CHAPTER 5
Networks and Telecommunications

SOCIETY TODAY RELIES on networks and telecommunications to support interaction and business transactions. The hardware components and software that provide these communications functions are critical parts of business infrastructure, and many organizations could not operate if their networks were unavailable or became unreliable. With the expansion of cloud-based and distributed services in enterprise operations, networks have become integral parts of critical infrastructure. Network security involves meeting an organization's fundamental need for network availability, integrity, and confidentiality. To satisfy this multifaceted need, data transmitted through the network must be protected from modification (either accidental or intentional) and encrypted so it cannot be read by unauthorized parties, and all network traffic sources and destinations must be verified (i.e., nonrepudiation). Secure networks must fulfill five basic requirements:

- Access control
- Network stability and reliability
- Integrity
- Availability
- Confidentiality, or nonrepudiation

This chapter examines how you can secure network infrastructures and telecommunications. Moreover, it introduces the basic elements of a network, explains the security issues surrounding networks, and presents some of the building blocks for securing both the data that travels throughout the network and the services the network infrastructure supports.

Chapter 5 Topics

This chapter covers the following topics and concepts:

- What the Open Systems Interconnection (OSI) Reference Model is
- What the main types of networks are
- What Transmission Control Protocol/Internet Protocol (TCP/IP) is and how it works
- What network security risks are
- How to identify and implement basic network security defense tools
- How wireless networks work and what threats they pose to network security

Chapter 5 Goals

When you complete this chapter, you will be able to:

- Describe the OSI Reference Model
- Understand network types, protocols, and security risks
- Choose basic tools to defend against network security risks
- Understand wireless networking and the threats it can pose to network security

The Open Systems Interconnection Reference Model

The **Open Systems Interconnection (OSI) Reference Model** is a theoretical model of networking with interchangeable stacked layers that can be used as a template for documenting, building, and using a network and its connected resources. The beauty of it is that you can design technology for any one of the layers without worrying about how the other layers work. You merely need to make sure that each layer knows how to talk to the layers above and below it. The OSI Reference Model defines a stack of layers, starting from the Physical Layer, at the bottom, which interacts with the physical hardware of the network infrastructure. **FIGURE 5-1** shows each layer of the OSI Reference Model.

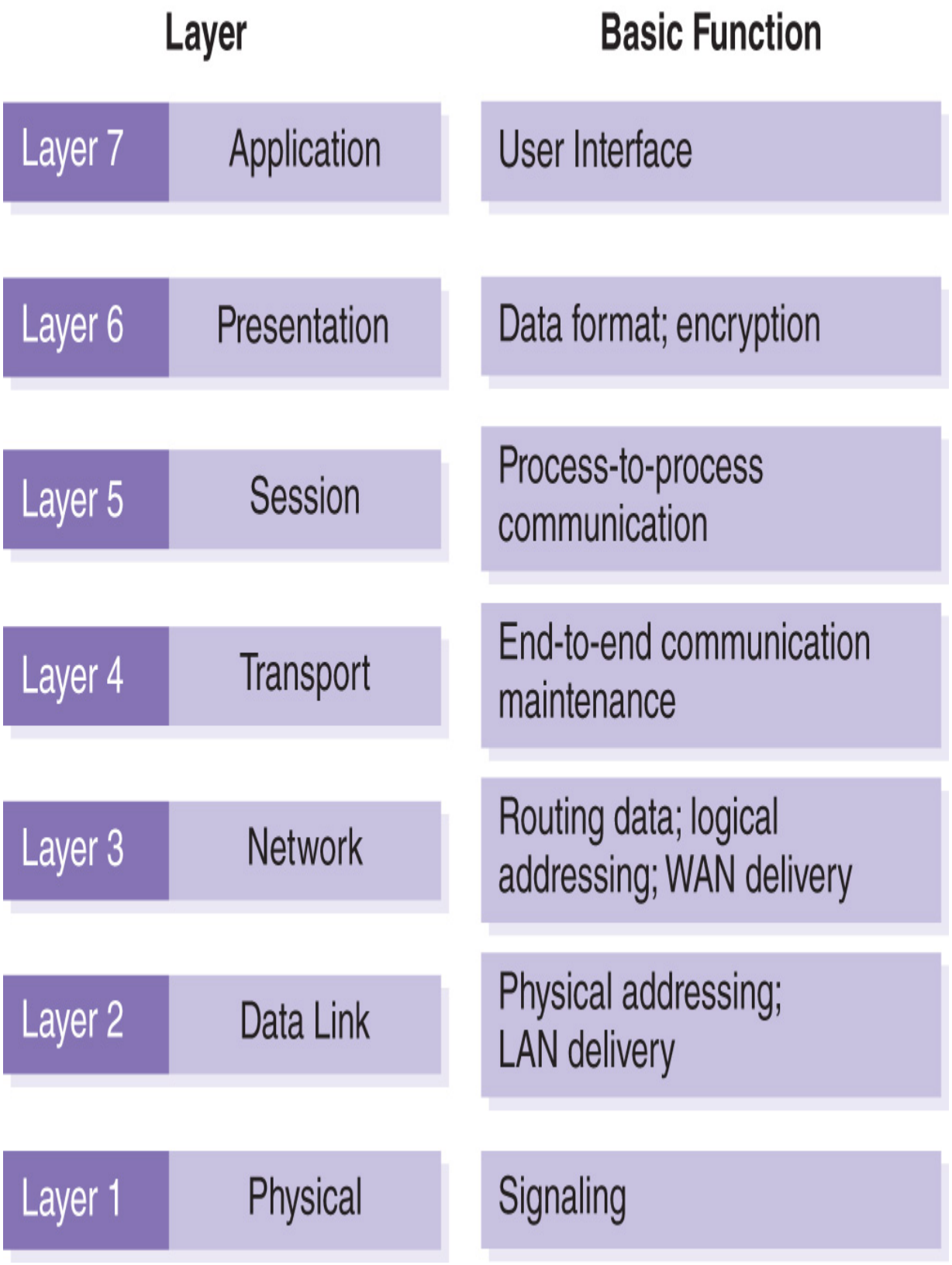


FIGURE 5-1 The OSI Reference Model.

Following are the individual layers of the OSI Reference Model (starting from the top of the stack):

- **Application Layer (Layer 7)**—This layer is responsible for interacting with end users through application software and thus includes all programs on a computer that allow users to interact with the network. For example, email software is included in this layer because it must transmit and receive messages over the network, whereas a simple game like Solitaire does not fit in this layer because it does not require the network in order to operate.
- **Presentation Layer (Layer 6)**—This layer is responsible for the coding of data, or translating it into a format that is more secure (sometimes) and efficient for transmission. This layer includes file formats and character representations. From a security perspective, encryption generally takes place at the Presentation Layer.
- **Session Layer (Layer 5)**—This layer is responsible for maintaining communication sessions between computers. It creates, maintains, and disconnects communications that take place between processes on different computers or devices over the network.
- **Transport Layer (Layer 4)**—This layer is responsible for breaking data into packets and properly transmitting them over the network. Flow control and error checking take place at the Transport Layer.
- **Network Layer (Layer 3)**—This layer is responsible for the logical implementation of the network. One very important feature of this layer is logical addressing (covered later in this chapter). In TCP/IP networking, logical addressing takes the familiar form of IP addresses.
- **Data Link Layer (Layer 2)**—This layer is responsible for transmitting information on computers connected to the same local area network (LAN). Device manufacturers assign each hardware device a unique Media Access Control (MAC) address, and this is the layer in which these MAC addresses are used.
- **Physical Layer (Layer 1)**—This layer is responsible for the physical operation of the network. It must translate the binary ones and zeros of computer language into the language of the transport medium by translating data into electrical pulses for copper network cables, bursts

of light for fiber-optic networks, and radio signals for wireless networks.

TIP

An easy way to remember the layers of the OSI Reference Model is with a mnemonic, for example, “All People Seem To Need Data Processing.” If you like food mnemonics better and want to remember the OSI layers starting from the bottom layer (Layer 1), you could use “Please Do Not Throw Sausage Pizza Away.”

The OSI Reference Model enables developers to produce each layer independently. As an example, if you write an email program that operates at the Application Layer, you only need to worry about getting information down to the Presentation Layer. The details of the network you’re using are irrelevant to your program because other software takes care of that automatically. Similarly, if you’re making cables at the Physical Layer, you do not need to worry about what Network Layer protocols will travel on that cable. All you need to do is build a cable that satisfies the requirements of the Data Link Layer.

The Main Types of Networks

A security professional must learn a lot about networking because a good working knowledge about networks and how to secure them is crucial to protecting an organization from network failure or data breach. Many of the devices used in the security field protect networks, and those that do not often rely on them to function. In this section, you will examine the two main types of networks—wide area networks (WANs) and LANs—and explore their function as well as some of the ways to connect a LAN to a WAN. Finally, you will take a brief look at the most important network devices.

Wide Area Networks

As the name implies, WANs connect systems over a large geographic area. **FIGURE 5-2** shows the Internet (the most common WAN), which connects many independent networks together, thus allowing people at different locations to communicate easily with each other. Moreover, the Internet hides the details of this process from the end user. For example, when you send an email message, you do not have to worry about how the data moves. You just click Send and let the network deal with all the complexity.

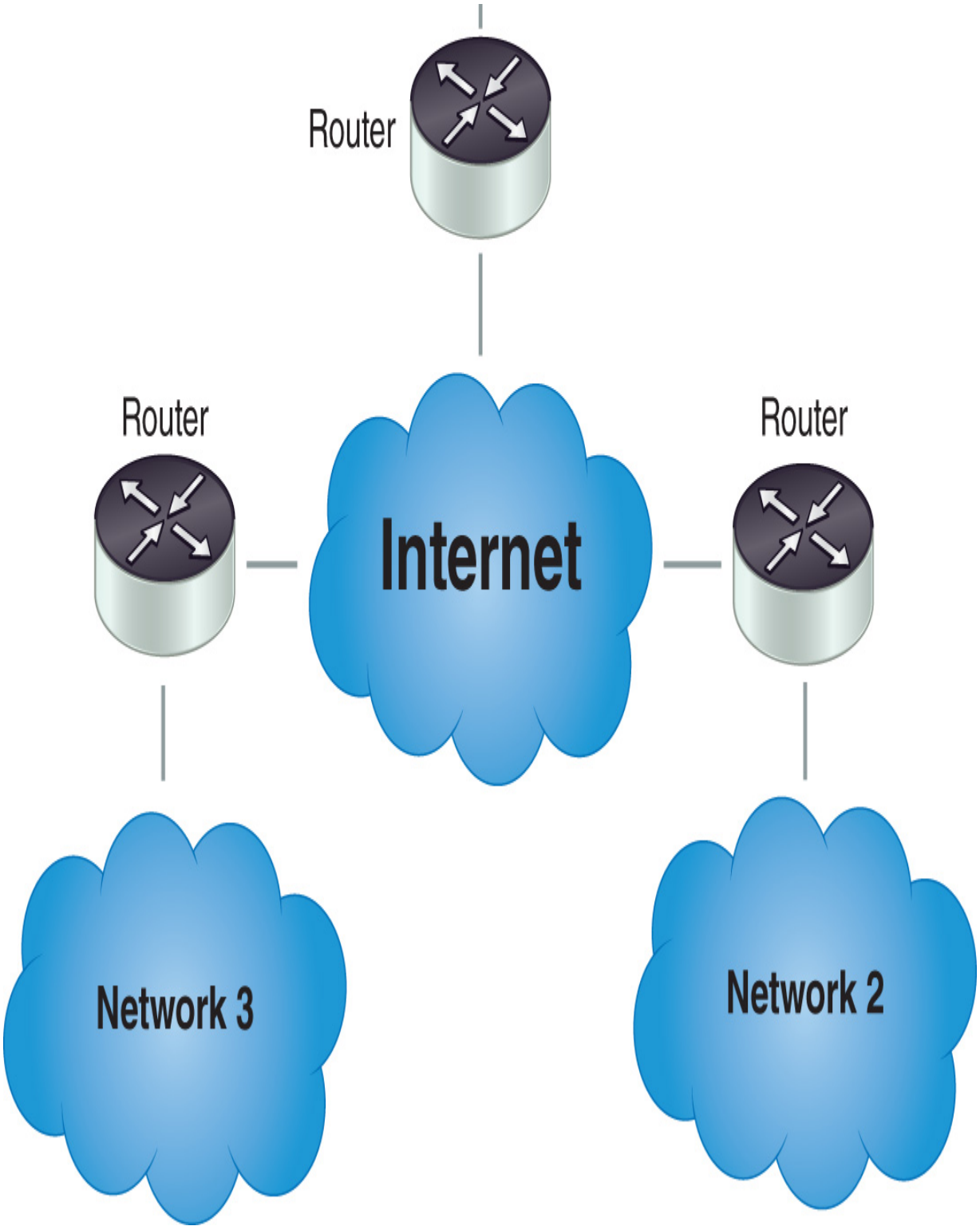


FIGURE 5-2 Wide area networks.

