. Half the battle of learning any new field or technology is learning the language used by professionals in the field. Computer and networking technologies are well known for their heavy use of acronyms. In this project, you use the Acronym Finder Web site to look up acronyms.

1. Start your Web browser and go to **www.acronymfinder.com**.
2. You can look up acronyms by typing them in the "Abbreviation to define" text box at the top and clicking the **Find** button. If there's more than one common definition for an acronym, Acronym Finder lists them by popularity ranking. Look up the following acronyms; you'll need some of them later:
   - TCP/IP
   - Wi-Fi
   - SSID
   - WEP
   - OSI
   - Ping
   - UTP

- Cat6
- EMI
- RJ-45

3. Bookmark *Acronymfinder.com* for future use and exit your browser. Shut down your computer, unless you're continuing to the case projects.

Chapter Summary

- All computers perform three basic tasks: input, processing, and output. Some components of computers are designed to perform only one of these three functions; others are designed to perform two or all three functions.
- Storage is a major part of a computer's configuration. Storage types include short-term storage (RAM) and long-term storage (disk drives and USB or flash drives). Data is stored as bits. A collection of 8 bits is a byte. When expressing an amount of computer data, you can use bits or bytes. Bits are expressed as a lowercase b while bytes are expressed as an uppercase B.
- PC hardware consists of four major components: a motherboard, a hard drive, RAM, and firmware. The motherboard is the nerve center of the computer and contains the CPU, expansion slots, and RAM slots.
- The components needed to make a standalone computer a networked computer include a NIC, a network medium, and usually an interconnecting device. In addition, network software consisting of client and server software, protocols, and the NIC driver are needed to enable a computer to communicate on a network.
- The layers of the network communication process can be summarized as user application, network software, network protocol, and network interface.
- The terms for describing networks of different scopes are LAN, internetwork, WAN, and MAN. A LAN is a single collection of devices operating in a small geographic area. An internetwork is a collection of LANs tied together by routers, and a WAN and MAN are geographically dispersed internetworks.
- Packets and frames are the units of data handled by different network components. Packets, which are processed by the network protocol, are units of data with the source and destination IP addresses added. Frames, which are processed by the network interface, have MAC addresses and an error-checking code added to the packet.

- A client is the computer or network software that requests network data, and a server is the computer or network software that makes network data available to requesting clients.
- A peer-to-peer network model has no centralized authority over resources; a server-based network usually uses a directory service for centralized logon, security settings, and resource management.

Key Terms

Active Directory
basic input/output system (BIOS)
binary digit
bit
bus
byte
chipset
client
complementary metal oxide semiconductor (CMOS) memory
core
credentials
directory service
domain
domain controller
encapsulation
extranet
firmware
frame
header
Internet
Internet of Things (IoT)
internetwork
intranet
local area network (LAN)
metropolitan area network (MAN)
multicore CPU
name server
network
network client software
network model
network protocols
network server software
nonvolatile memory
packet
peer-to-peer network
server
server-based network
stand-alone computer
trailer
Unified Extensible Firmware Interface (UEFI)
volatile memory
wide area networks (WANs)

Review Questions

1. Which of the following is one of the three basic functions a computer performs? (Choose three.)
   a. Processing
   b. Internet access
   c. Input
   d. Graphics
   e. Output
   f. E-mail
2. Which computer component executes instructions provided by computer programs?
   a. CPU
   b. NIC
   c. Hard drive
   d. USB
3. What do you call each of the processors inside a CPU?
   a. I/O
   b. Core
   c. OS
   d. Flash
4. Which of the following is considered long-term storage? (Choose two.)
   a. USB or flash drive
   b. RAM
   c. Working storage
   d. Hard drive

