chapter 11

Supporting a Small-Business Network

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

- Explain how to address the needs of a small business network
- Identify network equipment requirements for small businesses
- Identify requirements for small business applications
- Describe issues in supporting a small business

Once an overlooked sector of users of information technology, small businesses are spending on information technology at a rapid rate. In the United States, small businesses spent more than $230 billion on IT in 2008 and are expected to spend $280 billion on IT products and services in 2012. IT companies and publishers of IT books and certifications have often overlooked this large market. This chapter covers some technology issues small businesses face to give you more insight into addressing a small business's computer and networking needs.

Addressing the Needs of Small-Business Networks

What exactly is a small business? The U.S. government has, in typical fashion, multiple definitions, but a small business is often defined as one that's independently owned and operated, doesn't dominate its field of operation, and has revenues of less than $500,000 and/or fewer than 500 employees. For the purposes of this chapter, a small business can be defined as one with fewer than 200 computers, only one or two locations, and modest technology needs. Modest technology needs have been included as a characteristic because this chapter is geared toward the entrepreneur, consultant, or small computer company that can design, install, and support a small business network without having to become an expert in more advanced computing technologies, such as minicomputers and mainframes, complex WAN environments, and so forth.

Small businesses usually have more modest requirements of networks than large corporations do. Most want to share files and printers, have a networked application that applies to their business, and networked Internet access. Most small businesses don't require a complex, highly restrictive security policy, data encryption, or advanced WAN technologies. That being said, there are plenty of exceptions. You should be aware that one size doesn't fit all, and the most important factors in being successful in supporting small businesses are listening to their requirements and designing a solution that works for them. Small business owners can be a frugal bunch, and part of the challenge a network designer or installer faces is providing a solution that gets the job done at a reasonable price.

Data and Application Sharing in a Small Business

One of the first decisions to make before determining how to set up a data-sharing scheme is whether the network should be peer-to-peer or server based. When possible and when funds allow, a server solution is almost always the best way to go, particularly if you're supporting the network after it's installed. A peer-to-peer network is fraught with problems, particularly when a user untrained in managing a networked computer is left in control of a computer that's sharing resources. On a peer-to-peer network, users can shut down their computers, unknowingly severing other employees' access to shared files or printers, which can cause data loss and corruption. In addition, a user controlling a network resource might not understand the company's security policy or how to follow it and could make sensitive data available to unauthorized users. If you're forced to use a peer-to-peer scheme, you should limit the number of computers hosting network resources to minimize potential problems.

Whether you're using a server-based or peer-to-peer scheme, the simplest file-sharing solution is usually the best. Designate as few computers as possible as file-sharing computers. A common practice is for each user to have a home directory on the server, thereby making backups easier and giving each user a place to save most of his or her files. In Windows, this arrangement can be set up by using roaming profiles and folder redirection. Depending on the security policy, other users might have read access (but usually not write access) to each other's home directories to facilitate file sharing. If the policy is more stringent, users have access only to their own home directories, with select managers also having access as needed.

In addition to home directories, a typical practice is having one or more common folders that the entire company has access to or perhaps departmental folders shared among department members. Having common folders is a convenient way to distribute master documents without employees having to know which user maintains a document. When changes to a document are made, the document developer can post a new version in the common folder. In most OSs, permissions can be set on a single document so that the developer can allow only read access to it; in this way, a user can't change or delete the master document inadvertently. Users can copy the file to their own home directories and make changes to the copy, if necessary.