From a security perspective, it's important to remember that the Internet is an open network, which means that, once data leaves the network, its security cannot be guaranteed. The data might travel any path to get to its destination, and anyone might be able to read or modify it along the way. A good analogy for this concept is to think of data on the Internet as being more like a postcard than a letter in a sealed envelope. Fortunately, security technology, such as encryption, enables you to hide the meaning of your data when you're sending it across the Internet, a process that is similar to sending a postcard but writing the message in a secret code. More information about network encryption will follow in the chapter.

Most of today's organizations use the Internet to connect different locations to each other and to connect with their customers. Using the Internet is a low-cost way to connect sites because it is usually easy and inexpensive to connect a network to the Internet; however, you must make sure that you consider the security issues surrounding the use of an open network such as the Internet. Again, encryption technology can help reduce this risk.

Some organizations prefer to use their own private networks for connecting remote sites, either for security reasons or they want the guaranteed reliability of those networks. However, even though this is a very good option for security and reliability reasons, it is also very expensive. An organization can work with a communications provider to develop its own private WAN, and it can also create a virtual private network (VPN) across a WAN (you'll learn about this later in the chapter).

Connectivity Options

There are multiple methods you can use to connect to the Internet. Most home users choose either a cable modem or a digital subscriber line (DSL) from the telephone company, but they can also choose Internet service providers (ISPs), most of which are increasingly providing high-bandwidth Internet service using fiber optics, a service option that enables much faster Internet connections than previous service options. As Internet use increases, ISPs continue to add more connection choices, but, in many cases, the number of available options for connecting to the Internet depends on where a person lives. More densely populated areas tend to offer more options and faster connection speeds. Even if users have no access to cable, DSL, or fiber-optic service, they can still connect to the Internet using satellite or old-

fashioned dialup services (yes, dialup still exists), or they can connect to the Internet through a wireless carrier. Advances in wireless technology make cellular connections affordable in many areas, and service area coverage increases daily.

Smartphones generally connect to third-generation (3G); fourth-generation (4G); and, most recently, fifth-generation (5G) networks, and many of these devices also have the ability to connect to Wi-Fi networks using 802.11 standards. Cellular 3G/4G/5G networks provide stable Internet and voice communication over a wide area. With cellular service, the connection to the Internet appears to be continuous to the user, even while the devices are actually moving from cell to cell. However, many cellular network carriers impose data transfer limits and charge fees for access or slow down connection speeds when users exceed these limits, and, thus, mobile device users often prefer Wi-Fi network connections due to the higher network speed and lower usage costs. Nowadays, it is easy to find free Wi-Fi access at many coffee shops and hotels and in a wide variety of other locations, which helps to make mobile computing a stable option for the average user.

Cellular network Internet connections are very popular with individual users and businesses due to the convenience of mobility. Today's carriers currently offer devices for laptops and mobile access points. In fact, many smartphones and tablets can act as wireless access points for other devices. These mobile access point devices connect to the Internet using a cellular network connection and convert the connection to a Wi-Fi connection for capable devices, which means that you can connect a laptop, smartphone, and several other devices to the Internet anywhere you are located in your carrier's coverage area. This ability can be a huge advantage over using free Wi-Fi because the Internet connection speeds are generally slower using 3G or 4G wireless access devices, whereas the newest 5G devices and networks can provide competitive connection speeds to Wi-Fi. Although 3G and 4G are slower, such connections are far more secure, which makes sharing an Internet connection at a coffee shop with an attacker on the same network less worrisome. Most public Wi-Fi networks are very insecure, so sacrificing a little speed to get a secure connection may be worth it.

Businesses also have many choices for Internet service, and, surprisingly, many of them are the same choices available to home users. For example, most ISPs offer business service in addition to their consumer offerings, but

it is often at a much higher speed than home connections to support the needs of business users. Of course, ISPs generally charge a premium fee for this increased speed.

Again, regarding the OSI Reference Model, the important thing to remember is that the chosen connectivity option will not affect what can be done with the network. Rather, the differences relate to the way the signal gets into the building (i.e., telephone lines, cable lines, dedicated wires, or radio signals) and the speed and reliability of the service.

Routers

A **router** is a device that connects a LAN to a WAN or other networks and selectively interchanges packets of data between them by examining network addresses to decide where to send each packet. The placement of a router within the network architecture affects configuration choices. You can place routers in two basic locations (see **FIGURE 5-3**):

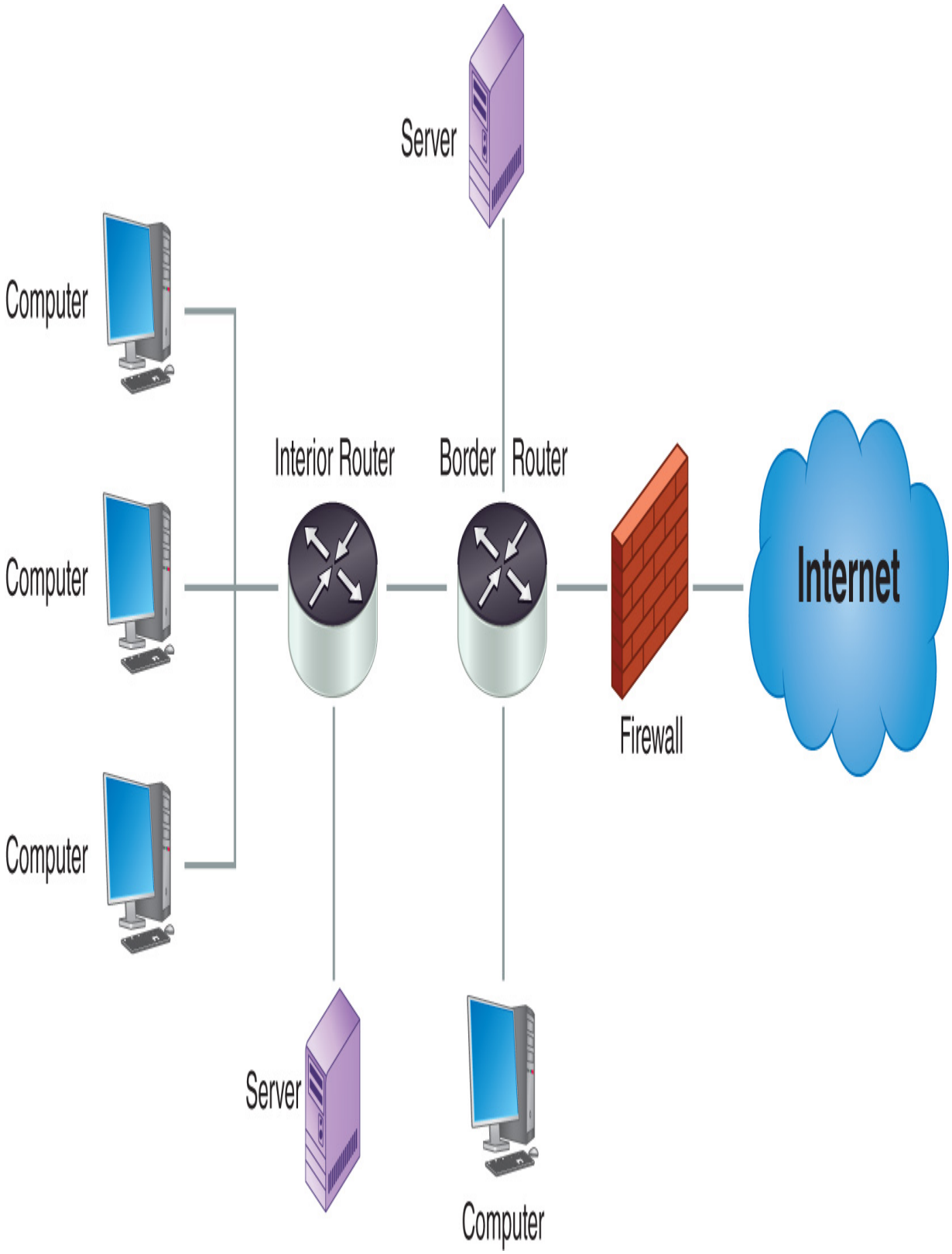


FIGURE 5-3 Router placement.

- **Border routers**—A border router sits between a WAN (normally the Internet) and an internal network. Because a border router is exposed to a WAN, it is subject to direct attack from outside sources. When you configure any router, you should determine whether it is the only point of defense or is one part of a multilayered defense. The latter, of course, is a far better and more secure option because a single defense router can protect some internal resources but is subject to attack itself.
- **Internal routers**—Internal routers can also provide enhanced features to internal networks. They can help keep subnet traffic separate and provide dual protection of keeping undesired traffic out of and desired traffic in a subnet. For example, an internal router that sits between the network of an organization's research department and the network for the rest of the organization can keep the two networks separate, keep confidential traffic inside the research department, and prevent nonresearch traffic from crossing over into the research network from the organization's other networks.

Routers can be configured to allow all traffic to pass or to protect some internal resources and can use **network address translation (NAT)** and packet filtering to improve security. One of the original purposes of NAT was to compensate for a shortage of IP addresses, but, today, NAT's purpose is to hide a system's real **IP address** by using an alternate public IP address. Therefore, an attacker will have more difficulty identifying the layout of networks behind a firewall that uses NAT.

TIP

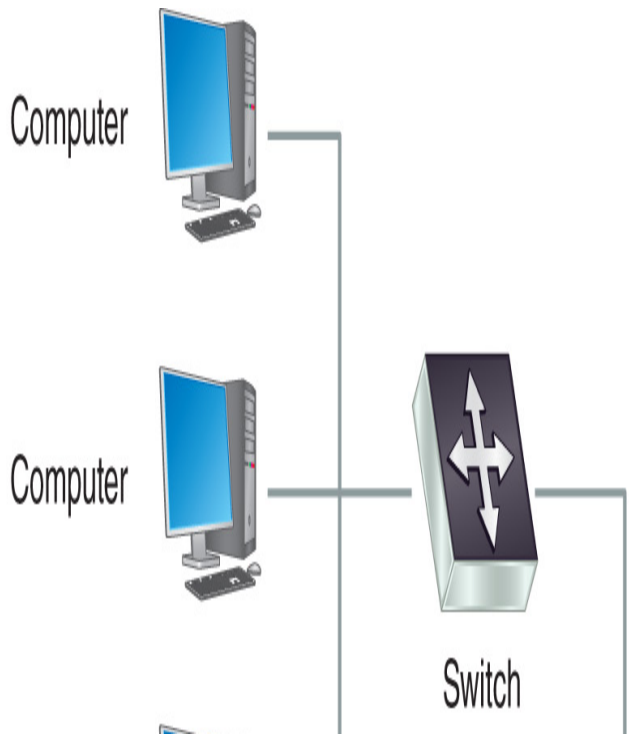
Regardless of where you place routers, you must ensure they are secure. A *secure router configuration* is a collection of settings that ensure that routers are allowing only valid network traffic to flow to and from valid nodes. Therefore, you must configure each router properly and then, because attackers like to reconfigure network devices to allow their attacks to be more successful, monitor to ensure that no unauthorized configuration changes occur.

