Introduction to Networking

Just about any computer you'll use today is on a network. Networked computers are so common it's easy to take them for granted. However, many components and technologies are working together behind the scenes to ensure a networked computer can access resources on the network.

In this chapter, I start by identifying the names of many of the physical and logical components of a network. I then introduce the components included in very small networks and show you how additional components are added as a network grows. I conclude with information on some standards organizations that help ensure all of these computers can work together no matter who manufactured them or where they're operating.

- **Comparing logical and physical networks**
- **Networking home computers**
- **Networking small offices and home offices**
- **Networking large offices**
- **Networking enterprises**
- **Understanding standards organizations**

Comparing Logical and Physical Networks

A network is a group of computers and other devices connected together. These connections can be with cables, wireless connections, or both. Networks are discussed in both logical and physical terms.

The *logical* organization of a network identifies the overall design of a network. It differentiates between local area networks (LANs) and wide area networks (WANs). The logical design of the network provides a high-level overview of the entire network and may not show smaller components such as all the switches, routers, and firewalls. By contrast, the *physical* network infrastructure includes the details of the physical components. The physical components are the devices and cabling that you can touch and feel.

This chapter presents concepts on logical network organization. You'll learn about the different types of network designs that you may find in home networks, small offices, larger offices or organizations, and enterprises.

Chapter 2 provides an overview of these physical components, and later chapters in the book (such as Chapters 7, 8, and 9) dig deeper into how these devices work.

It's important to understand how devices in a logical structure work to fully understand how data moves through a network. Once you understand how the data moves through the network, you are better prepared to maintain it and troubleshoot it when problems occur.

Networking Home Computers

Most home computers are part of a network today. At the very least, home computers have the ability to connect to the Internet, which is a massive network of networks. Figure 1.1 shows a simple networked home computer.

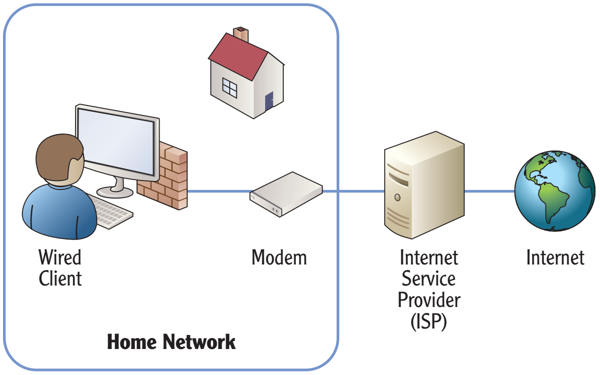

FIGURE 1.1 Home computer with access to Internet

In the figure, the computer has access to the Internet through a modem to an Internet service provider (ISP). This could be a cable modem used in a broadband connection or a modem used for dial-up connections. Broadband connections are widely available in urban areas. This includes connections through cable TV systems, fiber-optic lines, and even phone connections such as ISDN and 3G/4G data services.

Even if a broadband connection isn't available, home users can connect to the Internet through a phone line, also known as a dial-up system. Dial-up connections are much slower but are used in rural areas where broadband connections are not available. Internet access via satellites is becoming available in more rural areas, providing better connections than dial-up but still not comparable in speed to broadband connections.

Enable the Local Firewall

When a computer connects directly to the Internet through an ISP (without going through an internal router or wireless access point), it is at significant risk. The computer has a public IP address and is accessible from any other computer on the Internet, anywhere in the world. Attackers often prowl the Internet looking for unprotected computers. Enabling the software firewall on this computer provides a layer of protection.

When home users add additional computers into their home, they typically want to network these computers. Users on the network are then able to share resources. For example, consider Figure 1.2, which shows a typical home network connected to each other and the Internet using both wired and wireless connections.

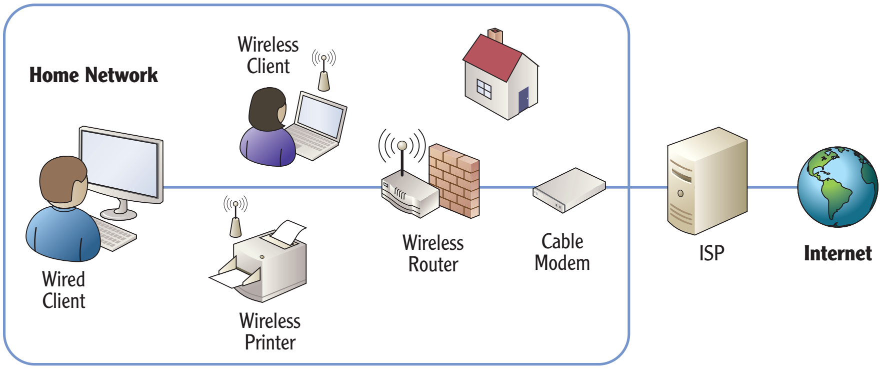

FIGURE 1.2 Typical home network

In the figure, the wired user is connected to a wireless router directly with a cable, and another user is connected via a wireless connection. A wireless printer is added that can be shared by any users with access to the wired network. An

ISP provides connectivity to the Internet, just as it would for a single user. A single cable modem connects to the ISP, and then the cable modem connects to a wireless router.