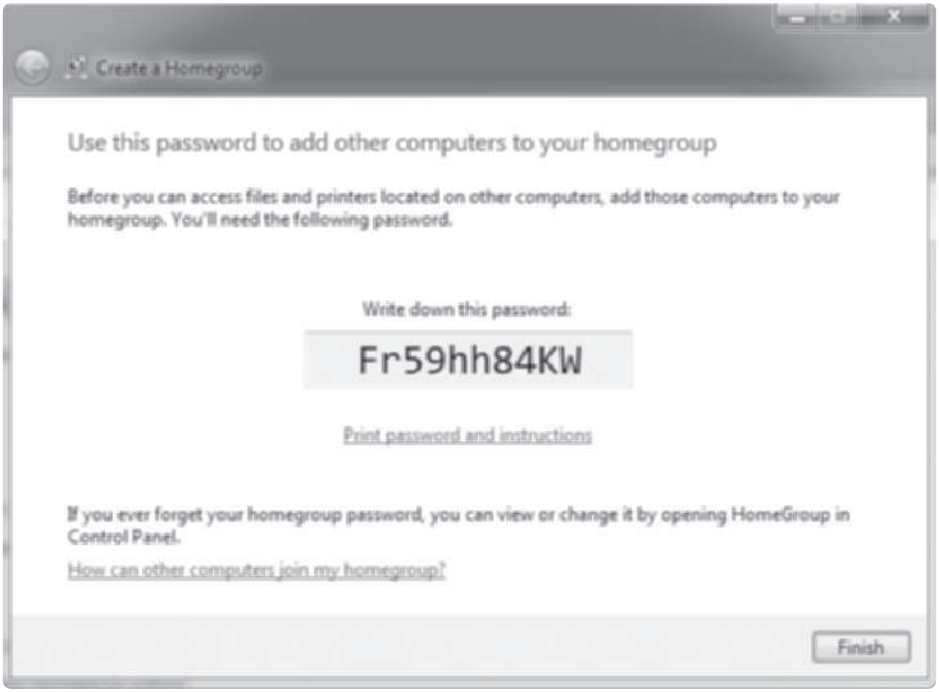
Applications can also be shared across a network. Many applications can be installed on a network file server and run from workstations via a shortcut installed on the desktop. Some applications have an installation program that creates a shortcut and sets up any Registry information the application requires, such as the location of data files. In other cases, an application allows sharing data across the network but must be installed in its entirety on each workstation running it. In either case, multiple computers having access to the same data is a big advantage compared with storing multiple sets of data or having only one computer with access to the application.

Configuring a Windows 7 HomeGroup Network Windows HomeGroups is a new peer-to-peer networking feature starting with Windows 7. A **homegroup** simplifies the process of sharing files and printers between multiple Windows 7 computers operating in a peer-to-peer network configuration. Be aware that the HomeGroups feature isn't backward-compatible with Windows Vista or XP; traditional file-sharing methods are required to share files in these OSs.

Homegroups simplify file and printer sharing by making it unnecessary to create user accounts on every computer that shares resources. In addition, configuring permissions and finding files on the network have been reduced to child's play. Homegroups are usually suitable only for small office/home office (SOHO) networks with fewer than 10 computers that operate under a fairly open security policy. For networks where homegroups are suitable, this feature might be just what small business owners have been looking for to simplify networks and increase productivity.

Creating and Joining a Homegroup The basic requirement for creating a homegroup is Windows 7 Home Premium, Ultimate, Professional, or Enterprise. Windows 7 Home Basic and Starter editions can join but not create a homegroup. Next, the network must be designated as a Home network rather than Work or Public. If you choose Home as your network location, you're prompted to create a homegroup. You can choose what type of files you want to share and whether you want to share printers. If your network is already designated as a Home network, you can create or join a homegroup by going to Control Panel and clicking "Choose homegroup and sharing options" under Network and Internet.

Homegroups are password-protected by a password that's generated randomly when the homegroup is created (see Figure 11-1). Users must enter this password when they join a homegroup. To view or change the password, open HomeGroup in Control Panel.



Use this password to add other computers to your homegroup

Before you can access files and printers located on other computers, add those computers to your homegroup. You'll need the following password.

Write down this password:

Fr59hh84KW

Print password and instructions

If you ever forget your homegroup password, you can view or change it by opening HomeGroup in Control Panel.

How can other computers join my homegroup?
Finish

Figure 11-1 A homegroup password is generated randomly

Courtesy of Course Technology/Cengage Learning

After a homegroup is created, other computers can join it by changing their network locations to Home or by going to HomeGroup in Control Panel. When a computer joins a homegroup, the same sharing options configured when the homegroup was created are available, allowing different computers to have different sharing options. After sharing options have been chosen, the homegroup password must be entered. When a computer joins a homegroup, all users logging on to the computer can access shared resources on the homegroup, but each user controls access to the files he or she shares. Users access shared files by opening the Computer window and clicking Homegroup in the left pane to display a list of other users currently logged on with their computer names in parentheses (see Figure 11-2).

Users can share or unshare a folder or library by right-clicking it in Windows Explorer and pointing to Share with (see Figure 11-3). A folder or library can be unshared (by selecting the option to share with Nobody), shared with the homegroup for read or read/write access, or shared with specific users whose computers may nor may not be members of the homegroup.