Another function of a router or firewall is to filter packets, a process that happens each time the router or firewall receives a data packet. The device filters packets by comparing them to rules configured by the network administrator, which tell the device whether to allow or deny the packet into the network. If no rule specifically allows the packet, the firewall blocks it, after which the firewall may send a rejection notice or just silently drop the packet.

NAT and filtering packets are two ways in which routers can be used to help defend a network because they provide some defense against basic attacks. However, because no single technology is a "silver bullet," you should still use firewalls to protect networks and other technologies described in this text to secure data.

Local Area Networks

LANs provide network connectivity for computers that are in the same geographic area and are typically connected to each other with devices such as hubs and switches. This switching infrastructure is located behind the organization's router, as shown in **FIGURE 5-4**.



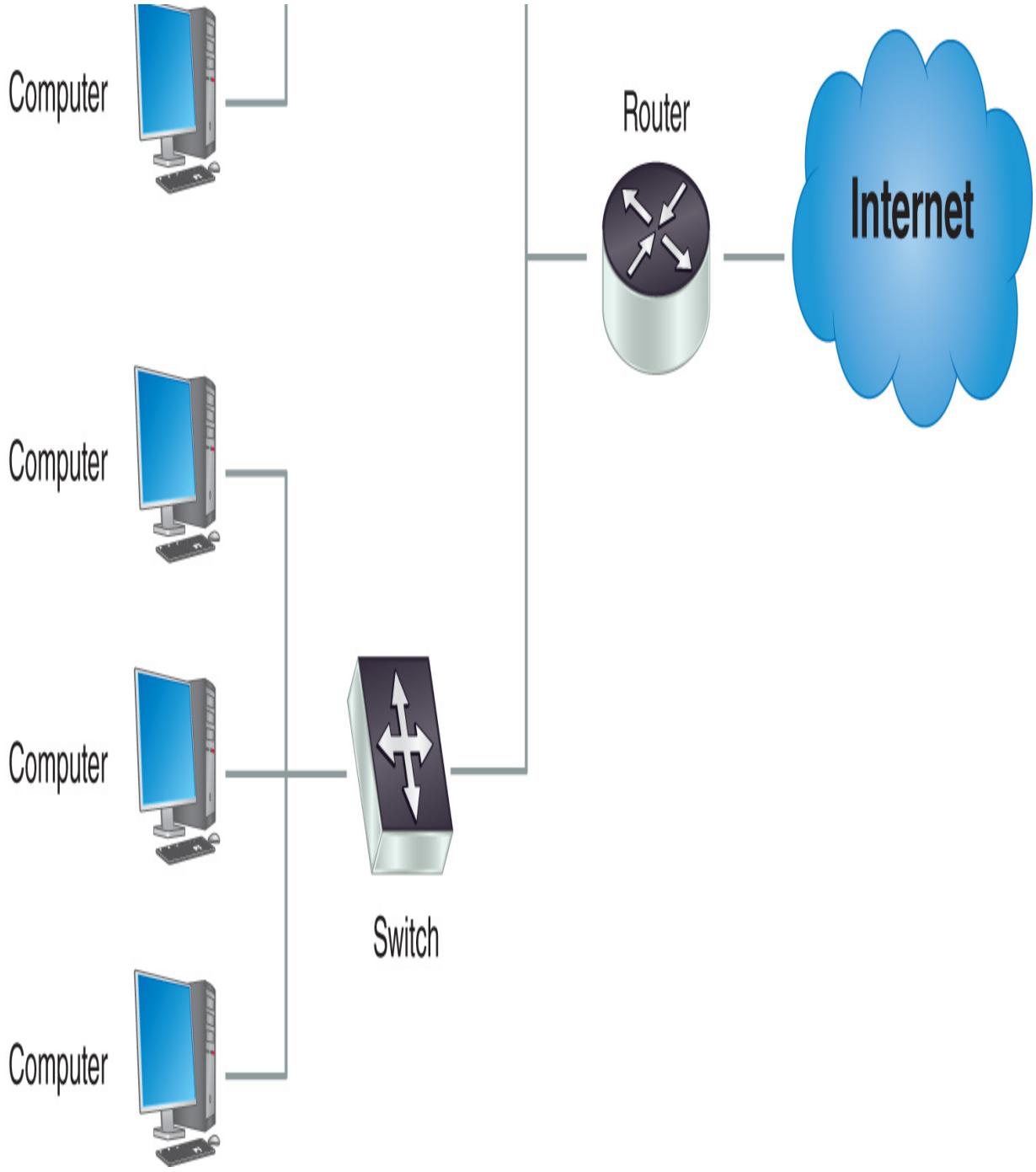


FIGURE 5-4 Local area networks.

In many cases, computers and devices on the same LAN do not protect themselves from each other. They are intentionally configured this way because collaboration between LAN systems often requires connections from the Internet that would not normally be allowed, which is another reason it is

extremely important to have good security on systems located on a LAN. If malware infects one system on the LAN and the other systems do not protect themselves, the malware can spread quickly to all of them.

Ethernet Networks

Through the end of the 20th century, many types of LANs existed, but, today, almost every network has switched to a single technology called Ethernet. In early Ethernet networks, all computers connected to a single wire and had to fight with each other for turns to use the network, which of course was very inefficient. Fortunately, technology has evolved so that, for each system, modern Ethernet networks use a dedicated wire, which connects each one back to a switch that controls a portion of the LAN.

Ethernet has become the most common LAN technology in use, and its standard defines how computers use MAC addresses to communicate with each other on the network and governs both the Physical and Data Link layers of the OSI Reference Model. Even many competing technologies now have variants that run on top of Ethernet. For example, Internet Small Computer System Interface (iSCSI) is a storage networking standard used to link data storage devices to networks using IP for its Transport Layer. An alternative to iSCSI for both optical and electrical networks is fibre channel, which was originally used in supercomputers to connect storage devices but has since spread into common usage across many types of computers. The Fibre Channel over Ethernet (FCoE) protocol makes it even easier than fibre channel to connect fibre channel–capable devices to an Ethernet network, which is yet another example of the way layered network protocols make it easy to implement many types of network devices.

LAN Devices: Switches

The primary LAN device is a **switch**, which is a hardware device that performs the basic function of connecting several systems to the network. Legacy networks from the past century commonly used a device called a **hub**, which simply connected a number of ports to one another and echoed all incoming traffic to all ports. Switches are different from hubs in that they can perform intelligent filtering because they "know" the MAC address of the system connected to each port. When they receive a packet on the network,

they look at the destination MAC address and send the packet to *only* the port where the destination system resides.

Virtual LANs

A virtual LAN (VLAN), which is created in the router and switch configuration setup, is a collection of logically related network devices that are viewed as a partitioned network segment. It gives administrators the ability to separate network segments without having to physically separate the network cabling and can also be used to isolate logical groups of devices to reduce network traffic and increase security. For example, if you create a VLAN for the Human Resources (HR) department, all sensitive information traveling from one HR computer to another HR computer is hidden from all non–HR computers.

TCP/IP and How It Works

Just as people need a common language in order to communicate, so do computers. Fortunately, almost every computer now speaks a standard language (i.e., protocol) called the Transmission Control Protocol/Internet Protocol (TCP/IP).

A **protocol** is a set of rules that govern the format of messages that computers exchange, and a network protocol governs how networking equipment interacts to deliver data across the network. Together, these protocols manage the transfer of data from a server to an endpoint device, from the beginning of the data transfer to the end. In this section, you will learn about the protocols that make up TCP/IP and the basics of TCP/IP networking.

TCP/IP Overview

TCP/IP is not just one protocol but rather a suite of protocols that operate at both the Network and Transport layers of the OSI Reference Model and govern all activity across the Internet and through most corporate and home networks. It was developed by the U.S. Department of Defense to provide a highly reliable and fault-tolerant network infrastructure, for which reliability, not security, was the focus.

TCP/IP has several responsibilities, as illustrated in **FIGURE 5-5**, which shows a portion of the suite. Note that TCP isn't the only protocol that runs over IP. Use Datagram Protocol (UDP) works alongside TCP at the Transport Layer to support upper-level protocols. These two common protocols provide different types of transport services and are useful in different scenarios. Also, note that not all protocols in this figure, such as Telnet and File Transfer Protocol (FTP), are secure. Always choose protocols based on their ability to support secure communication.

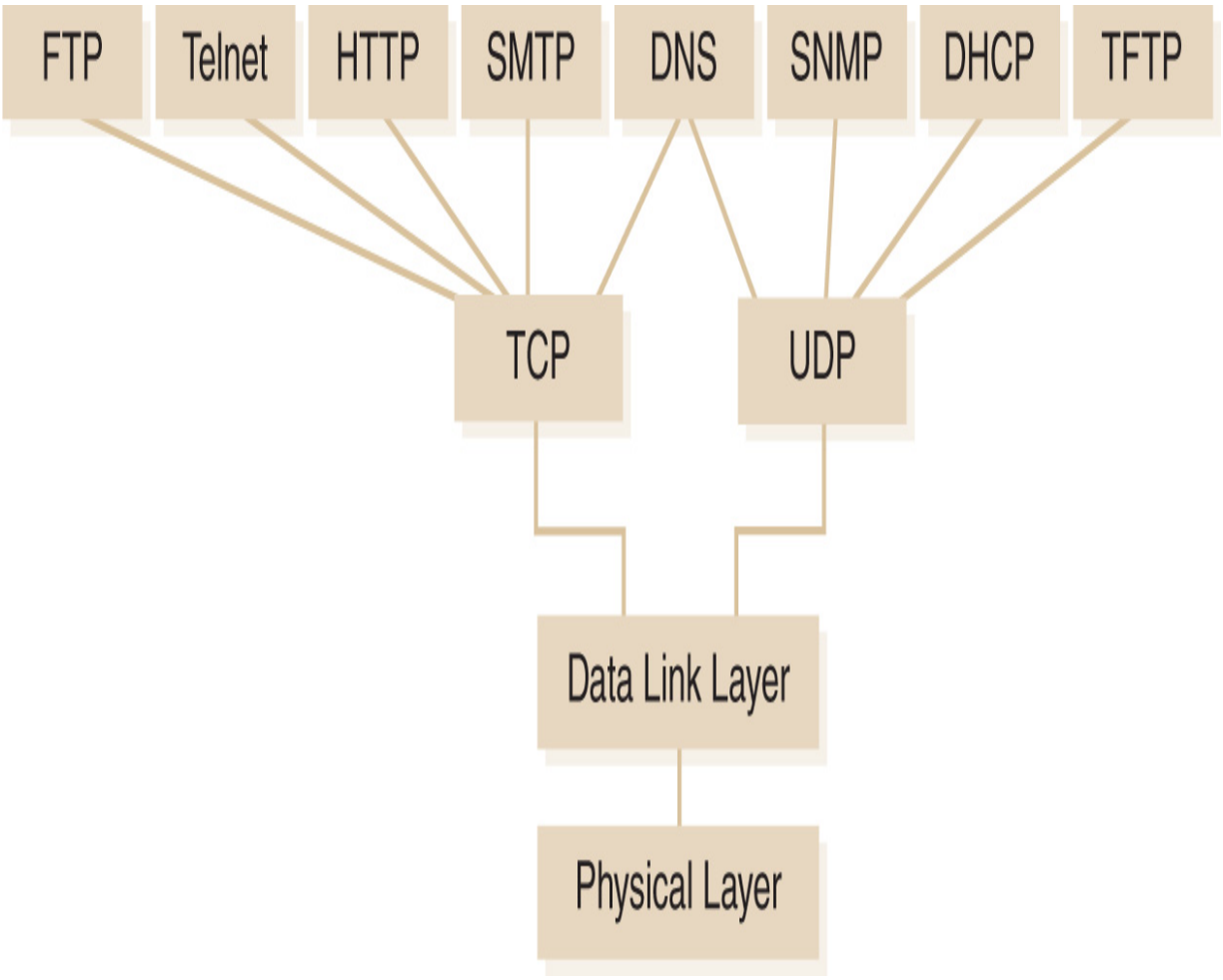


FIGURE 5-5 TCP/IP protocol suite.