Some ISPs provide a router instead of a cable modem. A wireless router can connect to a router just as easily as it can connect to a cable modem.

Without a network, each individual computer would need to connect to the Internet separately, incurring individual access charges. However, the single Internet connection can be shared by adding the wireless router. A great benefit of wireless is that you don't have to install cables to each computer.

Most wireless routers include several additional capabilities. For example, it's common for a wireless router used in most home networks to include the following:

Wireless Access Point (WAP) The core purpose of the wireless device is to support connectivity for wireless clients. The WAP provides this connectivity.

Routing Capabilities A built-in router will route data from the internal network to the Internet and from Internet data back to the internal network. Chapter 2 provides an overview of routers, and Chapter 9 includes in-depth details on routers.

Chapter 9 covers routers and NAT in more depth.

Network Address Translation (NAT) NAT translates the public IP addresses used on the Internet to private IP addresses on the internal network, and vice versa. If NAT wasn't used, you'd have to purchase or lease public IP addresses for each internal computer. Additionally, each computer would be directly on the Internet and exposed to unnecessary risks. NAT hides the internal computers from Internet attackers.

Chapter 5 covers DHCP and IP addressing schemes.

Dynamic Host Configuration Protocol (DHCP) DHCP provides clients with IP addresses and other TCP/IP configuration information. The other TCP/IP information includes the address of the DNS server and the address of the router that provides a path to the Internet. The router address is also known as the *default gateway*.

Chapter 11 covers more advanced configurations of the firewall. Chapter 12 includes important wireless security concepts.

Firewall A WAP will provide basic firewall capabilities. This blocks unwanted traffic from the Internet, providing a layer of protection for internal clients.

Networking Small Offices and Home Offices

Small offices and home offices (SOHOs) are very similar to the sophisticated home network. They are both considered LANs. SOHOs have access to the Internet and can have either wireless clients, wired clients, or both. Figure 1.3 shows the configuration of sample SOHO network.

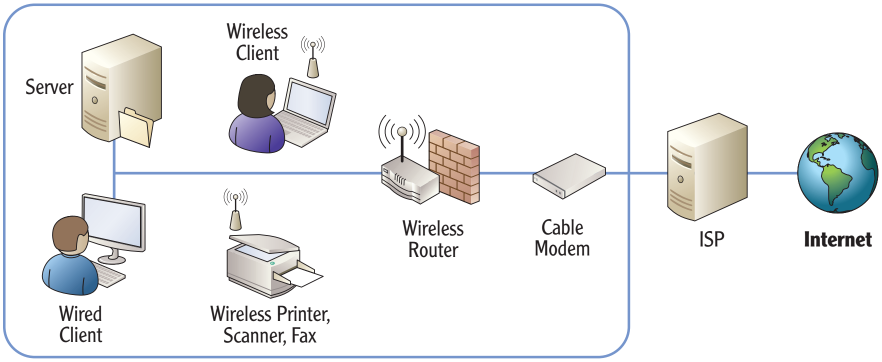

FIGURE 1.3 SOHO network

The primary difference is that a SOHO will typically have a server to provide additional capabilities for the office. For example, the server can be used as a file server to store files used within the business.

Although most offices will have a server, it's not necessary. Important files could be stored on a primary user's computer and shared to other users from there if needed. However, if important files are stored on multiple computers, it becomes harder to back up these files.

Additionally, a business may have a wireless multifunction printer that can print, scan, and fax documents to meet the needs of the business. It's not necessary to have a wireless printer. However, these are becoming more popular in SOHOs because they are easier to share between the network users.

The WAP used in a SOHO can be the same as the WAP used in the home network.

SOHOs typically have up to 10 workers but may have as many as 100.

Secure Wireless Networks

It's very important to lock down wireless networks with the best security available. The primary method of security for wireless networks is WPA2 (or 802.11i), which is discussed in greater depth in Chapter 12. If the network is not locked down, an attacker can use a simple laptop with a wireless NIC while driving by in a car to compromise it. This "war driving" technique allows an attacker to tap into the network and access the network's resources if the network isn't secured. Historically, wireless networks were notoriously insecure. However, technologies available today make it possible to provide sufficient security for most wireless networks.