To access files shared by another user, click the user to see a list of available shared libraries and folders. If you access another user's shared library frequently, you can add it to your library, thereby making the files accessible directly from your Libraries folder in Windows Explorer.

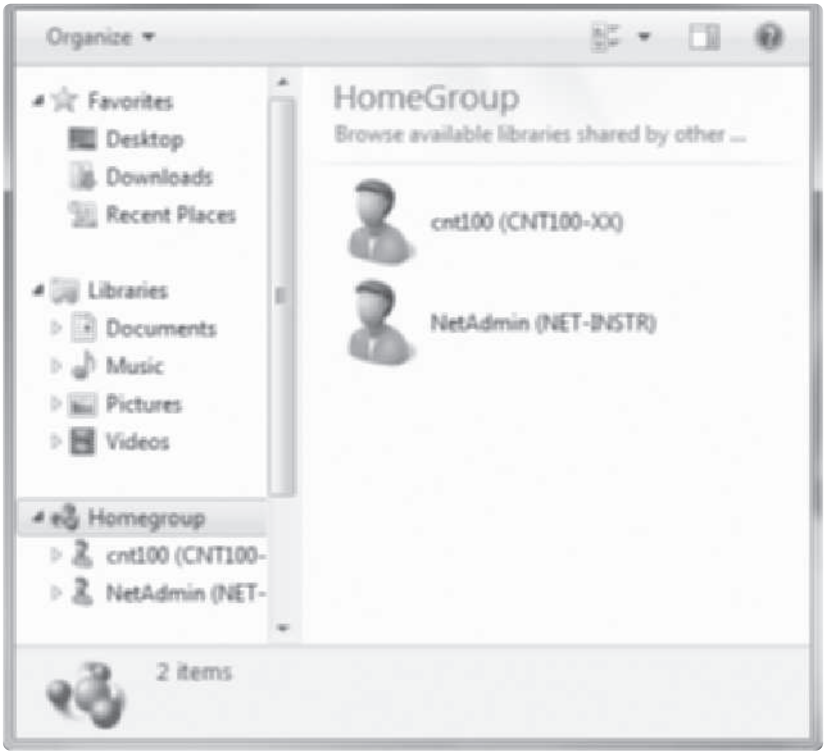


Figure 11-2 Viewing members of a homegroup

Courtesy of Course Technology/Cengage Learning

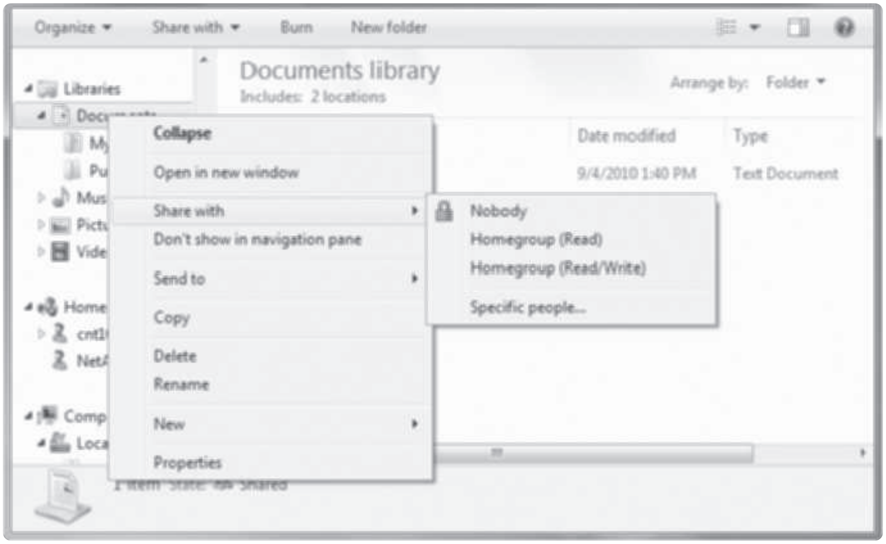


Figure 11-3 Changing homegroup sharing options

Courtesy of Course Technology/Cengage Learning

Troubleshooting HomeGroups At times, you might not see all computers that are members of a homegroup, or you might have problems creating homegroups. In these situations, you can use the HomeGroup Troubleshooter to solve some of these problems. To open it, right-click Homegroup in Windows Explorer. HomeGroup Troubleshooter attempts to verify the firewall and permission settings required for homegroups to work and tries to detect network problems that might prevent homegroups from working correctly. If it doesn't solve the problem, check the following:

- *Routers*—Homegroups don't operate across routers, so all computers must be on the same subnet.
- *IPv6*—IPv6 must be enabled to create or join homegroups.
- *Clock settings*—All computers must have the same time settings, including the correct time zone.
- *Third-party firewalls*—HomeGroups sets Windows Firewall when you create or join a homegroup, but if you're running a third-party firewall or antivirus program that performs firewall functions, you might have to disable or configure it. Microsoft publishes a document describing how to set firewalls to allow HomeGroup functionality.
- *Network Discovery*—Network Discovery must be enabled. To access this setting, click Advanced sharing settings in the Network and Sharing Center.

Homegroups can simplify file and printer sharing when your security needs are modest and you want files to be shared between several computers in a peer-to-peer network. For more advanced sharing options in a peer-to-peer network, use traditional file sharing and permissions, discussed in Chapter 9. For an all-around better file-sharing solution with centralized account management, use a domain-based network.

Hands-On Project 11-1: Sharing Files with Windows HomeGroup

Time Required: 20 minutes

Objective: Configure Windows 7 computers to join a homegroup.

Required Tools/Equipment: Your classroom computer running Windows 7

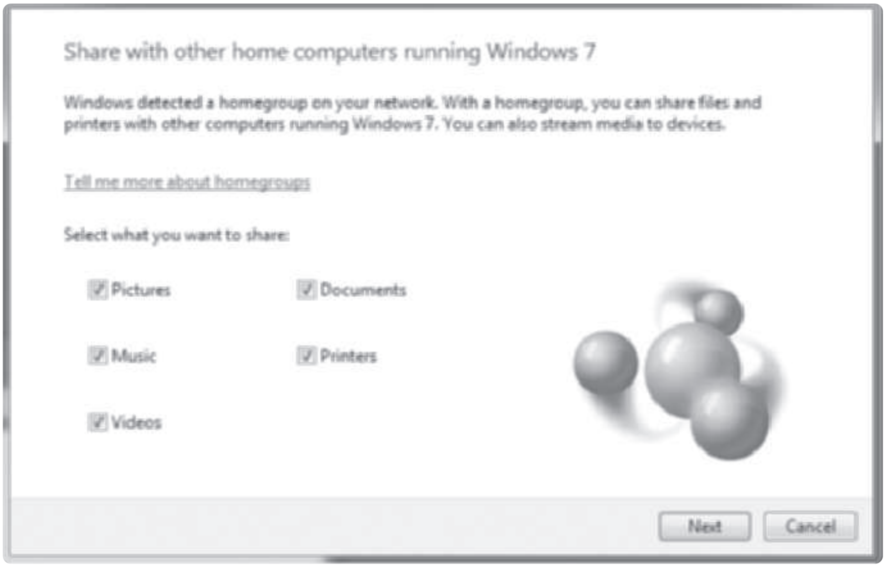
Description: In this project, you configure Windows 7 to use the HomeGroup file-sharing feature. The instructor should lead this project by creating a homegroup first (or designate one student to create the homegroup), using the steps outlined in the previous section. You then join the homegroup by following the steps in this project. You need the homegroup password.

NOTE

The homegroup creator can change the randomly generated password to make it simpler.

1. Log on to your computer as an administrator.
2. Click **Start**, **Documents**. Create a text document in your Documents folder named **DocOnNet-***XX* (replacing *XX* with your student number).

3. Open the Network and Sharing Center. Under View your active networks, click the **Work network** link. (You set your network type to Work network in Hands-On Project 5-1; if it's set to Public network, click this option instead.)
4. In the Set Network Location window, click **Home network**. If the homegroup hasn't been created yet, the next window prompts you to create a new homegroup. Your homegroup should already have been created, so click **Cancel**, wait until the instructor creates the homegroup, and start this step again.
5. In the Join a Homegroup window, click the **Documents** check box so that your documents are also shared (see Figure 11-4). Click **Next**.



Share with other home computers running Windows 7

Windows detected a homegroup on your network. With a homegroup, you can share files and printers with other computers running Windows 7. You can also stream media to devices.