5. Which motherboard component controls data transfers between memory, expansion slots, I/O devices, and the CPU?
   a. RAM slots
   b. IDE connectors
   c. Chipset
   d. PCI Express
6. You want to purchase a high-performance graphics card for your computer. Which type of connector should it have?
   a. PCI
   b. SATA
   c. IDE
   d. PCI Express
7. What is the term for the time it takes for read/write heads to move to the correct spot on the hard disk platter?
   a. Rotational delay
   b. Seek time
   c. Transfer time
   d. Access time
8. Which of the following is a task usually performed by the firmware? (Choose two.)
   a. Perform a POST.
   b. Create an interrupt.
   c. Store the operating system.
   d. Begin the boot procedure.
9. Which of the following is the correct order of the steps of the boot procedure?
   1. The OS is loaded into RAM.
   2. CPU starts.
   3. OS services are started.
   4. Power is applied.
   5. The POST is executed.
   6. Boot devices are searched.

   a. 2, 4, 6, 1, 3, 5
   b. 1, 5, 2, 4, 3, 6
   c. 4, 2, 5, 6, 1, 3
   d. 5, 4, 1, 3, 2, 6
10. You have just installed a new NIC in your PC to replace the old one that had started malfunctioning. What additional software must be installed to allow the OS to communicate with the new NIC?
    a. Network application
    b. Device driver
    c. BIOS
    d. Protocol
11. Which of the following requests information stored on another computer?
    a. NIC
    b. Network client
    c. Network server
    d. Network protocol
    e. Device driver
12. Choose the correct order for the process of a user attempting to access network resources:
    1. Network protocol
    2. Application
    3. Network client
    4. NIC driver

    a. 4, 2, 1, 3
    b. 3, 2, 1, 4
    c. 1, 4, 2, 3
    d. 2, 3, 1, 4
    e. 3, 1, 2, 4
13. TCP/IP is an example of which of the following?
    a. NIC
    b. Network client
    c. Network server
    d. Network protocol
    e. Device driver

14. In network communication, what type of address is used to deliver a frame to the correct computer on the network? (Choose two.)
    a. MAC
    b. Logical
    c. IP
    d. Physical
15. What type of message is used to determine whether a computer is listening on the network?
    a. MAC
    b. Ping
    c. IP
    d. TCP
16. What does TCP/IP use to look up a computer's IP address, given its name?
    a. DNS
    b. Ping
    c. MAC
    d. TCP
17. What is the unit of information containing MAC addresses and an error-checking code that's processed by the network interface layer?
    a. Packet
    b. Ping
    c. Frame
    d. Chunk
18. Data is processed from the time an application creates it to the time it reaches the network medium. This process includes adding information such as addresses and is called which of the following?
    a. Packetization
    b. Encapsulation
    c. Deencapsulation
    d. Layering
19. You're the network administrator for a company that has just expanded from one floor to two floors of a large building, and the number of workstations you need has doubled from 50 to 100. You're concerned that network performance will suffer if you add computers to the existing LAN. In addition, new users will be working in a separate business unit, and there are reasons to logically separate the two groups of computers. What type of network should you configure?
    a. WAN
    b. MAN
    c. Internetwork
    d. Extended LAN
20. Which of the following best describes a client?
    a. A computer's primary role in the network is to give other computers access to network resources and services.
    b. A computer's primary role in the network is to run user applications and access network resources.
    c. It's the software that responds to requests for network resources.
    d. The OS installed on a computer is designed mainly to share network resources.
21. You work for a small company with four users who need to share information on their computers. The budget is tight, so the network must be as inexpensive as possible. What type of network should you install?
    a. Server-based network
    b. Peer-to-peer network
    c. Wide area network
    d. Storage area network

22. Which of the following characteristics is associated with a peer-to-peer network? (Choose three.)
    a. Decentralized data storage
    b. Inexpensive
    c. User-managed resources
    d. Centralized control
    e. Uses a directory service
23. A device interconnects five computers and a printer in a single office so that users can share the printer. This configuration is an example of which of the following?
    a. LAN
    b. MAN
    c. WAN
    d. Internetwork
24. A company has just made an agreement with another organization to share their two networks' resources by using TCP/IP protocols. What best describes this arrangement?
    a. MAN
    b. LAN
    c. Intranet
    d. Extranet
25. You have installed Windows Server on a new server and want to centralize user logons and security policies. What type of software should you install and configure on this server?
    a. Naming services
    b. Application services
    c. Communication services
    d. Directory services
26. A network interface can transfer data at 1 Gbps. Approximately how many bytes can the interface transfer per second?
    a. 1 billion
    b. 125 million
    c. 100,000
    d. 8 billion