Similarly, the WAP used in the SOHO will provide many of the same capabilities to the office as a WAP provides for a home network. This includes routing, NAT, DHCP, and a firewall.

Understanding Local Area Networks

A LAN is a group of computers in the same geographical location. It can include multiple subnetworks.

The home network shown earlier (in Figure 1.2) and the SOHO (shown in Figure 1.3) are both considered *local area networks*. A LAN is a group of computers and/or other devices that are connected in a single physical location (such as a home, office, or corporate building). LANs can be much bigger than the networks shown so far. As you go through the book, you'll see how many different devices are used within the LAN.

LANs have fast network connectivity between the different devices in the LAN. Common speeds of wired LANs today are 100 Mbps or 1000 Mbps (also called 1 Gbps) and 54 Mbps or 300 Mbps for wireless.

Megabit and Gigabit

LAN speeds identify how much data they can transfer. Mbps is short for megabit per second, and a megabit represents a million bits. A LAN with a speed of 100 Mbps can transfer data at a rate of 100 million bits per second. A gigabit LAN (1 Gbps or 1000 Mbps) transfers data at a rate of 1 billion bits per second.

Occasionally, data is measured in bytes instead of bits. A byte consists of 8 bits. When bytes are mentioned, a capital ***B*** is used. For example, a system may have 4 gigabytes (GB) of random access memory (RAM). This is commonly listed as 4 GB. It is not accurate to list this as 4 Gb (with a lowercase ***b***). Similarly, it not accurate to list a 100 Mbps LAN as 100 MBps (with a capital ***B***).

A LAN is an internal network. Most LANs will have connectivity to the Internet through a router or firewall, but the LAN itself is internal. Traffic back and forth through a firewall to the Internet is filtered for security purposes. However, traffic within the LAN itself is usually not filtered. The internal network is considered a high trust area, so any traffic on the network is allowed.

Comparing Workgroups and Domains

A SOHO will typically include from one to ten workers and will usually be configured as a *workgroup*. A workgroup is a group of networked computers that share a common workgroup name. The default name of a Microsoft workgroup is simply *Workgroup*, and all computers in the workgroup will share the same workgroup name. User accounts are located on each individual computer.

Consider Figure 1.4, which shows an office with four users. Each of the users has their own computer, and an additional server is available to them. For Sally to log onto her computer, she needs a computer account on her computer. However, this account won't work on Bob's, Alice's, or Joe's computers. If Sally needs to log onto any other computer in the workgroup, she must have a separate account on that computer.

Even though Internet access is not shown here, a SOHO configured as a workgroup will typically have Internet access. The focus here is the internal LAN.

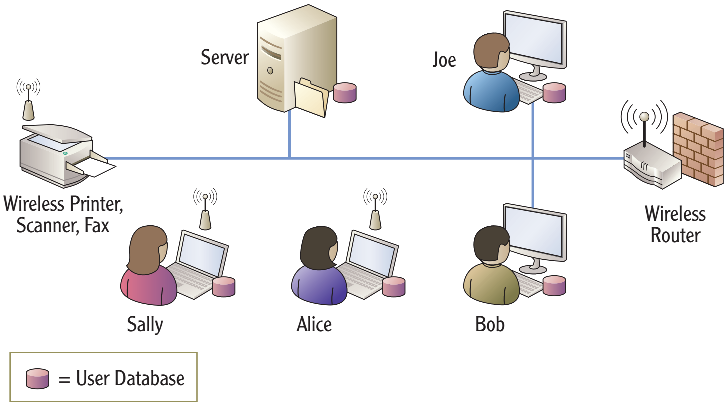

FIGURE 1.4 SOHO as a workgroup

In this scenario, there are five separate user databases—one on the server and one on each of the four computers. Similarly, each user would need to remember five usernames and five passwords to log onto each of the five computers.

However, most users in a SOHO will typically log onto only one computer in the network and will need only one user account. If users had to remember five usernames and five passwords, they would probably break a cardinal rule of security. They would probably start writing down the usernames and passwords.

When offices get larger than 10 computers or whenever offices need to have more centralized user and computer management, they move into a *domain* configuration. You can add a server and promote it to a domain controller or promote an existing server to a domain controller.

A Microsoft Windows domain includes a domain controller hosting AD DS.