Select what you want to share:

☑ Pictures ☑ Documents

☑ Music ☑ Printers

☑ Videos

Figure 11-4 Joining a homegroup

Courtesy of Course Technology/Cengage Learning

6. In the next window, enter the password your instructor has supplied for the homegroup, and then click **Next**.
7. The next window states that you have joined the homegroup. Click **Finish**.
8. To view other computers in your homegroup, click **Start**, **Computer**. In the left pane, a list of users in the homegroup, with their computer names in parentheses, is shown under Homegroup, similar to Figure 11-2 shown previously.
9. Click a user listed under Homegroup to see the list of shared folders. (If you don't see a list of users, right-click **Homegroup** and click **Start the HomeGroup troubleshooter**.)
10. Click **Documents** and verify that you can see the document created in Step 2.
11. Change your network location back to **Work network**. Close all open windows.

Sharing Files in a Windows Domain Environment If you require more than the minimum security and sharing files is a major part of your business network, using a file server with a centralized user database is the best way to go. In Windows, these requirements mean installing a domain controller. After installing a Windows server configured as a domain controller, user accounts need to be created only on the domain controller. All desktop computers and other servers simply need to be made domain members. After user accounts are created, they, along with group accounts, can be used to assign file and folder permissions on any computer in the domain. You can share folders on the domain controller, other servers, and even desktop computers, and permissions can be set by using accounts created on the domain controller. This centralization of accounts vastly simplifies resource management and improves network security.

Sharing Files in a Linux Environment Typically, you have two choices for sharing files in a Linux environment. One is using Samba, discussed in Chapter 9, for compatibility with a Windows environment. The other choice is using Network File System (NFS), which might be a good choice if the environment consists of mostly Linux computers. In both cases, the Linux client computer mounts a shared folder in its own file system and accesses the shared folder as though it were a local resource. Permissions are set in the Linux file system, as discussed in Chapter 9. The advantage of using Samba rather than NFS is Samba's compatibility with Windows file sharing.

Using an NAS to Share Files As discussed in Chapter 8, an NAS is a server dedicated to sharing files. A device sold as an NAS has its own user interface, usually accessed via a Web browser for creating user accounts, groups, and shared folders. Many NASs can also be configured to integrate with a Windows domain controller, so user accounts need to be created only on the domain controller. An NAS can be a good compromise between a peer-to-peer network and a domain-based network. NAS configuration is usually straightforward and doesn't normally require the expertise that Active Directory in Windows Server 2008 does. In addition, an NAS can cost much less than a server with Windows Server 2008 installed. Some NASs have a few slots for installing hard drives and a network interface and are no larger than a thick book. So if space is at a premium and simplicity in configuration is preferred, an NAS might be the ideal solution.

Equipment Sharing in a Small Business

A printer is the most common piece of equipment shared in a network. A typical issue in small businesses is sharing personal printers attached directly to a user computer's USB port. Sharing printers in this manner is challenging because the user has control over this printer's operation. The user could shut down the computer, turn off the printer, or take some other action that prevents network users from printing to the shared printer. Nonetheless, printer sharing is an important requirement of most small business networks.

One way to facilitate printer sharing is to connect the printer to the network rather than to a user's desktop. Some printers come equipped with a network interface or a slot to plug in a network interface, thereby allowing you to connect the printer directly to the network. If this option isn't available, some companies make small print server boxes that plug into the network on one end and plug into the printer via a USB port. Whether the network interface is built into the printer or is an add-on device, these print servers can be assigned an IP address and accessed by most OSs.

Scanners can also be shared. Scanners that can be shared on a network come with their own sharing software and can't be shared by using the same method printers use. Hewlett-Packard (HP), for example, has a utility that runs on the computer to which the scanner is attached. This utility shares the scanner and allows you to specify a password, if needed. Other computers must have the HP scanning software installed and run the remote scanning software supplied by HP. Because high-end scanners can be expensive and take up a lot of desktop space, sharing them among several users makes sense.

Other devices that can be shared on a network include external hard drives that connect via a USB interface and card readers that read Secure Digital (SD) and Compact Flash (CF) cards, such as those in digital cameras and PDAs. These external hard drives are a good solution for backing up data in lieu of tape or removable media, such as CDs or DVDs. Because hard drives have so much capacity, they can be set to back up data files of many users over the network quickly and easily.