Packet Tracer Labs

Packet Tracer Lab 1-1: Installing the Packet Tracer Network Simulator

Time Required: 30 minutes

Objective: Install Packet Tracer.

Required Tools and Equipment: A computer with Internet access

Description: In this project, you create an account on the Cisco Netacad Web site and then download and install Packet Tracer, a network simulator. If you already have an account on the Netacad Web site, simply sign in with your credentials and then download and install Packet Tracer.

1. Open a browser window and go to ***www.netacad.com***. Click **Packet Tracer** (see Figure 1-28).
2. Click **Enroll to download Packet Tracer** (see Figure 1-29). You will be enrolling in a free, self-paced tutorial about Packet Tracer. Enrolling allows you to use the Packet Tracer software for free.

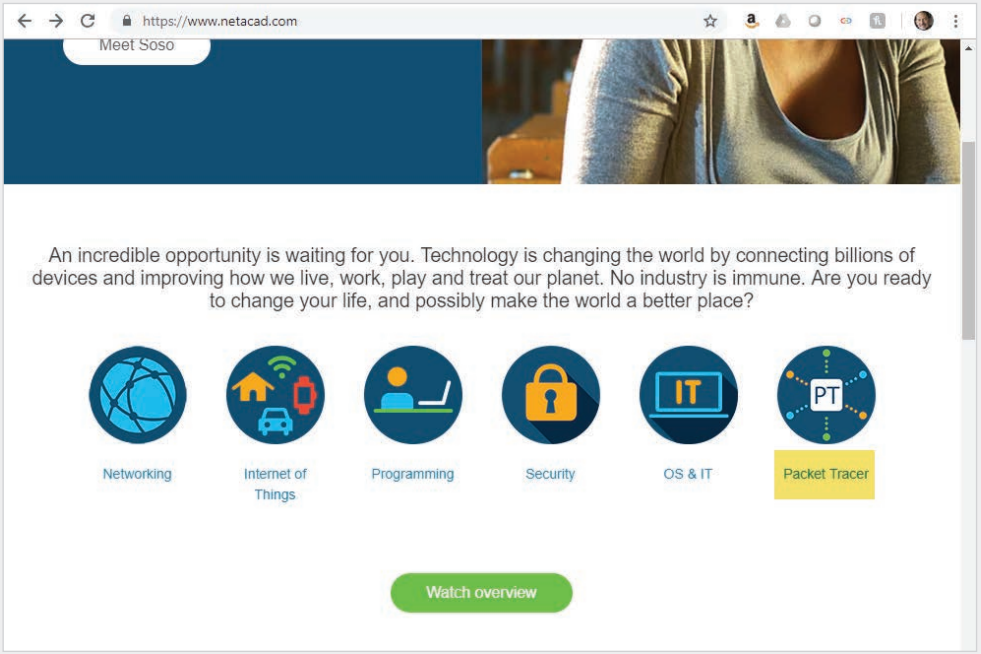

Figure 1-28 The first screen for downloading Packet Tracer

Source: Cisco Systems, Inc.