IP Addressing

One of the primary functions of Network Layer protocols is to provide an addressing scheme, and TCP/IP is located in this layer. There are two versions of the IP protocol, and thus IP address formats, in use today. IP version 4 (IPv4) is still the more common version, even though its addressing space was exhausted in 2011, over 10 years ago, but its replacement version, IP version 6 (IPv6), is gaining in popularity and percentage of Internet traffic. Currently, in 2021, IPv6 makes up only 32 to 35 percent of total Internet traffic, with its slow adoption being caused primarily by legacy applications that are dependent on IPv4. Even so, most countries prefer and continue to roll out IPv6-capable networks, so adoption is coming. All told, even in the 2020s, it's still worthwhile to learn how IPv4 addressing works.

An **IPv4 address** is a 4-byte (32-bit) address that uniquely identifies every device on the network. With an explosion in the number of network devices during the end of the past century, it was clear that IPv4 would not accommodate unique addresses for each device, which is one of the reasons IPv6 was developed. **IPv6 addresses** are 128 bits long and can provide far more unique device addresses than the older standard as well as containing many additional features and being more secure.

FIGURE 5-6 shows the difference between the notation for an IPv4 and IPv6 address. As you can see, IPv4 addresses use the dotted-quad notation, which represents each of the 4 bytes as an integer between 0 and 255. Moreover, each IPv4 address consists of a network address and a host address. For example, the IPv4 address 192.168.10.1, shown in the figure, is for the network address 192.168 and the host address 10.1. The dividing line between the network and host addresses is a network configuration parameter known as the subnet mask, which can change based on the way an administrator configures the network. All hosts that share the same network address are part of a **subnet**, which is a partition of a network based on IP addresses. Because IPv6 addresses are so much larger than IPv4 addresses, IPv6 uses a completely different notation. As shown in the figure, IPv6 addresses are expressed as hexadecimal values, separated into eight groups of 16 bits, whereas IPv4 addresses consume only the two rightmost groups of 16 bits of an IPv6 address. The difference between the number of addresses available in IPv4 and IPv6 cannot be illustrated in a simple figure. Think of it this way: If you could write every IPv4 address in a two-inch-square block, the space you would need to write all IPv6 addresses, using the same font, would be about as big as the solar system.

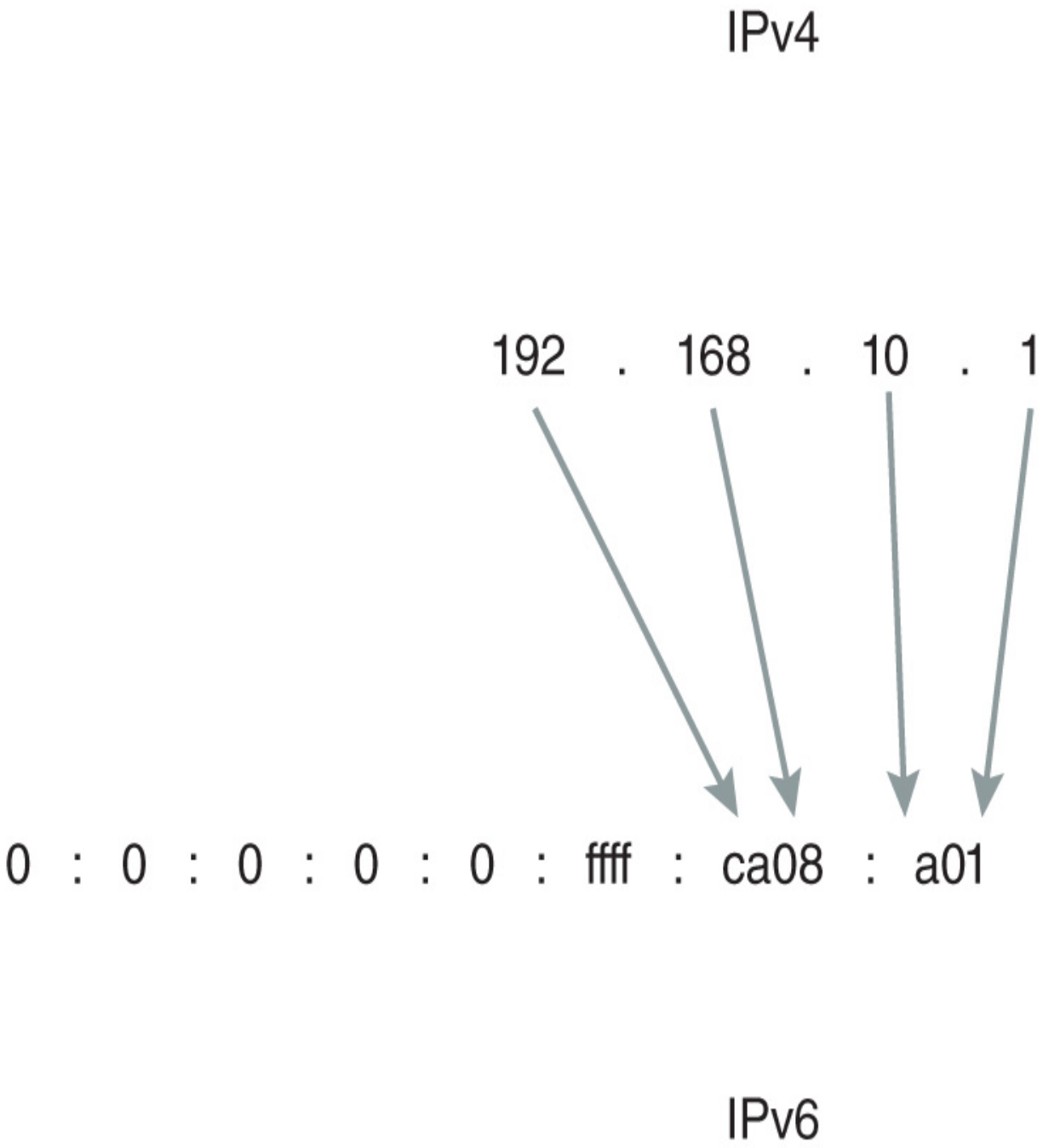


FIGURE 5-6 IP addressing.

Because every computer needs its own IP address, keeping track of address assignments can become time consuming; therefore, many organizations that use IPv4 use the **Dynamic Host Configuration Protocol (DHCP)** within a network to simplify the configuration of each user's computer. This protocol allows each computer to get its configuration

information dynamically from the network instead of the network administrator's providing the configuration information to the computer. DHCP provides a computer with an IPv4 address, subnet mask, and other essential communication information, which greatly simplifies the network administrator's job. An example of DHCP communication appears in **FIGURE 5-7**. Technically, DHCP works only with IPv4 networks, whereas DHCPv6 provides IPv6 addresses.

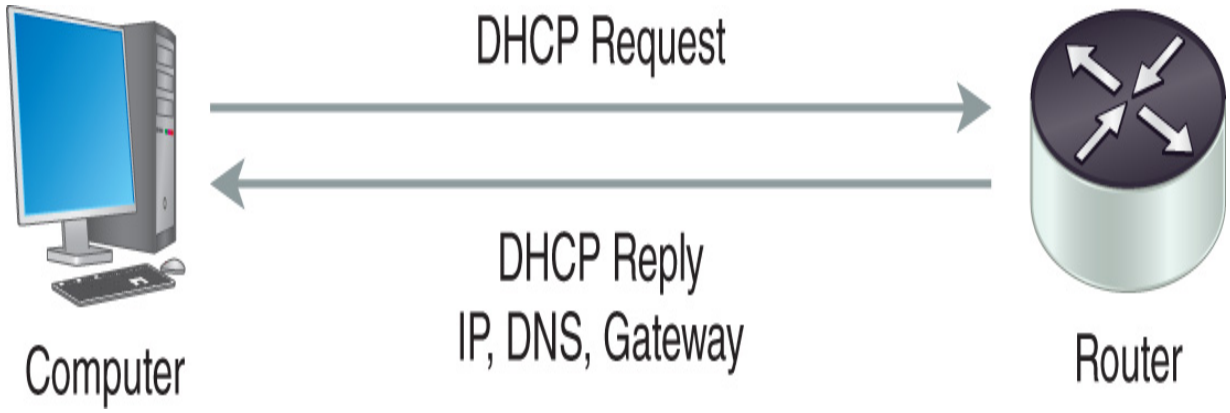


FIGURE 5-7 DHCP communication.

NOTE

The Internet Assigned Numbers Authority (IANA) has released only about 20 percent of the available IPv6 addresses for use. While this addressing restriction may suggest a limit on available IPv6 addresses, remember that IPv6 addresses are 128 bits long, which allows for 128-bit (2,128) addresses, or 3.4 × 1,038 unique IP addresses. That would mean, even with making the first few bits static, there are still trillions of trillions of IPv6 addresses for every person on Earth! Much more information on IPv6 is available on IANA's dedicated IPv6 site at *www.arin.net/resources/guide/ipv6/*.

Common Ports

Computers and devices that are connected to networks commonly use the network for more than one purpose, and software application programs use the network to communicate with many other remote services running on remote computers and devices. Because any network computer or device may host several services, programs need a way to tell one service from another. Therefore, to differentiate services running on a device, networking protocols use a **network port**, which is just a number that tells a receiving device where to send messages it receives. Once the address of the remote device is known, client software sends network messages to specific ports, and server software listens to ports for incoming messages. For example, almost all unencrypted traffic between web browsers and web servers uses port 80, which is commonly used for Hypertext Transfer Protocol (HTTP) traffic. No one forces software to use the common ports, but most use them to make it easy for clients and servers to communicate. **TABLE 5-1** lists ports that common services use.

TABLE 5-1 Common port numbers.

PORT	SERVICE/USE
20	FTP data transfer
21	FTP control
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67/68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
88	Kerberos
110	Post Office Protocol v3 (POP3)
139	Network Basic Input/Output System (NetBIOS) Session Service
143	Internet Message Access Protocol (IMAP)
161	Simple Network Management Protocol (SNMP)
162	SNMP Trap
443	HTTP over Secure Sockets Layer/Transport Layer Security (SSL/TLS)
445	Simple Message Block (SMB) over IP
3389	Terminal Server

Common Protocols

You have learned about some of the most common network protocols, but there are many more protocols that define communication rules for many uses. Although the list in **TABLE 5-2** is not comprehensive, it does include some of the more common and recognizable network protocols.

Technical TIP

Notice that there is no port number listed for SSL or TLS, the reason being that these two protocols are used to provide encryption for higher-level protocols. For example, HTTPS is just HTTP running over SSL or TLS, which means that SSL or TLS will use just the HTTP port (80). Conventionally, HTTPS from a client browser to the server uses port 443. However, the port itself means nothing with regard to security; the SSL protocol is what encrypts the HTTP data. SSL has been around longer than the more secure TLS but is slowly being replaced by it.

TABLE 5-2 Common network protocols.

PROTOCOL	COMMON PORT(S)
DNS (Domain Name System)	53
FTP (File Transfer Protocol)	20 (data), 21 (control)
FTPS (FTP over SSL/TLS)	989 (data), 990 (control)
HTTP (Hypertext Transfer Protocol)	80
HTTPS (HTTP over SSL/TLS)	443
iSCSI (Internet Small Computer System Interface)	860; 3,260 (target)
NetBIOS (Network Basic Input/Output System)	137 (Name service) 138 (Datagram service) 139 (Session service)
SCP (Secure Copy—part of SSH)	22
SFTP (Secure File Transfer Protocol—part of SSH)	22
SNMP (Simple Network Management Protocol)	161
SSH (Secure Shell)	22
Telnet	23
TFTP (Trivial File Transfer Protocol)	69

Internet Control Message Protocol

Once you have configured all the network components, you need to monitor the network for health and performance, which can be done using the **Internet Control Message Protocol (ICMP)**. ICMP is a management and control protocol for IP that delivers messages between hosts about the health of the network. The messages carry information on hosts ICMP can reach as well as information on routing and updates.

NOTE

The IANA maintains a list of well-known services and port numbers. You can find this list at *www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml*.

Two ICMP tools are *ping* and *traceroute*. The ping command sends a single packet to a target IP address called an **ICMP echo request**. This packet is equivalent to asking the question "Are you there?," to which the computer on the other end can either answer yes, by sending an ICMP echo reply packet, or ignore. Because attackers sometimes use the ping command to identify targets for a future attack, many system administrators configure their computers to ignore all such requests.