Equipping Small-Business Networks

Most TV and print advertisements for network equipment are aimed at large enterprise network administrators. The equipment needs of most small businesses are far more modest. A rack full of blade servers is overkill for most small businesses, unless their business is Web hosting. A typical small-business environment might consist of one or two servers, some workstations, a few switches, and a router to connect to the Internet.

However, don't be enticed by low prices and the seemingly equivalent functionality of network devices sold as consumer products. Consumer products are intended for residential users and might lack important security or management features found in more robust products targeted at small-businesses. Most well-known equipment manufacturers have a small business or small and medium business (SMB) line of products with features that are often worth the extra cost.

Servers and Desktops

Most computer manufacturers, such as Dell and Hewlett-Packard, have small-business solution centers with products focused on the needs of small businesses. Go to any of these companies' Web sites, and you'll see a link to their small-business offerings. Usually, you can purchase a server fully loaded with a small-business edition of an OS and features you can choose, such as e-mail, Web, and database servers. Many companies give you an option of which OS you want preinstalled, or you can install your own. Common choices are Windows Server 2008 Standard Edition, Windows Small Business Server 2008, and Linux. Several server manufacturers offer a buying guide listing features and servers supporting these features.

A general rule of thumb when purchasing a server for a network is to buy as much hardware as the budget allows that will meet the company's estimated needs for the next two to three years. Buying hardware with expandability features that you can't foresee using in more than two to three years makes little sense because by that time, upgrading to a new computer might make more sense than upgrading the hardware on an existing one—assuming you *can* upgrade. An example of buying too much expandability is purchasing a server with one CPU that can be upgraded to four CPUs. If one CPU meets your needs today, it's unlikely you'll need four CPUs in a year or two. In addition, because CPU technologies change so quickly, acquiring the additional CPUs you need to upgrade might be difficult. Besides, in two to three years, a single CPU will probably be able to do as much work as four older CPUs for less money. That being said, you should consider being able to upgrade to a faster CPU or add a processor because these needs are likely to come up within a year after your initial purchase.

Memory expansion and storage expansion are critical design features to look for in a server. You might think a server with 2 GB of RAM and 500 GB of hard drive space is enough, but when this simple file and print server turns into a database server and Web server, the OS might be starving for resources.

Another feature to look for is fault-tolerant storage solutions. That usually means a RAID disk system, which makes it possible for the server to continue operating even if a disk drive fails. A common disk configuration is using RAID 1 (disk mirroring) on the drives containing the OS and applications and RAID 5 (disk striping with parity) on data drives. Disk mirroring requires two disk drives of the same size because everything written to one disk is written to the second disk automatically. If one disk fails, the other disk has a complete up-to-date copy of the system, and the server can continue running as though nothing happened. Disk striping with parity requires at least three disks. When data is written to a RAID 5 disk system, it's spread evenly over two of the disks, and parity information is written to the third disk. With this arrangement, if a disk fails, the data on the failed disk can be reconstructed from the data and parity information on the remaining disks.

Desktop computers for a small business usually differ from a computer designed for home use in the software installed and some hardware components. In most home computers, multimedia and entertainment components and software are emphasized, but in most business computers, the focus is on productivity software and manageability. For example, many home computers have a home edition of the OS installed, whereas a business computer is better off with a professional, ultimate, or enterprise edition. Computers running one of these editions can be part of a Windows domain, and this OS offers more management and security features than home editions do.

Networking Equipment

Another decision to make before you select networking equipment for a small business is where to put the equipment. Most small businesses don't have a large wiring closet, so you might need to get creative. For example, in a business consisting of only eight peer-to-peer computers, an existing cabinet can be used with an eight-port switch bolted to the cabinet wall. Care has to be taken to ensure adequate ventilation, but a small switch doesn't require much. In a small business, the space used for network equipment is often shared with another function, such as phone and alarm system equipment. Common sense must be used to make sure the space is adequate to the job. Servers and some network switches can generate a lot of heat, so cooling is essential. If the system gets too warm, hard disks and motherboard components can fail or become corrupted. As with servers and desktops, look for the SMB line of products from network equipment manufacturers, such as NetGear, Linksys, and D-Link.

Linksys is owned by Cisco Systems. You can find Linksys products at *www.linksys.com* or *http://home.cisco.com/en-us/wireless/linksys/*.