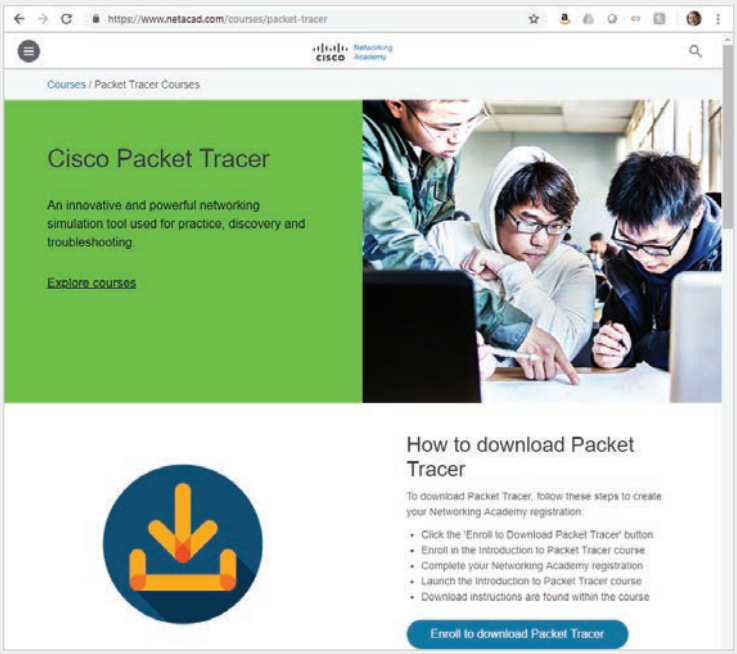

Figure 1-29 The second screen for downloading Packet Tracer

Source: Cisco Systems, Inc.

3. Click **Sign up today!** (see Figure 1-30). As you can see, the course is self-paced and free. Once Packet Tracer is installed, you should go through the course to get a good idea of how to use Packet Tracer. It will be used in the Packet Tracer Labs throughout this book.
4. Follow the instructions to create an account. When you are finished, you will be able to return to *www.netacad.com*, log in, click **Resources** at the top of the screen, and then click **Download Packet Tracer**. Follow the instructions to download and install Packet Tracer.

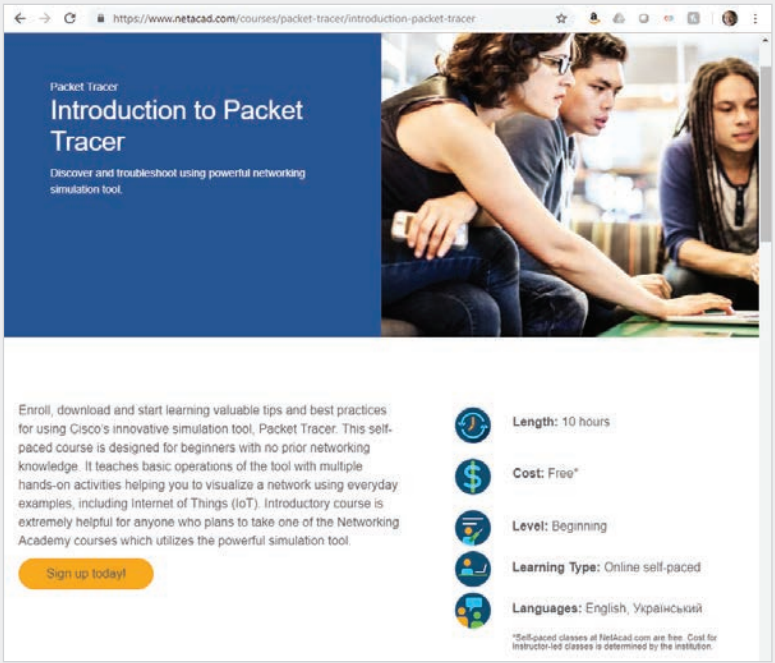

Figure 1-30 The third screen for downloading Packet Tracer
Source: Cisco Systems, Inc.

Packet Tracer Lab 1-2: Introduction to Packet Tracer

Time Required: 15 minutes

Objective: Use Packet Tracer to build a small network.

Required Tools and Equipment: A computer with Packet Tracer installed per the instructions in Packet Tracer Lab 1-1

Description: In this project, you run Packet Tracer and explore the user interface. As of this writing, the most current version is 7.2.1. Your version may be different and look somewhat different.