In Microsoft domains, the domain controller hosts Active Directory Domain Services (AD DS). AD DS includes objects such as user and computer accounts. Each user would have one user account in the domain, and each computer would have one computer account.

Figure 1.5 shows a SOHO configured as a domain. It has eight users with nine computers connected to the LAN. The server has been promoted to a domain controller and is hosting Active Directory. Instead of requiring users to memorize passwords for each computer, each user has a single account hosted on the domain controller.

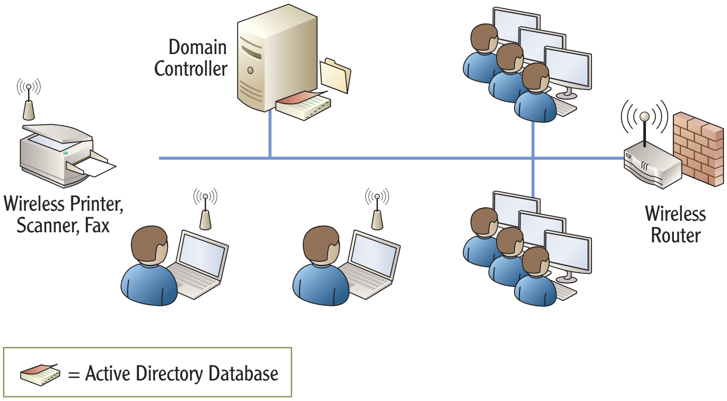

FIGURE 1.5 SOHO as a domain

This supports *single sign-on (SSO)* where a user needs to sign on only once. All access to domain resources for the user is granted using this single account. Additionally, this one account is used to log onto almost any computer in the domain.

By default, domain users are authorized to log onto any computer in the domain except for domain controllers. Administrators are granted the right to log onto domain controllers. However, it is possible to restrict users from logging onto other computers within the domain if necessary.

Even though the server has been promoted to a domain controller, it can still perform other functions on the network. For example, a domain controller can still host files as a file server.

When to Switch from a Workgroup to a Domain

There isn't a specific number defining when networks must change from a workgroup to a domain. It's based on preference and usability. However, most offices switch over when the number of users reaches between 10 and 20. Multiple reasons encourage the switch.

The primary reason to switch is when users have to remember multiple user accounts to perform their job. The domain provides single sign-on capabilities where users need to remember only a single user account to log on.

A secondary reason is to help administrators reduce their workload. A domain provides centralized administration through Active Directory. It also includes advanced administration tools such as Group Policy. Group Policy allows an administrator to configure a setting once in a domain and have it apply to many or all of the computers and users.

Another reason is to allow more concurrent connections from other devices on the LAN. In older operating systems such as Windows XP, each computer was restricted to only 10 concurrent connections. For example, if a computer shared a printer, only 10 other users could send print jobs to it at a time. The 11th connection was refused. This worked the same if a computer hosted a shared application. Ten users could connect, but the 11th connection was refused. This became a logical reason to switch to a domain when the office had more than 10 computers. Windows 7 Professional and Ultimate editions support 20 concurrent connections.

Exploring the Benefits of Domains and Domain Controllers

Promoting a server to a domain controller provides several benefits beyond single sign-on. These include the following:

Simplified Management Managing accounts in a domain is done with a group of centralized tools. For example, Active Directory Users and Computers is used to perform common administration tasks for all the users and computers in the domain. Additionally, user and computer accounts are organized in organizational units within the domain.

Group Policy Group Policy is used in a domain to configure, control, and manage users and computers. For example, Group Policy can be used to configure password-protected screen savers for all computers in the domain. An administrator can configure the setting one time in Group Policy, and the setting is configured on all the computers in the domain. It doesn't matter if the organization has 20 users or 20,000 users; the setting is configured once, and Group Policy does the rest. Thousands of settings can be configured through Group Policy.

Built-in Redundancy and Fault Tolerance If you have at least two domain controllers, the domain data is automatically replicated to each domain controller. If an account is added on one domain controller, it's copied to the other. If a user changes a password, the change is copied. This ensures you always have a redundant copy of Active Directory providing fault tolerance. In other words, if one domain controller develops a fault or fails, the domain can tolerate the fault. The other domain controller will carry the load.

Chapter 10 covers DNS and other name resolution methods.

Microsoft domains require a Domain Name System (DNS) server. DNS is used primarily to resolve computer names to IP addresses, but it's also used to locate domain controllers within a domain. If you don't have DNS or DNS fails, Active Directory fails.

Networking Large Offices

A *subnet* is a group of computers separated from other computers by one or more routers.