Making a Wired Connection In a small network of only a few computers, simply running cable from computers to the hub or switch might be tempting, but don't give in to this temptation. The biggest problem with running a single cable from station to switch is that when you move the computer, you might not have enough cable slack to reach the new location. Even if you have only a few computers to connect, you should have network jacks at the work area wired to a patch panel in the wiring closet near the switch. Then make the connection from the jack to the computer's NIC and from the patch panel to the switch with patch cables. (This cabling arrangement was shown previously in Figure 4-9.) Category 5e or 6 cable should be used, and after it's installed, it should be tested. If you're working with an existing cable plant, test all cable runs before you begin your work, and replace or reterminate any cables that fail or have suspect terminations.

Switches should be used to connect workstations; if you're upgrading a network, replace hubs with switches. When choosing a switch, you should consider the following options:

- *Switch speed*—100 Mbps and Gigabit Ethernet switches are the norm today. In a server-based environment, an asymmetrical switch is recommended, with most ports being 100 Mbps ports and one or two being Gigabit Ethernet ports. Servers should be attached to the Gigabit Ethernet ports.
- *Managed or unmanaged*—A managed switch has several advanced configuration options and can sometimes gather network data on a per-port basis. The extra functionality comes at a price—usually 5 to 10 times that of an unmanaged switch. In most cases, an unmanaged switch is adequate. A smart switch (discussed in Chapter 7) might be a good compromise if you need some of the advanced features it offers. A 24-port 100 Mbps switch with two Gigabit Ethernet ports can cost from $100 up to $400 or more.
- *Support for multiple media types*—Higher-end switches might have provisions for both copper and fiber-optic connections. In some cases, the fiber-optic connections come as an optional plug-in module, called a gigabit interface converter (GBIC) or mini-GBIC. This type of switch is ideal when you have to connect to computers or another switch exceeding the distance limitations of UTP cable or if the cable must pass through an electrically noisy environment, such as a manufacturing floor.

As you plan and install wiring for the network, be sure to keep in mind the company's security policy. Although many small businesses don't have a defined security policy, physical security issues should be discussed before equipment is installed so that the business owner and you can make informed decisions.

Making a Wireless Connection The availability of wireless equipment at a good price with good performance makes going unwired an attractive option, especially for new installations with a fairly small number of computers. Vendors don't usually provide information on the maximum wireless connections an access point (AP) can handle, but independent testing has shown that most consumer products (such as an AP you find at an office supply store) max out at around 40 connected computers. More expensive commercial products, such as those manufactured by Cisco Systems, can likely handle more than 100 connections with little data loss. These restrictions don't mean that you can't use wireless in a larger network; they simply mean that multiple APs might be needed, especially if computers are spread over a large area.

That being said, wired connections are recommended when the environment accommodates running wires and the computers are stationary. If the environment consists mainly of users running around with laptops or handheld computers, a wireless infrastructure is definitely an advantage. Of course, nothing prevents you from using a combination of wired and wireless networking. In fact, a combination is the most common design. A wired infrastructure is used for all desktop computers and servers, and a wireless AP is set up for mobile users. The wireless AP connects to the wired network so that the two networks can communicate, as shown in Figure 11-5.