The traceroute command uses ICMP echo request packets for an entirely different purpose: to identify the path that packets travel through a network. Packets may travel several routes to get from one point on a network to another, and the traceroute command is used to display the path that a particular packet follows so you can identify the source of potential network problems.

Attackers can use ICMP to create a denial of service (DoS) attack against a network. This type of attack is known as a *smurf attack*, named after one of the first programs to implement it. It works by sending spoofed ICMP echo request packets to a broadcast address on a network, hoping that all the hosts on that network will respond. If the attacker sends enough replies, it is

possible to bring down a large network from any Internet-connected device. Fortunately, it is very easy to defend against smurf attacks by configuring a network to ignore ICMP echo requests sent to broadcast addresses.

Network Security Risks

Any data in transit presents a potential attack target, which is the very reason that network security is so important. So far, in this chapter you've learned about how networks carry data and about a few risks facing networks, such as smurf attacks. This section will provide an in-depth look at network security risks as well as cover some of the network security controls that you can put in place to protect a network.

NOTE

Attackers want to gain control of systems on a network because, by controlling computers and devices, they can control the data as well. To achieve their goals, they will exploit network security holes, a discussion of which is beyond the scope of the chapter.

TIP

Historically, network security separated the "good guys" from the "bad guys." Employees, contractors, and partners (and their devices) were generally trusted, and only the anonymous users were explicitly untrusted. As attackers increasingly compromised trusted users to infiltrate networks, security got more complex so that, now, network security philosophy suggests viewing every network as a *zero trust network*, meaning one in which no user or device is implicitly trusted and every user and device must provide a reason to be trusted. Adopting this approach makes it harder for attackers to "sneak into" a network.

Categories of Risk

The three main categories of network security risk are reconnaissance, eavesdropping, and DoS. Each of these risks has different impacts on the confidentiality, integrity, and availability (C-I-A) of data carried across a network and may affect the security of the network itself.

Reconnaissance

Reconnaissance involves an attacker's gathering information about a network for use in a future attack. As an illustrative analogy, consider an army that wants to attack a country. To be successful, the attacking military forces need to gather advance information about their adversary, some of which may include the following:

- Terrain
- Location of roads, trails, and waterways
- Locations and types of enemy defenses
- Weaknesses in the enemy's perimeter
- Procedures for allowing access through the perimeter
- Types of weapons used by the enemy

Similarly, a network attacker would want to know many things before attacking, such as the following:

- IP addresses used on the network
- Types of firewalls and other security systems
- Remote access procedures
- Operating system(s) of computers on the network
- Weaknesses in network systems

Normally, you would not simply make this information available to an attacker, and, therefore, the attacker must employ many tools to obtain it. One such tool is ICMP echo requests, which have already been covered as to why it is important to block them when they are received from outside the organization's network. By taking this simple action, attackers are stopped

from using the ping and traceroute tools to gather information. Another effective strategy to limit the effectiveness of network reconnaissance attacks is to configure systems to provide as little information as possible to outsiders.

Eavesdropping

Attackers might also want to violate the confidentiality of data sent on the network. Again, as an illustrative analogy of network eavesdropping, consider a less complex technology—the telephone. A telephone is easy to tap by hooking up a cable to the telephone switch box on the building and connecting a handset to listen in on calls.

Network eavesdropping is actually easier than telephone eavesdropping because, even though physical access to the network makes it easier to eavesdrop, it is not required. An attacker can compromise a computer on the network and use that computer for eavesdropping. Following are a few options that you can use to protect against this type of attack:

- Limit physical access to network cables.
- Use switched networks. The attacker will then see only information sent to or from the computer attached to the tapped cable.
- Encrypt sensitive data. The attacker still might be able to see the transmission but will not be able to make sense of it.

Using switched networks and encryption will help limit the effectiveness of this type of attack as well as securing systems on the network from malicious code.

Denial of Service

Often, an attacker is not interested in gaining access to the network but, instead, wants to deny its use, which can be an extremely effective tactic because many businesses cannot operate if they lose their networks. An attacker has two primary methods to conduct a DoS attack: flooding a network with traffic and shutting down a single point of failure.

NOTE

Wireless networking presents a completely new world of eavesdropping challenges. You will learn more about that topic later in the chapter.

To make a network unavailable, flooding it with traffic is the simpler of the two methods. A network is like a pipe in that it can carry only so much data before it gets full. Knowing this information, attackers can create a DoS attack by simply sending more data through a network than it can handle. A variation on this theme is a distributed denial of service (DDoS) attack. In this type of attack, black-hat hackers use many systems around the world that they have compromised to flood the network from several directions, making it difficult to distinguish legitimate from attack traffic and, therefore, eventually halting the processing of data on the network.

Even though DDoS attacks have been around for years, they are not considered old types of attacks and are still used to slow down or disable their victims. Today, hacktivists, or activists with hacking abilities, are behind increasing numbers of large-scale attacks to attract attention, generally to a political issue. One such attack came in mid-March of 2020 when a group of hacktivists launched a series of DDoS attacks against the U.S. Department of Health and Human Services (HHS) website. This attack was intended to stop U.S. citizens from getting up-to-date official information on COVID-19 policies and guidelines and to protest rumored nationwide shutdowns to help control the pandemic. Fortunately, HHS was prepared for such attacks and was able to withstand the onslaught of network traffic.

Other DDoS attacks in 2020 focused on various U.S. human rights organizations and often coincided with political and social justice protests that occurred throughout the year. Information technology (IT) service organizations have also become attractive targets because many of their clients are targets of hacktivists. One such company, Cloudflare, which provides anti-DDoS services, was the target of a large DDoS attack that started on June 18, 2020, and lasted four days; at its peak measurement, 754 million packets per second were coming from 316,000 IP addresses. As with

the HHS attack, Cloudflare was properly prepared to fend off the massive attack, which, unfortunately, not all organizations are.

Advances in technology have provided even more opportunities for attackers to cause problems with DoS attacks. One type of attack, the *telephony denial of service (TDoS) attack*, which can be dangerous for essential services, started to become prevalent in 2013 and has become more common in recent years. In a TDoS attack, the attacker attempts to prevent telephone calls from being successfully initiated or received by a person or an organization that depends on telephone calls as a primary mode of communication. Such an attack can disrupt or totally disable telephone communications, thus causing an enormous impact to an organization, such as revenue loss, potential fines, the inability to conduct operations, and a loss of customer confidence. In February 2021, the U.S. Federal Bureau of Investigation (FBI) announced a public warning about TDoS attacks being disruptive to 911 emergency call services.

Protecting an organization against a DoS attack can be difficult, but the most obvious approach is to ensure that the Internet bandwidth is adequate to withstand an extreme load. Some new technologies on the market seek to defend against DDoS attacks, but they are unproven and limited in their effectiveness. The best defense is to detect attacks as early as possible and take action to block the incoming traffic before it renders the network unusable.

Basic Network Security Defense Tools

Defense against these kinds of risks begins with some basic hardware and software tools, such as firewalls, virtual private networks (VPNs), and network admission control.

Firewalls

A **firewall** controls the flow of traffic by preventing unauthorized network traffic from entering or leaving a particular segment of a network. You can place a firewall between an internal network and the outside world or within internal subnetworks to control access to particular corporate assets by only authorized users. Firewalls are critical elements of networking security, but they are just that, elements; they will not solve all security problems, but they do add a much-needed deterrent.

FIGURE 5-8 shows the role of a firewall in a network, which is to separate private networks from the Internet as well as to separate different private networks from each other. This section covers the different types of firewalls and the roles they play in the network topology.

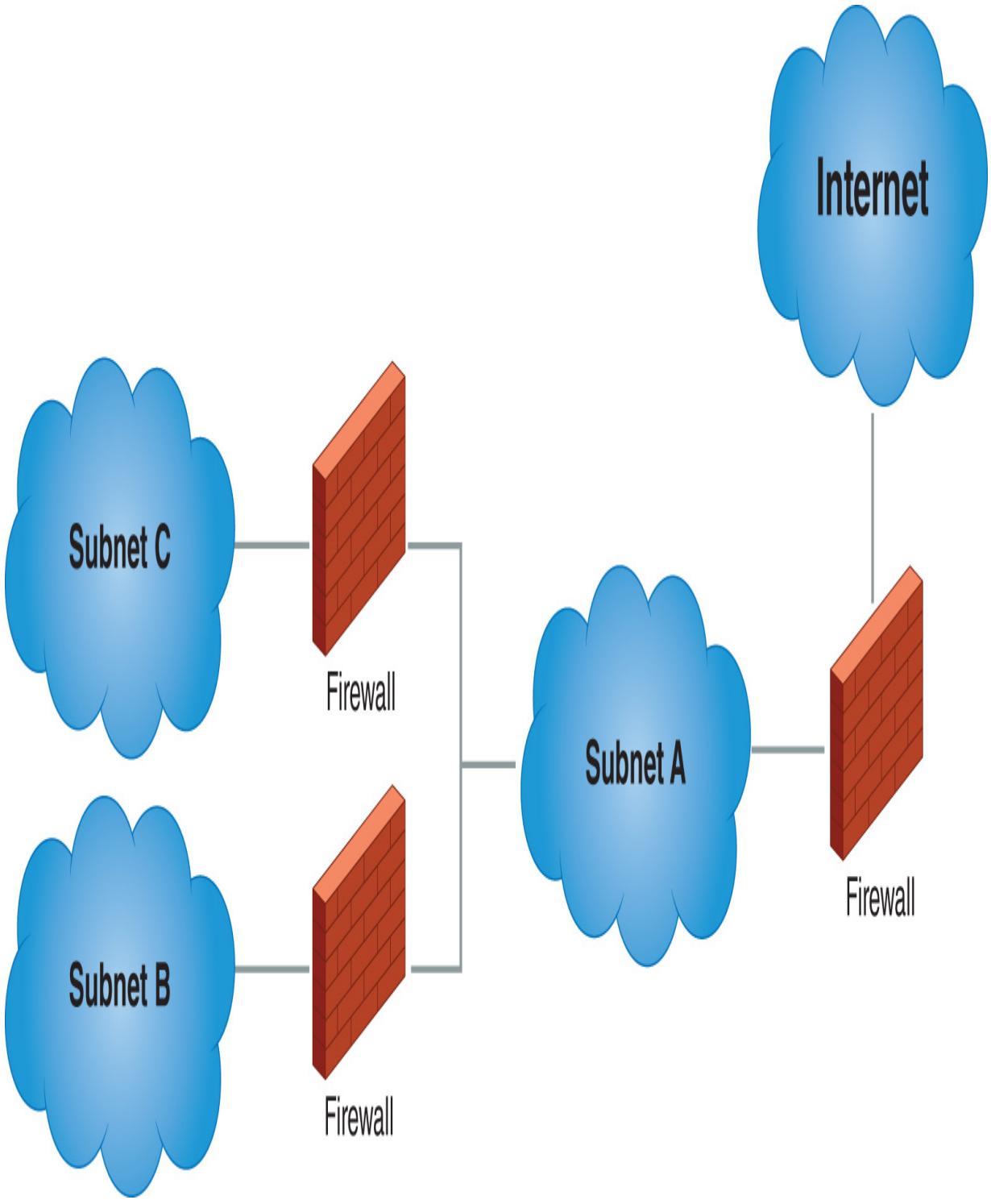


FIGURE 5-8 Firewalls.

Firewalls can be very powerful tools in securing networks. Because each firewall is configured using rules, it provides the most common way to

implement rule-based management, which means simply managing the security of a network by defining rules of what network traffic is and is not acceptable. Firewall rules are filters, defined in a firewall's configuration, that make it easy to implement many of these security requirements. Different types of firewalls use different types of rules, but even the simplest firewalls support access control lists (ACLs), which define rules for handling traffic from one or more hosts using a specific protocol and one or more ports. In addition to securing a host, firewalls can also filter traffic based on ports, often called port security. ACLs can contain very specific rules for a single host, protocol, and port or may contain ranges of hosts and ports with multiple protocols. Each rule tells the firewall how to handle certain types of messages, with the most common actions being allowing and denying. To create the most secure network, configure the firewall to deny all messages except the ones that are explicitly allowed, an approach called implicit deny. This approach can be very secure, but it requires more effort on the part of network administrators to open ports as needed.