1. Open Packet Tracer. You may be asked to sign in to Netacad with the credentials you created in Packet Tracer Lab 1-1.
2. In the Packet Tracer window, turn your attention to the lower-left part of the screen, where you see a palette of device types from which to choose (see Figure 1-31). Hover your mouse over the top row of device types to see your choices. For each device type you select on the top row, you'll see the device choices change on the bottom row and in the middle pane. Click **Network Devices**.

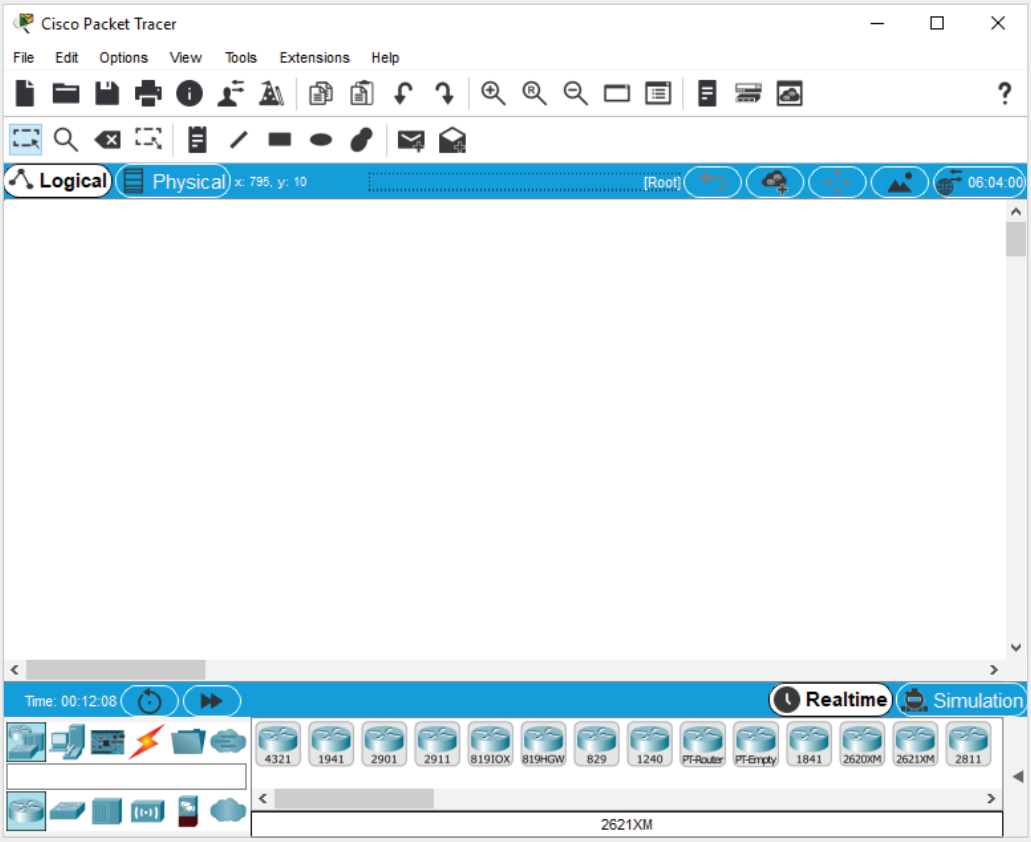

Figure 1-31 The main Packet Tracer window

Source: Cisco Systems, Inc.

3. Hover your mouse over each device in the bottom row and click **Switches**. In the middle pane, you see a selection of switches. Click and drag the second switch from the left, which is labeled **PT-Switch**. Drag and drop the switch into the main Packet Tracer window.
4. Next, on the top row of device types, click **End Devices**. In the middle pane, click and drag **PC** into the main screen. Repeat this action until there are two PCs and one switch (see Figure 1-32).