Large offices include more people, more end user computers, and more users. Although you can network thousands of people in a single LAN, you do have to take additional steps to improve the performance of the LAN. The primary difference is that you subdivide groups of computers into different *subnets*.

Figure 1.6 shows a diagram for a larger office. Notice that the office includes multiple subnets and each subnet is separated by a router. The computers are separated on the different subnets so that each subnet has less traffic. Notice that subnet A has only servers while other subnets have users. Placing the servers on separate subnets is common in larger networks.

Traffic on a network is similar to traffic on roads and highways. When there are fewer cars, traffic runs smoother. When there are more cars, traffic becomes congested, and the potential for collisions increases. You can improve traffic flow by adding more roads and highways, providing multiple paths to common destinations, and widening commonly used roads.

Similarly, more computers on a network results in more network traffic and more congestion. You can improve performance by adding subnets to control and limit traffic in different areas.

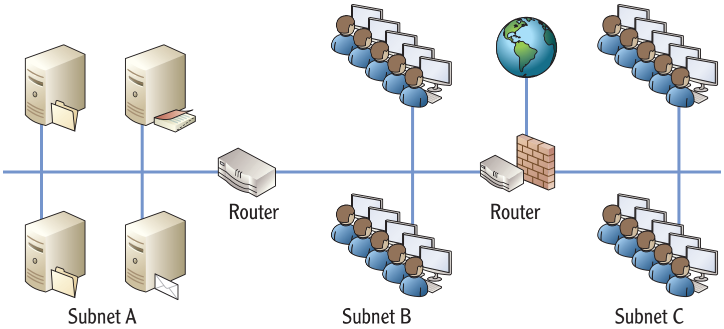

FIGURE 1.6 LAN for a large office

Just as cars can have collisions on a road, data packets sent on a network can collide, resulting in collisions. When two computers on the same subnet send data at the same time, the data collides and is unreadable. Both computers must then send the data again. They both wait a random amount of time and send the data again. If the network is very busy, the data can collide again when it's resent.

Of course, every time data has to be resent, it makes the network that much busier since there is more traffic. More traffic results in more collisions, and more collisions results in even more traffic. If the network isn't optimized, the network performance can slow to a crawl. This is similar to rush-hour traffic in a city where it may take you an hour to get somewhere that normally takes only 10 minutes.

Routers and Switches

Although Figure 1.6 shows how routers are used to subnet the LAN, the diagram doesn't fully show how computers are connected within each subnet. Switches or hubs connect computers to each other within a subnet. Routers connect the subnets together.

For example, all the servers in subnet A could be connected with a switch. Similarly, all the computers in subnet B could be connected with a second switch, and all the computers in subnet C could be connected with a third switch.

Switches are used to connect computers within a subnet. Routers are used to connect subnets. These two important points are repeated and expanded on throughout this book.

Networking Enterprises

There is no formal definition of an enterprise, but it generally implies an organization with multiple locations. Occasionally, documentation defines an enterprise as an organization with more than 250 users to differentiate it from a large office, while other documentation defines it as more than 5,000 users.

From an IT professional's perspective, the biggest difference between a large office and an enterprise is the number of IT professionals supporting the network. Some offices with as many as 50 users are supported by only one or two administrators. These administrators do a little of everything.

In contrast, an enterprise may have dozens of IT professionals, with many of them having specialized knowledge. Some may be experts on email systems such as Microsoft Exchange. Others may be experts on database systems such as Microsoft SQL Server. End user help-desk professionals are experts on Windows 7 and other desktop operating systems and provide direct support to the users.

While remote access technologies are more common in enterprises, they can be used anywhere, including SOHOs.

Another significant difference with enterprises is the method used to connect the different locations. Instead of just a single LAN in a single location, the organization is connected using different WAN technologies. WANs can be used to connect large offices to large offices. WANs can also connect smaller branch offices to the larger main offices.

Last, many workers are mobile. For example, salespeople are often traveling to meet customers. These mobile workers still need access to resources on the main network. Remote access technologies allow mobile workers to connect to the main network from remote locations.

Understanding Wide Area Networks

A LAN has one or more subnets in the same geographic location. A WAN is two or more LANS connected in different geographical locations.

A *WAN* is created when two or more LANs in separate geographical locations are connected. The connection between the LANs is almost always slower than the speed of the LANs themselves. For example, consider Figure 1.7. The organization headquarters has a high-speed 1000 Mbps (1 Gbps) LAN connecting all the computers and other devices. Similarly, the regional office also has a high-speed 100 Mbps LAN.

The T1 WAN link connects the two LANs at a much slower connection speed of 1.544 Mbps. Although a speed of 1.544 Mbps is much quicker than a dial-up speed of 56 Kbps, it is significantly slower than the internal speeds of the LANs (100 Mbps and 1 Gbps).