Firewalls can help secure networks in several ways, a few of which have already been covered. In addition to these filtering features, they can also provide the following:

- **Flood guard**—Rules can limit traffic bandwidth from hosts, thus reducing the ability for any one host to flood a network.
- **Loop protection**—Firewalls can look at message addresses to determine whether a message is being sent around an unending loop, which can be another form of flooding.
- **Network segmentation**—Filtering rules enforce divisions, or separations, between networks, thus keeping traffic from moving from one network to another.

Firewall Types

The basic function of a firewall is quite simple—to block any traffic that is not explicitly allowed. Firewalls contain rules that define the types of traffic that can come and go through a network, and, each time the firewall receives a network message, it checks the message against its rules. If the message

matches a rule, the firewall allows it to pass, whereas, if the message does not match a rule, the firewall blocks it.

Going beyond this basic functionality, firewall technology includes three main types:

- **Packet filtering**—A **packet-filtering firewall** is very basic. It compares received traffic with a set of rules that define which traffic it will permit to pass through the firewall. It makes this decision for each packet that reaches the firewall and has no memory of packets it has encountered in the past.
- **Stateful inspection**—Unlike the packet-filtering firewall, a **stateful inspection firewall** remembers information about the status of a network communication. Once the firewall receives the first packet in a communication, the firewall remembers that communication session until it is closed. This type of firewall needs to check rules only when a new communication session starts, not each time it receives a packet.
- **Application proxy**—An **application proxy firewall** goes even further than a stateful inspection firewall in that it does not actually allow packets to travel directly between systems on opposite sides of the firewall. Instead, it opens separate connections with each of the two communicating systems and then acts as a broker (or proxy) between the two, which allows for an added degree of protection because the firewall can analyze information about the application in use when making the decision to allow or deny traffic.

Firewalls are not simply preventive controls; instead, they also operate as detective controls and can log as much information as can be analyzed. A structured log analysis process can help identify reconnaissance activity or even attacks that have already occurred. You should regularly monitor all firewall logs to identify potential problems. Because log files from firewalls and other network devices can become very large, using automated log monitors and analysis tools helps to efficiently sort through the log data.

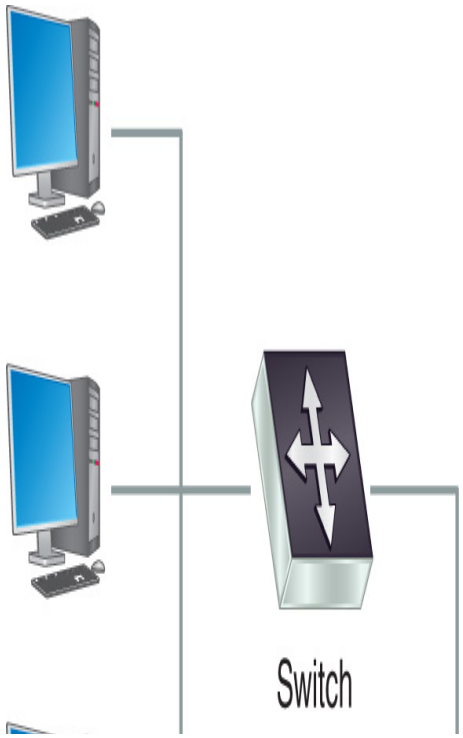
The type of firewall chosen for a network will depend on many factors. If you're placing a simple firewall at the border of a large network, you may want to use a basic packet filter. On the other hand, if you're protecting a highly secure data center that hosts web applications, an application proxy might be more appropriate.

Firewall Deployment Techniques

You can deploy firewalls in several ways on a network. This section will cover three of the most common firewall deployment techniques—border firewalls, screened subnet (or DMZ) firewalls, and multilayered firewalls. Depending on an organization's security needs, one or more of these approaches may be a good fit.

Border Firewall.

The **border firewall** is the most basic approach. These firewalls simply separate the protected network from the Internet, as shown in **FIGURE 5-9**; they normally sit behind the router and receive all communications passing from the router into the private network as well as all communications passing from the private network to the Internet. Border firewalls normally use either packet filtering or stateful inspection.



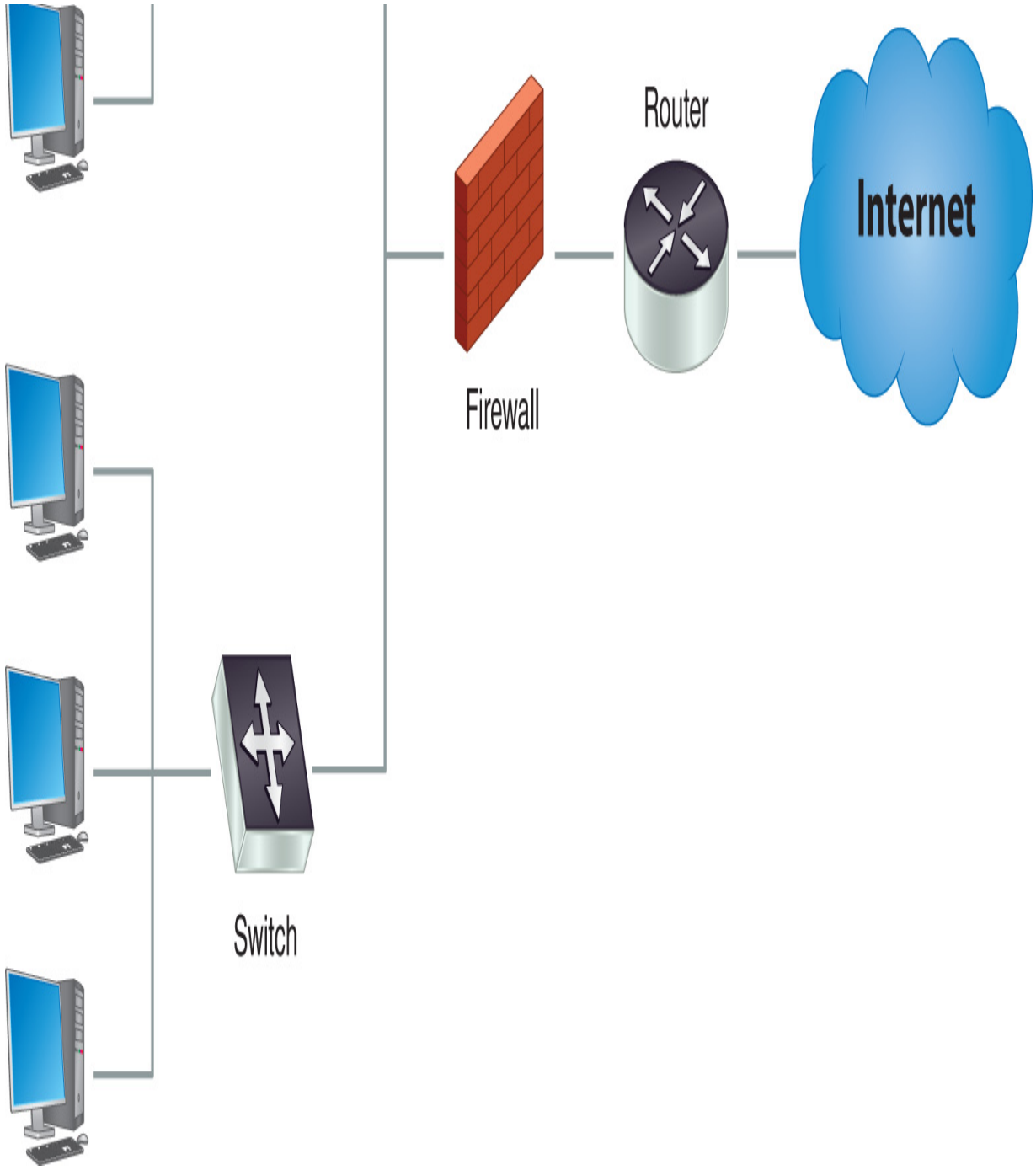


FIGURE 5-9 A border firewall.

Border firewalls are most common for organizations that do not host public services. If an organization outsources its website and email and does not provide any Internet-facing services, it might not need to allow the public access to the network at all. In this case, simply blocking most (or sometimes

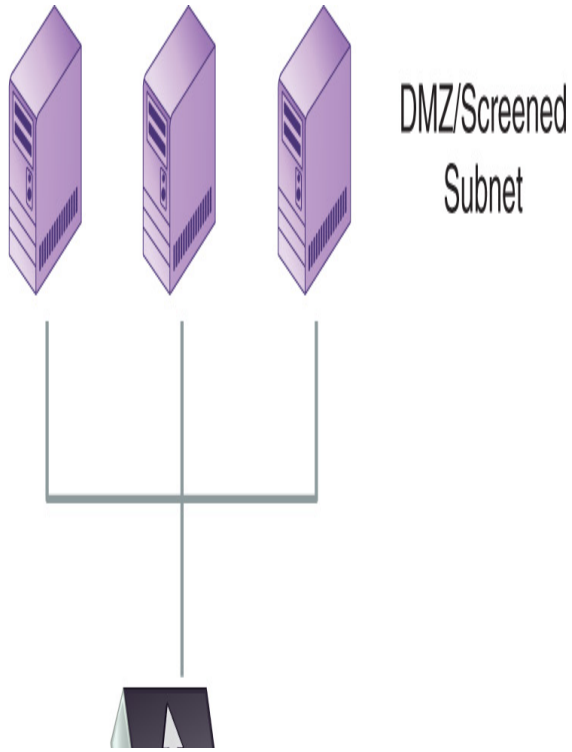
all) inbound traffic is all that is necessary, and a border firewall excels in this scenario.

Screened Subnet.

Often, it's not possible to block all traffic into a network, such as when an organization hosts a public website or its own email server, thus making it necessary to allow inbound connections on a limited basis. The screened subnet firewall topology, shown in **FIGURE 5-10**, is the best approach for this type of requirement. This firewall has three network interfaces. Two are set up identically to a border firewall, with one of them connected to the Internet and the other connected to the private network. The third interface connects to a special network known as the screened subnet, or **demilitarized zone (DMZ)**.

NOTE

The screened subnet is the most common firewall topology in use today.