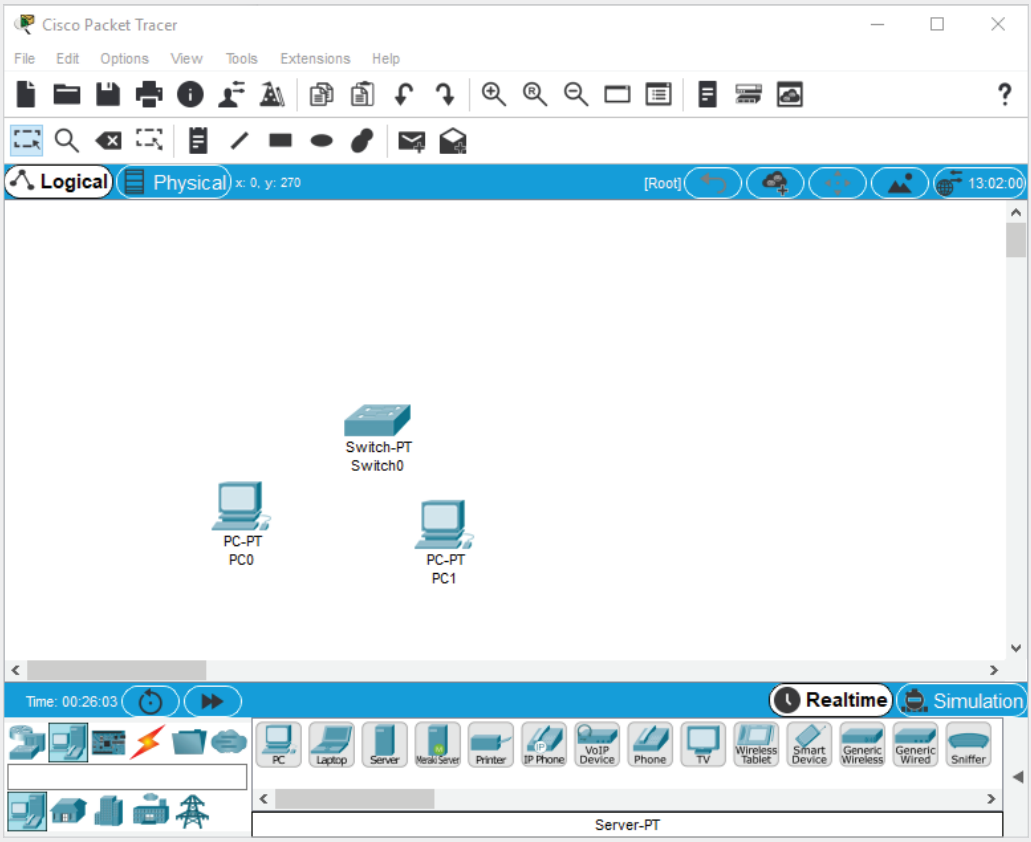

Figure 1-32 Two PCs and one switch in Packet Tracer

Source: Cisco Systems, Inc.

5. Next, you'll connect the PCs to the switch. Click the **Connections** icon on the top row of device types. In the middle pane, click the **Copper Straight-Through** cable, which looks like a solid black line.
6. Click **PC0** and then click **FastEthernet0** to plug the cable into PC0's Ethernet port. Click **Switch0** and click **FastEthernet0/1** to plug the other end of the cable into the switch. Repeat the process for PC1, but choose **FastEthernet1/1** on the switch this time. Your Packet Tracer diagram should look like Figure 1-33. Congratulations, you have built your first LAN with Packet Tracer!
7. Before this LAN can be useful, you must assign an IP address to each PC. Hover your mouse over each PC and you'll see that the IP address column of the pop-up window reads "<not set>." Click **PC0** to open the PC0 configuration dialog box. Click the **Desktop** tab (see Figure 1-34).
8. Click **IP Configuration** and fill in or confirm the following values:
   - IP Address: **172.20.1.1**
   - Subnet Mask: **255.255.0.0** (this value is filled in automatically)