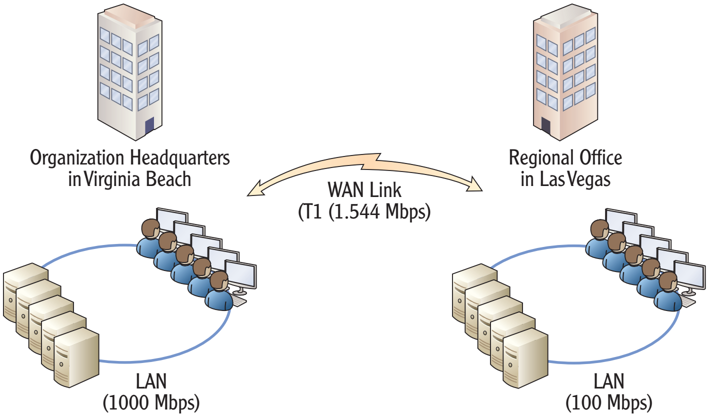
Organization Headquarters in Virginia Beach
WAN Link (T1 (1.544 Mbps)
Regional Office in Las Vegas
LAN (1000 Mbps)
LAN (100 Mbps)

FIGURE 1.7 WAN connecting two LANs

When a WAN is created, users are able to access resources in the other LAN. For example, users in the Virginia Beach LAN can access resources such as files on servers in the Las Vegas LAN. Similarly, users in Las Vegas can access servers in Virginia Beach.

Many organizations lease the WAN links they use. This is similar to people leasing phone lines for telephone access. It's not reasonable for phone users to run their own phone lines to everyone they want to call. Similarly, it's too expensive for most organizations to run their own cables to their different locations.

Leasing the lines from telecommunications companies can be expensive. These lines usually need to carry more data than a typical phone connection. For example, a regular phone connection can carry about 50 Kbps of data and may cost $30 to $50 a month. A T1 carries about 30 times that much data with a bandwidth of 1.544 Mbps. The cost isn't quite 30 times as much, but it often runs in the hundreds of dollars per month.

Other alternatives to leased lines include WAN DSL and WAN Ethernet. Chapter 13 covers the alternatives in more depth.

Understanding Branch Offices

Large organizations often have branch offices. This allows the organization to have a broader reach and allows their employees to be closer to their customers.

Branch offices are often much smaller than the main headquarters of the organization. They have fewer people and limited local computing resources. Individuals will have computers, but the branch office may not have any servers on site. However, employees still need to access organizational resources such as servers at the headquarters location. It's common for a branch office to be connected to either a headquarters or a regional office using a WAN link.

Consider Figure 1.8, which shows a branch office connected to the main headquarters of the organization and another branch office connected to the regional office. An organization can have as many branch offices as desired. However, each WAN link costs additional money.

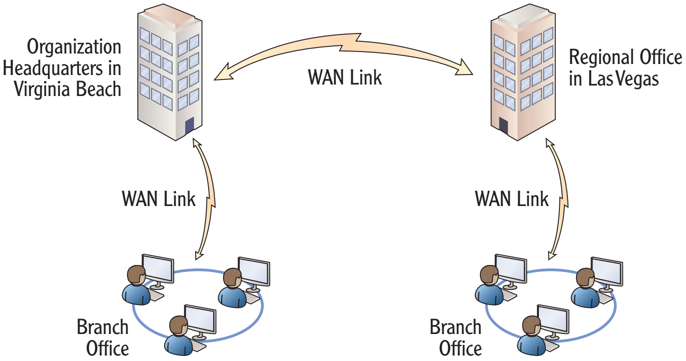
Organization Headquarters in Virginia Beach
WAN Link
Regional Office in Las Vegas
WAN Link
WAN Link
Branch Office
Branch Office

FIGURE 1.8 Branch offices connected in an organization

Since a branch office has fewer people, they have limited support. In other words, the headquarters' location will have many information technology (IT) professionals, but a branch office may not have any. Instead, the IT staff often provides remote support via the phone or using remote technologies.

Several remote assistance technologies are available to help users remotely. For example, Microsoft includes Remote Assistance. This allows administrators in one location to take control of the user's desktop (with the user's permission) to resolve a problem or show the user how to accomplish a task.

Accessing Networks Remotely

Many organizations also set up remote access capabilities. Remote access allows individuals working outside the company to be able to access resources internal to the company. These are the two primary methods of remote access:

Dial-up A client uses a modem and phone line to connect to a remote access server that also has a modem and a phone line. After authenticating with the server, the server provides connectivity to the internal network. A dial-up remote access server is accessible to any client that has access to phone lines. Figure 1.9 shows a dial-up connection.