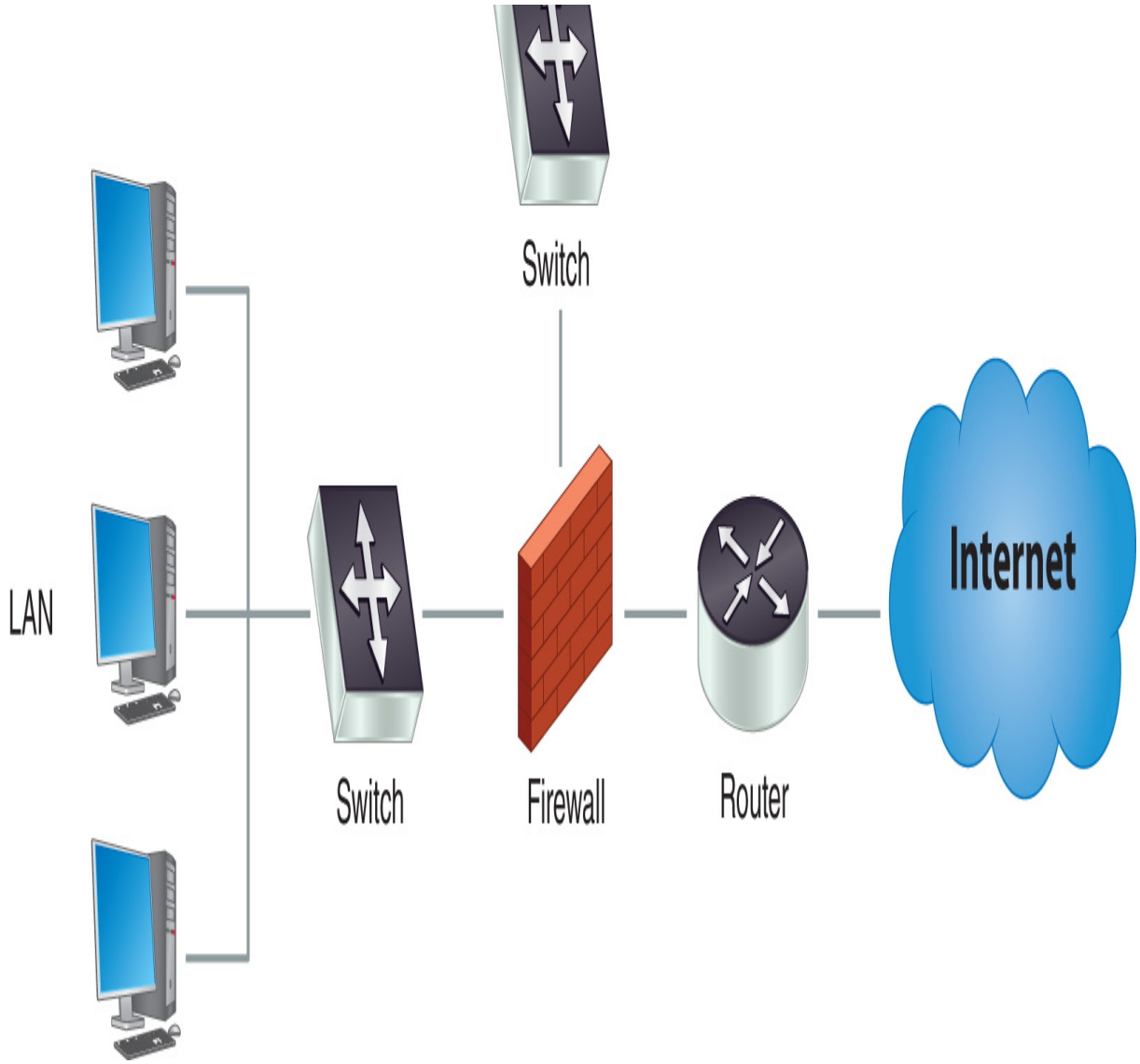


FIGURE 5-10 A screened subnet firewall.

The DMZ is a semiprivate network used to host services that the public can access. Thus, users are allowed limited access from the Internet to systems in the DMZ but are blocked from gaining direct access from the Internet to the private network by a secure network.

This approach recognizes that systems accessed from the Internet pose a special risk because they are more likely to be targets of attacks and, therefore, more likely to suffer successful ones. If these machines are confined to the DMZ, then the only other systems they can jeopardize are those also in the DMZ. Therefore, an attacker who gains access to a DMZ

system will not be able to use that system to directly access systems on the private network.

Multilayered Firewalls.

In large and/or highly secure environments, organizations often use multiple firewalls to segment their network into pieces. This is the case illustrated in Figure 5-8, which shows that one firewall acts as the border firewall, protecting subnets A, B, and C from the Internet, and the other two firewalls separate subnets B and C from each other and from subnet A.

Multilayered firewalls are useful when networks have different security levels. For example, referring to Figure 5-8, general users may connect to subnet A, users working on a secret research project might connect to subnet B, and executives might connect to subnet C. This structure provides the secret project and the executives with protection from the general user community.

Unified Threat Management.

Firewalls are so important to network security that they have matured into devices that do far more than just inspect packets. In fact, multipurpose firewalls are more commonly referred to as unified threat management (UTM) devices. These devices do provide filtering as well as many other security services, some of which follow:

- **URL filter**—This feature filters web traffic by examining the Uniform Resource Locator (URL) as opposed to the IP address.
- **Content inspection**—The device looks at some or all network packet content to determine whether the packet should be allowed to pass. This type of inspection can help identify malicious content from trusted sources, which could happen if a trusted source is compromised.
- **Malware inspection**—Providing a specialized form of content inspection, the device looks at packet content for signs of malware.

These unified services make it possible to reduce the number of devices that must analyze network packets. Fewer UTM devices can provide the same level of security as many older devices. However, even with fewer devices inspecting packets, introducing UTM devices can slow down a network

because of the sheer amount of work the devices must accomplish. It takes time to inspect and analyze each network packet at multiple layers of the network stack. For this reason, some organizations have elected a "middle-of-the-road" approach, such as implementing a web security gateway, which performs URL filtering but does not examine the content of the packets and therefore accomplishes some of what a UTM device does but without all the overhead.

NOTE

Another useful feature of firewalls is that they can be configured as load balancers, which can dynamically route network traffic to different network segments to avoid congestion. They do this by monitoring known network segments and directing traffic onto a segment that is appropriate for the destination host and has the necessary bandwidth, a process that can keep networks from slowing down when the demand is high.

Virtual Private Networks and Remote Access

With the advent of telecommuting, remote access has become a common part of many corporate networks. When the COVID-19 pandemic hit, the migration toward support for a remote workforce had already begun, and the pandemic simply accelerated support for remote and distributed workers to keep business functions from completely stopping. Today, many companies have employees who rarely if ever come into the corporate office, instead working at home or on the road. Even so, they still need access to corporate resources, which means opening access to more corporate resources from the Internet than IT professionals are comfortable with. The trick is to allow corporate personnel the access they need but to keep attackers out of these potentially open doors.

Virtual private networks (VPNs) are an effective way to increase the security level of data that is transmitted across a public data network by using encryption to protect all the data sent between a user and the

organization's network. The cost difference between using a VPN and paying for a dedicated connection between two sites is significant. Therefore, using a VPN for remote access not only provides security but is also cost effective. **FIGURE 5-11** shows an example of VPN access to a network.

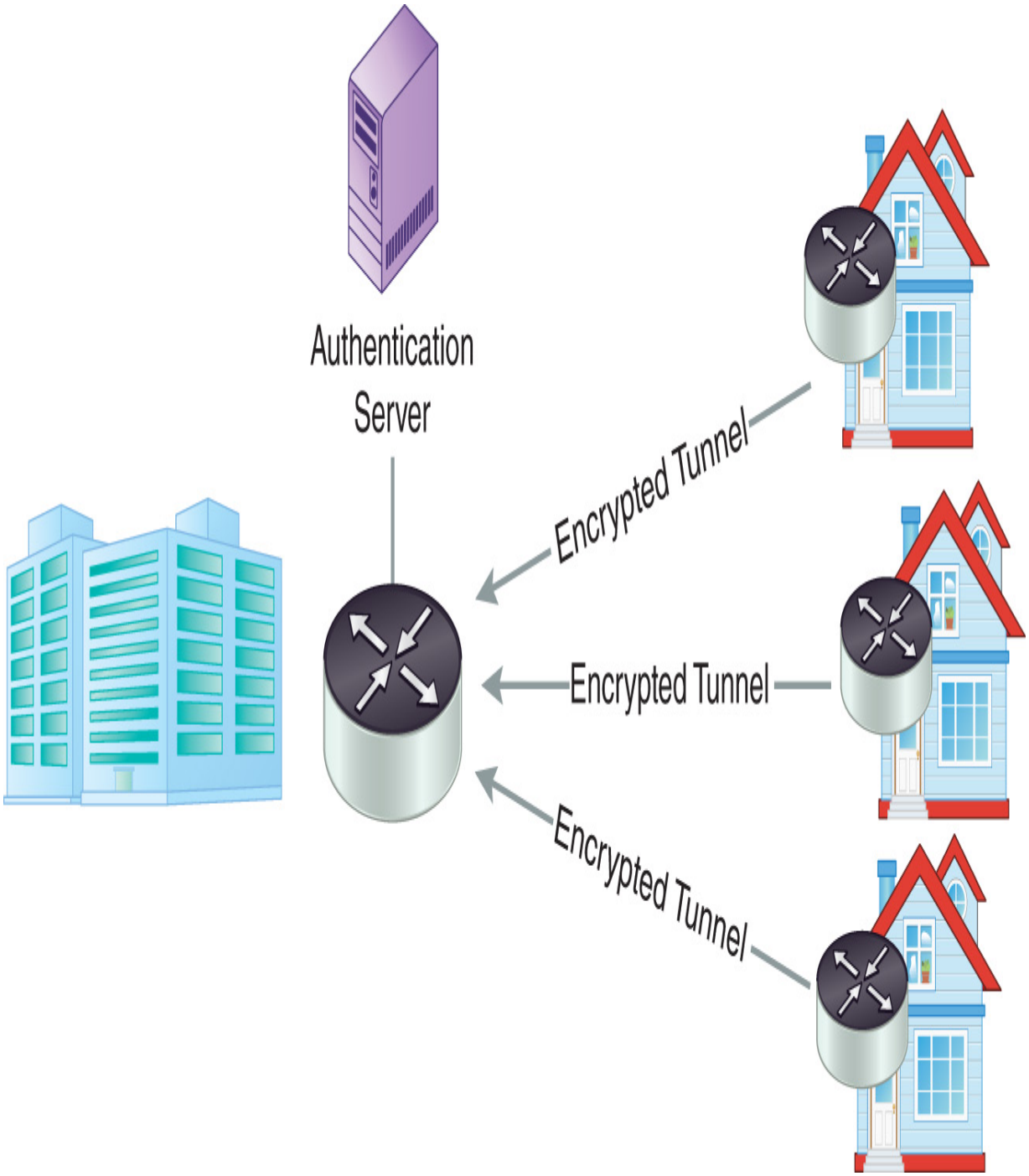


FIGURE 5-11 VPN access.

VPNs require gateway equipment with high processing power to handle the encryption algorithms. You can offload this processing power to another device by using a dedicated VPN concentrator rather than having the router or firewall terminate the VPN.

In deploying a VPN, the security of the end users' computers must be considered because, once users connect to the corporate network, their computers could be open portals into those resources for an attacker who gains access to them. For this reason, many organizations require that employees install security software on their home computers as well as limiting VPN access to laptop computers that the organization owns and manages.

Following are the major VPN technologies in use today:

- **Point-to-Point Tunneling Protocol (PPTP)**—The PPTP was once the predominant VPN protocol and almost all VPNs used it. It is easy to set up on client computers because most operating systems include PPTP support.
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)**—The **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)** protocol encrypts web communications, and many VPNs use it. Users connect to an SSL/TLS-protected webpage and log on. Their web browser then downloads software that connects them to the VPN. This setup requires no advance configuration of the system. For this reason, SSL/TLS VPNs are quickly growing in popularity.
- **Secure Socket Tunneling Protocol (SSTP)**—Microsoft's SSTP is available only for the Windows operating system. This protocol is a more modern approach to VPNs that route traffic over SSL, which makes it easy to set up VPN connections that can go through firewalls and proxy servers.
- **Internet Protocol Security (IPSec)**—**Internet Protocol Security (IPSec)** is a suite of protocols designed to securely connect sites. Although some IPSec VPNs are available for end users, they often require the installation of third-party software on the user's system and, therefore, are not popular. The required IPSec VPN functionality is built into many routers and firewalls, allowing for easy configuration.

- **OpenVPN**—OpenVPN is an open source VPN protocol that is available for most current operating systems. It uses SSL/TLS for its preshared key exchange process and then sets up a tunnel for communication. Two versions are available, OpenVPN TCP and OpenVPN UDP, to support the two most common transport protocols.

VPNs provide clear benefits to an organization by offering an inexpensive, secure replacement for dedicated connections between sites and enabling users to connect securely to the organization's network from remote locations. Being able to securely connect from remote locations promises increased productivity because workers can easily get to resources they need while on the road.

Network Access Control

Network access control (NAC) systems enable you to add more security requirements before allowing a device to connect to a network. These systems perform two major tasks—authentication and posture checking—and work on both wired and wireless networks. Although NAC is a new technology, it is growing in popularity, and many organizations now deploy NAC for both internal users and guests using their network.

The IEEE 802.1x, commonly referred to as simply 802.1x or 1x, standard governs how clients, through the authentication component of NAC, may interact with a NAC device to gain entry to the network. The authentication process involves software on users' computers that prompts them to log on to the network. After verifying the users' credentials, the NAC device then instructs the switch (for a wired network) or access point (for a wireless network) to grant the user access to the network.