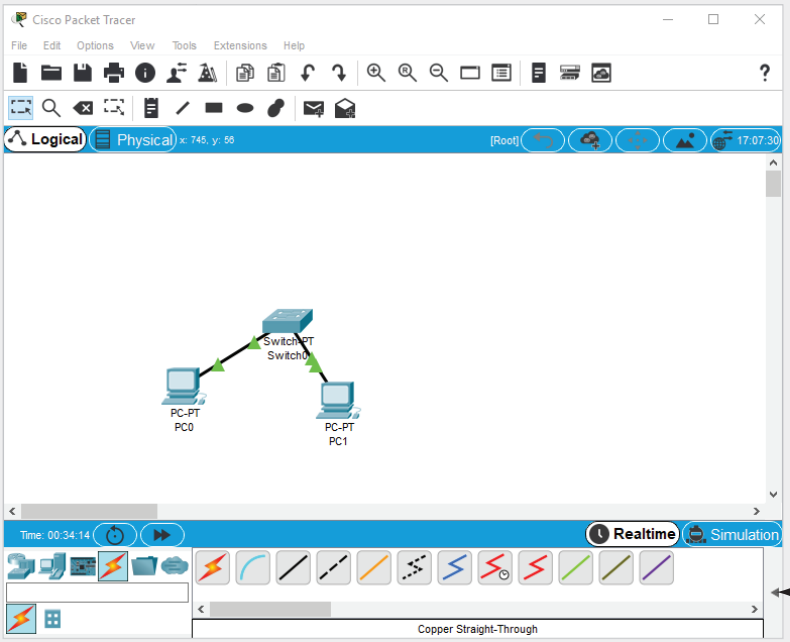

Figure 1-33 Two PCs connected to a switch in Packet Tracer

Source: Cisco Systems, Inc.

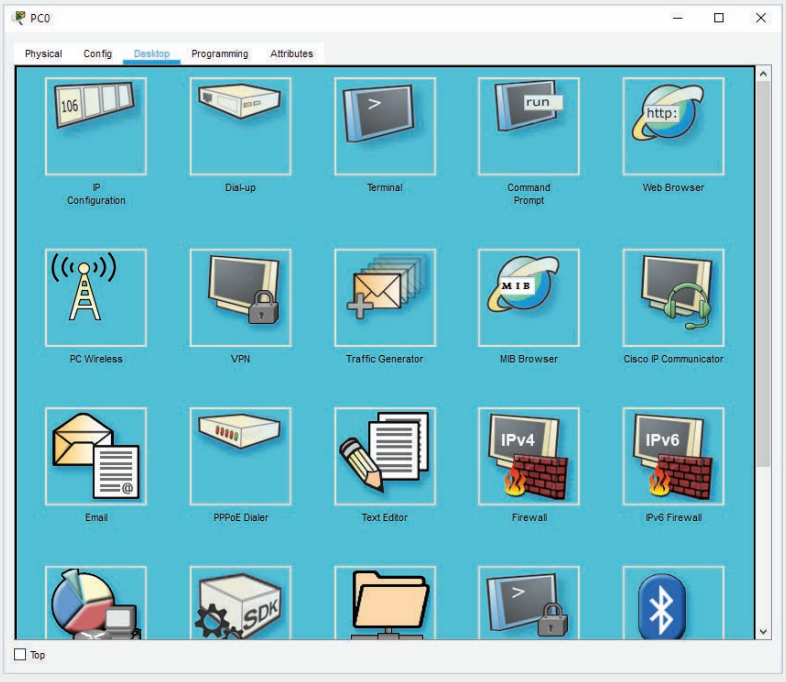

Figure 1-34 The Desktop tab for configuring a PC

Source: Cisco Systems, Inc.