Chapter 13 presents remote access services in more depth.

Virtual Private Network (VPN) A VPN provides access to an internal network over a public network such as the Internet. The client accesses the Internet using any available means. The client then connects to the VPN server, which is reachable through the Internet. After authenticating with the server, the VPN server provides connectivity to the internal network. The VPN server is accessible to any client that has access to the Internet. Figure 1.10 shows a VPN connection.

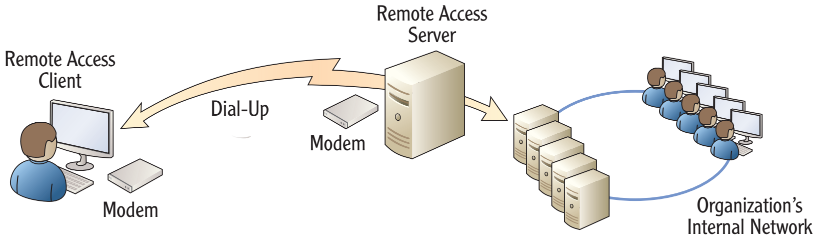

FIGURE 1.9 Remote access via dial-up

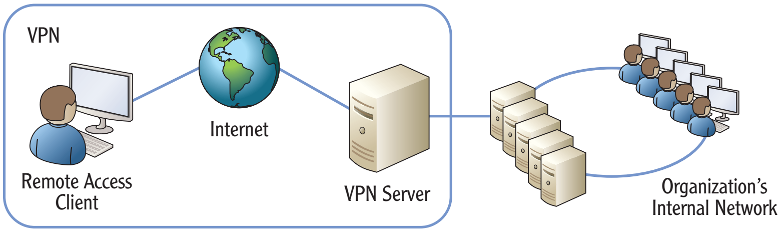

FIGURE 1.10 Remote access via VPN

Remote Access or VPN Server

The terms *remote access server* and *VPN server* have subtle differences. In short, a VPN server is a remote access server. However, not all remote access servers are VPN servers. Some remote access servers can use dial-up technologies only. If it's a remote access server using dial-up only, it's not correct to call it a VPN server.

Understanding Standards Organizations

Several standards organizations are important in networking, because they develop different types of standards to meet specific needs. For example, the IETF has created standards for the Internet communications. Without a central authority creating standards used by everyone, there is no way the Internet would be the valuable global resource it is today.

These organizations include the following:

- Internet Engineering Task Force
- World Wide Web Consortium
- Institute of Electrical and Electronics Engineers
- International Telecommunication Union

Understanding the Internet Engineering Task Force

The *Internet Engineering Task Force (IETF)* defines Internet communications standards. Its goal is to make the Internet work better. It does so by creating high-quality, relevant technical documents used by designers, managers, and users of the Internet.

Transmission Control Protocol/Internet Protocol (TCP/IP) is the protocol suite used on the Internet. It's also the primary protocol suite used within Microsoft networks. The IETF has produced a wide range of documents that define how the different protocols are used.

Chapter 3 introduces many of the protocols in the TCP/IP suite. Chapter 4 covers them in more depth.

Most documents created by the IETF are known as RFCs. *RFC* is short for *request for comments*. RFCs are written and then released to the world for comments. Many RFCs are assigned to the Standards Track category and go through a standards track. There are four primary stages for an RFC in the Standards Track category:

Proposed Standard (PS) An RFC starts at the PS stage, the first official stage where the standard is introduced. Many standards never progress beyond this level.

Draft Standard (DS) The second official stage is DS. At this stage, the standard has been tested and verified to work as expected. It is on the track to become an actual standard but isn't yet.

Standard (STD) The final stage of an RFC is STD. RFCs at this stage are widely used.

Best Current Practice (BCP) BCP is a single-stage alternative to the previous stages. A BCP provides operational specifications.

When an RFC is released, it is given a number. This number stays with the RFC, and the RFC is never changed once it's assigned a number. If a change is desired or required, a new RFC is created, and the new RFC starts over at the proposed standard stage.

Some RFCs are Informational or Experimental and do not follow the standard track stages.

As an example, RFC 791 describes the 32-bit IPv4. Even though this was created in 1981, it's still in use today. The IETF recognized that the Internet was running out of IPv4 addresses, so it tasked a working group with creating a solution. The working group first came up with RFC 1819 (commonly called the 64-bit IPv5). However, comments on RFC 1819 made it apparent that if 64-bits were used for IPv5, then the Internet would probably run out of IP addresses again in about 10 years or so. RFC 1819 was scrapped. The IETF ultimately released RFC 2460, defining 128-bit IPv6 addressing. RFC 2460 is on the standards track and currently has a status as a DS.