Posture checking is an optional second use of NAC technology. When posture checking is used, the NAC device checks the configuration of the user's computer to ensure that it meets security standards before allowing it access to the network. Following are some things commonly checked:

- Up-to-date antivirus software
- Host firewall enabled
- Operating system supported

- Operating system patched

If a user attempts to connect a noncompliant system to a network, the NAC device offers two options: either the administrator can decide to block such systems from the network until they are fixed, or the system can connect to a special quarantine network where it can be fixed before gaining access to the main network. One of the most common protocols that NAC devices use to authenticate devices is the **Extensible Authentication Protocol (EAP)**. EAP is an authentication framework, not a specific protocol implementation, that defines the transport of keys and authentication credentials used by other protocols, such as wireless network authentication, and exists in several variations. Such variations include EAP Flexible Authentication via Secure Tunneling (EAP-FAST), which is an EAP extension that sets up a secure tunnel to protect the authentication process; EAP Transport Layer Security (EAP-TLS), which uses TLS to secure authentication credentials; EAP Tunneled Transport Layer Security (EAP-TTLS), which extends TLS to create a tunnel for authentication; and the Protected Extensible Authentication Protocol (PEAP), which is basically EAP running in a TLS tunnel but providing more security than EAP for authentication exchanges.

Voice and Video in an IP Network

Historically, homes and businesses communicated with the rest of the world using telephone lines, the endpoints of which could be standard telephones, fax machines, modems to support computer communications, and voice/video devices for multimedia communication. Regardless of the endpoint device being used, the device would connect to the public switched telephone network to communicate with some remote endpoint. Security primarily consisted of stopping attackers from making calls without paying for them or severing connections. Because all telephone line connections were leased from a communication company, attackers making unauthorized calls could cost an organization large amounts of money.

As LANs and the Internet became more commonplace, organizations began to replace traditional phone systems with devices that use IP networks to communicate. Many of today's businesses use their IP networks for voice and video calls, the cost of which can be reduced by replacing traditional phone

lines with Voice over IP (VoIP) software and services. Though VoIP is not free, it can be far less costly than leasing traditional phone lines.

The Session Initiation Protocol (SIP) establishes and manages connections between endpoints by setting the stage for a connection that VoIP or other media-related protocols can use to support audio and video calls. Although using an existing network for SIP/VoIP traffic can reduce phone line costs, doing so has several drawbacks: increases in traffic, service costs, and risk. Adding voice and video to an existing network increases that network's usage and can cause performance problems if the available bandwidth is insufficient to handle the traffic; implementing SIP/VoIP likely requires software and agreements with external service providers to carry the content outside the local environment and interface with the traditional telephone system; and, finally, SIP/VoIP traffic is subject to the same network attacks as any other network traffic.

Securing voice and video communications is essentially just like securing any other network traffic. However, there are a few steps that each organization should take to keep SIP/VoIP communications secure. Following are some of the best practices for securing SIP/VoIP:

- Patch all SIP/VoIP software and network component firmware.
- Use VLANs to separate voice and video from other network use (i.e., workstations and printers).
- Enforce encrypted VPN use for all remote access (including SIP/VoIP).
- Require end-to-end encryption for all voice or video calls using TLS or Secure Real-Time Transport Protocol (SRTP).
- Enforce strong authentication for all network users.
- Use firewalls to protect all SIP/VoIP devices and services.
- Harden all SIP/VoIP devices and software.

Wireless Networks

Wireless networks have become very popular for connecting devices within the home and office, such as laptops; desktops; smartphones; and many other devices, including the growing number of Internet of Things (IoT) devices. Wireless networking allows users to work from any location in the building without worrying about finding a place to plug in a network cable.

Configuring a wireless network is quite easy and inexpensive. The question becomes, what does wireless technology do to the security of the network? If it is so easy for personnel to connect to the network, does that mean that others can connect as well?

Setting up a secure wireless network—at least one as secure as any wired network—is possible with properly configured strong encryption. However, it takes careful planning, execution, and testing. This section covers wireless networking technology and how to configure and secure wireless networks.

Wireless Access Points

A **wireless access point (WAP)** is a radio, sending and receiving networking information over the air between wireless devices and the wired network. Anyone with a wireless device who is within radio range of a WAP can communicate with and attempt to connect to the network via the device.

Attackers who want to undermine the security of a wireless network understand that wireless networks extend the range of an organization's network beyond its walls. While you can easily control physical access to a wired network, walls and fences do not stop wireless signals. Therefore, wireless networks without proper security present an easy target for attackers who want to connect to them. Moreover, attackers know that it is much easier to eavesdrop on a wireless than a wired network. Anyone within radio range of a network can easily capture all the data sent on that network, and, if the data is unencrypted, that organization is fair game for an attack.

Wireless Network Security Controls

Fortunately, you can do quite a bit to secure a wireless network with wireless network security controls, which are the subject of this section. The most important security control is wireless encryption to prevent eavesdropping. Other techniques that provide added security include disabling service set identifier (SSID) broadcasting, implementing **MAC address filtering**, and adding strong authentication to the wireless network.

VPN over Wireless

One of the most secure ways to implement secure wireless networks is to use VPNs for all wireless connections. Access to a VPN for internal users is easy to manage, whereas guest access is more difficult. One common solution is to create at least two separate wireless networks—one network for internal users who require VPN access and greater connectivity into the internal network and one network for guests that does not allow VPN access and has very limited connectivity to the internal network.

Wireless Encryption

Encryption is the single most important thing you can do to secure a wireless network because encryption makes an outsider's viewing information traveling over that network impossible, whereas, without encryption, all wireless users' activities are visible to anyone who comes within radio range of the network. Without encryption, an attacker could, with an inexpensive antenna attached to a standard laptop, sit in the parking lot of an organization's building and monitor everything happening on its wireless network.

Another consideration in using encryption is that it must be strong, unlike the basic encryption provided by the **Wired Equivalent Privacy (WEP)** standard, which was developed in the early days of wireless networking. WEP relies on the RC4 encryption algorithm, which was created by Ron Rivest for RSA in the late 1980s. Since its release, security analysts have discovered that it has significant flaws that make it insecure. With software freely available on the Internet, it is simple to break the encryption on a WEP network in a matter of seconds. In fact, using WEP on a wireless network is probably worse than using no encryption at all because it provides a false sense of security. People feel they are safe because their wireless network

encrypts traffic. What they do not realize is that they're using the equivalent of a Cap'n Crunch® decoder ring to protect their data.

LEAP and PEAP

To help manage wireless keys and authentication, Cisco Systems developed the Lightweight Extensible Authentication Protocol (LEAP), which could use either WEP or Temporal Key Integrity Protocol (TKIP) for setting up secure connections. Because WEP weaknesses were well known, TKIP emerged as a stopgap substitute for WEP that would operate on existing hardware that supported only WEP.

Later, Cisco, Microsoft, and RSA joined together to address LEAP's weaknesses, and from that collaboration came the Protected Extensible Authentication Protocol (PEAP), which differs from LEAP in that it does require a certificate on the server.

Fortunately, several alternatives were developed to address WEP's weaknesses. One of these alternatives is the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is an encryption protocol that implements the IEEE 802.11i standard and provides enhanced security using the Counter Mode of the Advanced Encryption Standard (AES). In addition to CCMP, the **Wi-Fi Protected Access (WPA)** standard, which became available in 2003, uses strong AES encryption to protect data on networks and does not have the same vulnerabilities that were discovered in WEP. WPA refers to the draft of the IEEE 802.11i security standard, which was intended to be an intermediate solution to WEP's vulnerabilities. To take the place of the temporary WPA, a more secure standard, WPA2 (official name 802.11i-2004), was made available in 2004, followed in 2018 by the latest and most secure standard, WPA3. WPA3 can operate in WPA-Enterprise mode, using AES-256 in GCM mode, and WPA3-Personal mode, using AES-128 in CCM mode. As of July 2020, WPA3 is mandatory for new Wi-Fi device certifications issued by the Wi-Fi Alliance.

All three standards, WPA, WPA2, and WPA3, are easy to configure. In their basic form, they require entering a shared secret key into the network

configuration of every computer on the network. In more advanced forms, you can replace the shared secret key by giving each user a unique username and password, which can be identical to the user's normal credentials by using a central authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS was introduced in 1991 and quickly became a popular protocol used for managing remote user connections because it provides a central method to manage authorization, authentication, and accounting (AAA) services. DIAMETER, its successor, was introduced in 1998 and has recently become more popular than RADIUS for handling wireless remote connections because it has the ability to address more mobility issues. For example, DIAMETER includes better roaming support and can use TCP or Stream Control Transmission Protocol (SCTP).

TIP

Disabling SSID broadcast provides a small degree of protection, but this technique is not foolproof. In fact, a skilled attacker can easily discover the presence of a network by using freely available software tools. Using this technique simply means you do not advertise the presence of the network, hoping to avoid the casual attacker's interest.

SSID Broadcast

By default, wireless networks broadcast their presence to the public by sending out announcements containing the network's SSID, which is the network's public name. For instance, when you boot up in a coffee shop with Wi-Fi, your computer shows you a list of the available wireless networks along with their SSIDs.

You can stop a network from announcing itself by disabling SSID broadcast on the wireless access points. If you disable SSID broadcast, users wanting to connect to that network will need to know it is there and provide its name themselves. Using this technique is fine if only regular users connect to the network, such as in a corporate environment, but will not work well if guests are allowed to access the network.

MAC Address Filtering

WAPs also enable the application of MAC address filters to control which computers can connect to a network. With this technology, the WAP is provided with a list of acceptable MAC addresses, which means that only approved computers are allowed access to connect to the network.

The major disadvantage of MAC address filtering is that it is very complicated to maintain, which limits its usefulness to no more than a handful of computers on the network. More than that, and it quickly becomes a major challenge to update the list of acceptable MAC addresses. As an example, imagine if you worked for an organization with 20,000 users. In such an organization, it would not be unusual to see 100 new computers on the network every week in addition to 100 dropping off the network as you replace them. Can you imagine trying to update 200 MAC addresses every week? Use MAC address filtering in cases where it makes sense.

Additional Wireless Security Techniques

In addition to the preceding suggestions, selecting the right hardware and placing that hardware in the right position can have a noticeable impact on a network's security. In particular, pay attention to these aspects of wireless hardware management:

- **Antenna types**—Wireless device antennas can have a large impact on the device's area of coverage and how it transmits and receives, so choosing the right antenna, based on an organization's use, is important. Generally, external antennas can reach farther than internal antennas, and all antennas can be omnidirectional (all directions), semidirectional (limited direction), or highly directional (focused direction).
- **Antenna placement**—Where antennas are placed determines who has access to the wireless network. For example, placing an omnidirectional antenna near an external wall will likely make the wireless network available to people outside the building.
- **Power-level controls**—The power a wireless device uses can be changed from the configuration settings. Lowering the power settings from the default will reduce the area the device covers, which can be helpful when attempting to limit the visibility of wireless networks.

- **Captive portals**—A captive portal is a webpage to which all new connections are directed until the connection is authenticated. The most common use of a captive portal is to provide a logon page for wireless networks.
- **Site surveys**—One of the most important nontechnical aspects to securing wireless networks is to survey the site, which includes examining the physical area the wireless network will serve. Using facility floor plans can help determine the best placement for wireless devices before they are physically placed.

Although no network is totally secure, the best way to make an IT infrastructure as secure as possible is to ensure that an attacker must compromise several controls to get to the data, and that means putting the right security controls in place. Always assume that a savvy attacker will be able to compromise one or more of the controls that are in place, which makes it necessary to never rely on a single control and to always use layered controls.

 **WARNING**

MAC address filtering is another weak security mechanism. In a type of address spoofing, using free tools, attackers can easily discover an active MAC address on a network and then change their network interface to use the discovered valid MAC address.

CHAPTER SUMMARY

In this chapter, you learned about the Open Systems Interconnection (OSI) Reference Model and how it serves as an example of how you can build and use a network and its resources. You learned about Network Layer protocols, including an overview of TCP/IP, as well as some basic tools for network security. Finally, you learned how wireless networks work and what threats they pose to the security of an organization.