9. Close the PC0 configuration dialog box and then repeat the process for PC1, using IP address **172.20.1.2** with the same subnet mask. Close the PC1 configuration dialog box.
10. Hover your mouse over each PC. You'll see that the IP address column of the pop-up window shows the new IP address.
11. To send a packet from PC0 to PC1, click the closed envelope icon in the top menus (the second icon from the right). Click **PC0** and then click **PC1**. It doesn't look like much happened. To see results, you need to open the results pane in the lower-right corner of the window. Click the left arrow shown in Figure 1-33 to see a panel open. You should see a Successful result (see Figure 1-35).

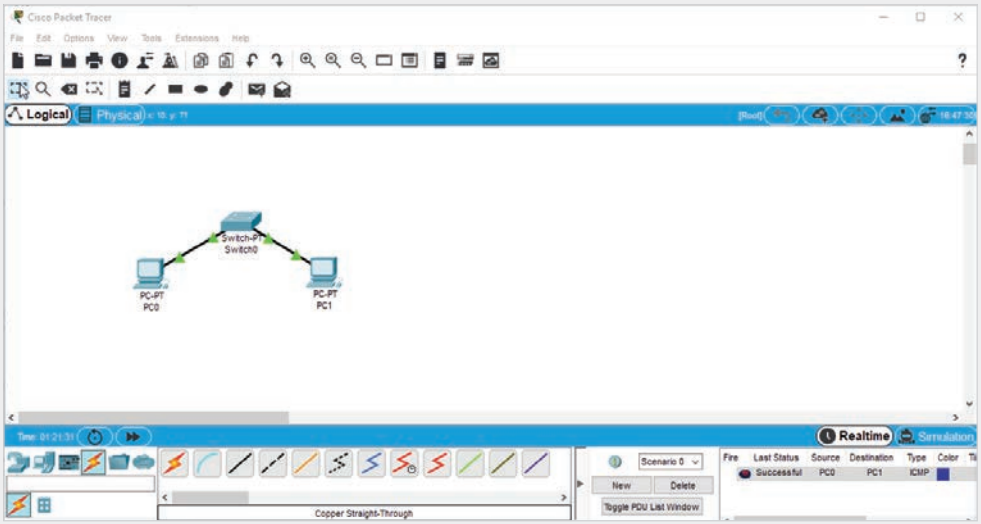

Figure 1-35 The results panel

Source: Cisco Systems, Inc.

12. With the results panel open, you can now send more packets and see the results in the panel.
13. Close Packet Tracer. When prompted to save the file, click **No**.

Critical Thinking

The following activities give you critical thinking challenges. The challenge labs later in this text give you an opportunity to use the skills you have learned. Case projects offer a practical networking problem for which you supply a written solution.

Case Project 1-1

Networking Gadgets, Inc. currently employs 8 people but plans to hire 10 more in the next four months. Users will work on multiple projects, and only users assigned to a project should have access to the project files. You're instructed to set up the network to make it

easy to manage and back up yet still provide centralized storage for project files. Would you choose a peer-to-peer network, a server-based network, or a combination? Why?

Case Project 1-2

CNT Books hired you as a productivity consultant. Currently, it employs six people who will be moving into new office space. You are to configure a network that allows them to share files and printers. Employees must also be able to control resources on their own machines. The company wants the most inexpensive solution and only minimal training for employees. Would you choose a peer-to-peer network or a server-based network? Write a list of supplies you might need to purchase to perform this task. What computer configuration tasks might you need to perform?

Case Project 1-3

CNT Books has expanded considerably since you got the network up and running three years ago. It now occupies an entire floor in the building, and its LAN has grown to include several servers and more than 60 workstations. CNT Books has recently purchased another book company and needs more space and computers. Expansion plans include leasing another floor four stories above the current offices in the same building and adding 35 workstations and at least one more server immediately, with additional equipment purchases expected. What type of network is called for—LAN, WAN, MAN, or internetwork? What additional devices might be needed to ensure efficient network communication?

Case Project 1-4

Chapter 2 discusses network hardware. To prepare for this topic, search for the following terms online. Read at least one article about each term and be prepared to discuss these terms in class:

- Network interface card
- Hub
- Switch
- Router