You can view the full RFC 2460 document at **`www.ietf.org/rfc/rfc2460.txt`**.

You'll read about many different protocols associated with TCP/IP throughout this book. Each of these protocols is defined in its own RFC.

For more information on the IETF, you can view its website at **`www.ietf.org`**. The IETF also has a page devoted to newcomers at **`www.ietf.org/newcomers.html`**.

Understanding the World Wide Web Consortium

The *World Wide Web Consortium (W3C)* defines standards for the World Wide Web (WWW). As an example, the Hypertext Transfer Protocol (HTTP) was defined by the W3C. HTTP is the primary protocol used to transfer WWW information over the Internet. Membership of the W3C consists of organizations rather than individuals. At the time of this writing, the W3C currently has 323 members.

Most web pages are created in a Hypertext Markup Language (HTML) format. It started as an Internet-based hypermedia initiative for global information and grew into what it is today. Tim Berners-Lee invented HTML and the World Wide Web. (His proper title is Sir Berners-Lee since he was knighted in 2004.) At the time of this writing, he is the director of the W3C.

Note that although the WWW runs on the Internet, it isn't the Internet itself. The Internet is a huge network of millions of networks and includes all the networking infrastructure hardware. The WWW is one of many methods used to access information over the Internet. The Internet also supports transferring files using the File Transfer Protocol (FTP) and sharing information through newsgroups, such as Usenet newsgroups.

Understanding the Institute of Electrical and Electronics Engineers

The *Institute of Electrical and Electronics Engineers (IEEE)* is a professional association dedicated to advancing technical innovation. It has more than 375,000 members in 160 different countries. A primary function of the IEEE is defining lower-level network standards.

IEEE standards are identified as IEEE (pronounced as I triple E) with a number. The IEEE has defined many different standards that you'll read about in this book. For example, IEEE 802.3 defines various standards for wired Ethernet networks. IEEE 802.11 defines various standards for wireless networks.

Understanding the International Telecommunication Union

The *International Telecommunication Union (ITU)* is a United Nations agency that includes members from 192 countries. It is focused on information and communication technology issues. It has contributed to shared global use of the radio spectrum and international cooperation in assigning satellite orbits. It has also helped improve telecommunication infrastructure throughout the world.

Many of the telephony standards used by computers today have been defined by the ITU. This includes standards used for modem communications and video conferencing.

The Essentials and Beyond

The logical network organization identifies the overall layout of LANs and WANs. A local area network is a group of computers and computing devices in a single high-speed layout. It can include one or more subnets. A wide area network is a group of two or more LANs connected with a slower WAN link. WAN links can also connect branch offices.

Additional Exercises

- If you are in a networked classroom environment, draw a diagram of the network. See whether you can identify the path to the Internet.
- If you have a home network, draw a diagram of it. Are computers connected with wires, or do they use a wireless access point? Does it have a dial-up or a broadband connection?

(Continues)

The Essentials and Beyond *(Continued)*

- Use the Internet to look up RFC 1918, which defines the private IP addresses used in internal networks. List the three private IP ranges defined by RFC 1918.
- Use the Internet to identify at least five different network standards in the IEEE 802 series (such as 802.3).

To compare your answers to the author's, please visit **`www.sybex.com/go/networkingessentials`**.

Review Questions

1. What should be enabled on a computer that has direct connection to the Internet?

   A. Router **C.** Firewall
   B. Switch **D.** VPN

2. True or false. A WAP often provides access to the Internet.

3. A group of computers are connected in a single location. What is this called?

   A. LAN **C.** VLAN
   B. WAN **D.** VPN

4. A network is connected using high-speed components rated at 1 Gbps. What does the *b* represent in Gbps?

5. Users in the network have to remember an average of five usernames and passwords to access different computers. How can you reduce the number of passwords remembered by users?

   A. Change the network to a workgroup **C.** Create a WAN
   B. Change the network to domain **D.** Create a VPN

6. Define a LAN.

7. Define a WAN.

8. An employee is able to connect to the employer's private network over the Internet. What is the employee using?

   A. Domain controller **C.** WAP
   B. LAN **D.** VPN

9. What are two types of remote access servers? (Choose two.)

   A. Dial-up **C.** VPN
   B. WAP **D.** Domain controller

10. True or false. All RFCs are known as standards.