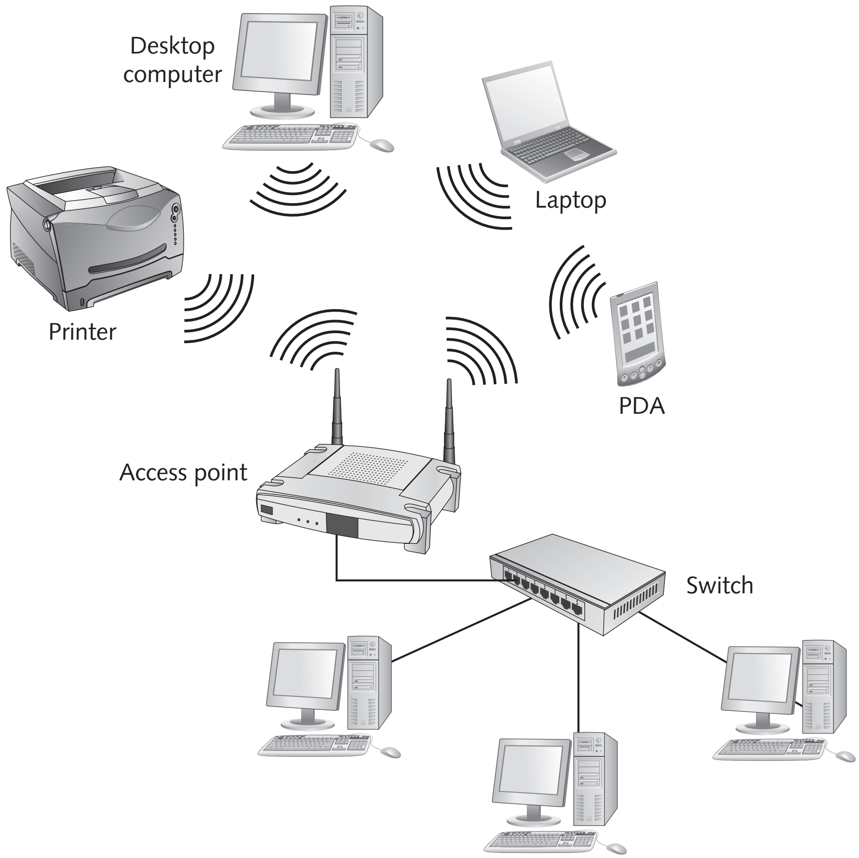


Figure 11-5 Wired and wireless networks coming together

Courtesy of Course Technology/Cengage Learning

Working with a wireless network involves special considerations that aren't a factor in wired networks. For example, outside (and unauthorized) people can access the wireless network simply by being close enough to the AP to receive a signal. This security concern is why using the wireless security practices discussed in Chapter 10 is imperative. Using a form of encryption is critical when installing a wireless network for a business; otherwise, data is at risk. Another issue with wireless networks is unique forms of interference. For example, cordless phones can use the same frequency as an 802.11 network. If a phone is in use, users can lose their connections with the network. This problem might not be too severe in a home network (although it's annoying), but it can grind business to a halt. When designing a wireless network, identify any sources of potential interference, such as cordless phones, microwave ovens, nearby wireless networks, and other radio frequency sources, and be sure they're on frequencies different from the wireless standard you plan to use. Also, make sure you test during normal business operations rather than after hours because equipment might be in use during business hours that you would be unaware of after hours.

When selecting wireless equipment, one of the most important considerations is the security standard supported. Whatever security standard (WPA or WPA2, for example) the AP supports must also be supported by the wireless NICs you use. Another feature to consider is whether the AP can be bridged to other access points. If your wireless network extends beyond the reach of one AP, multiple access points might be required, and you need to make sure all access points can communicate with one another.

Communicating with the Outside World

Even small businesses need to communicate with the outside world, particularly to access the Internet. Besides Internet connections, many businesses need employees to be able to access the company network from home or while away on business. Some issues discussed in this section include Internet access, dial-up connections, and virtual private network (VPN) connections.

Accessing the Internet Most small businesses require Internet access. For 10 to 20 computers, a broadband cable or DSL connection is usually enough. A typical setup includes a cable or DSL modem connected to a router and the router connected to one of the switches, as shown in Figure 11-6.

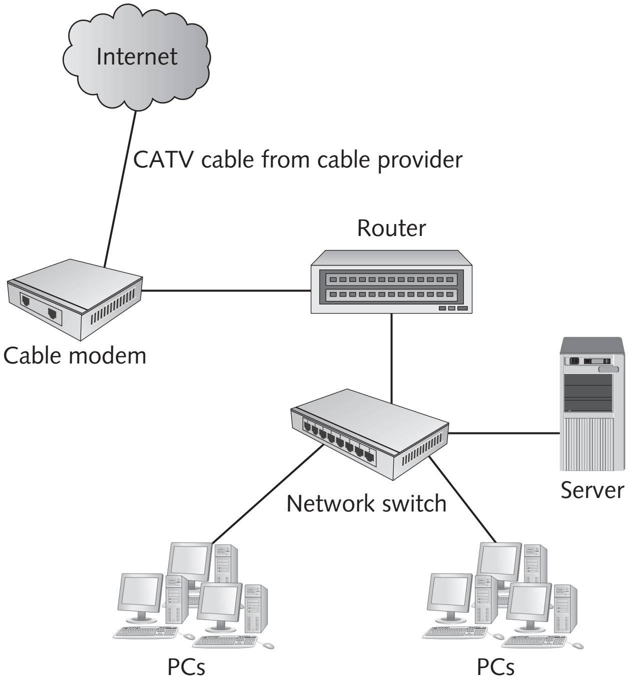


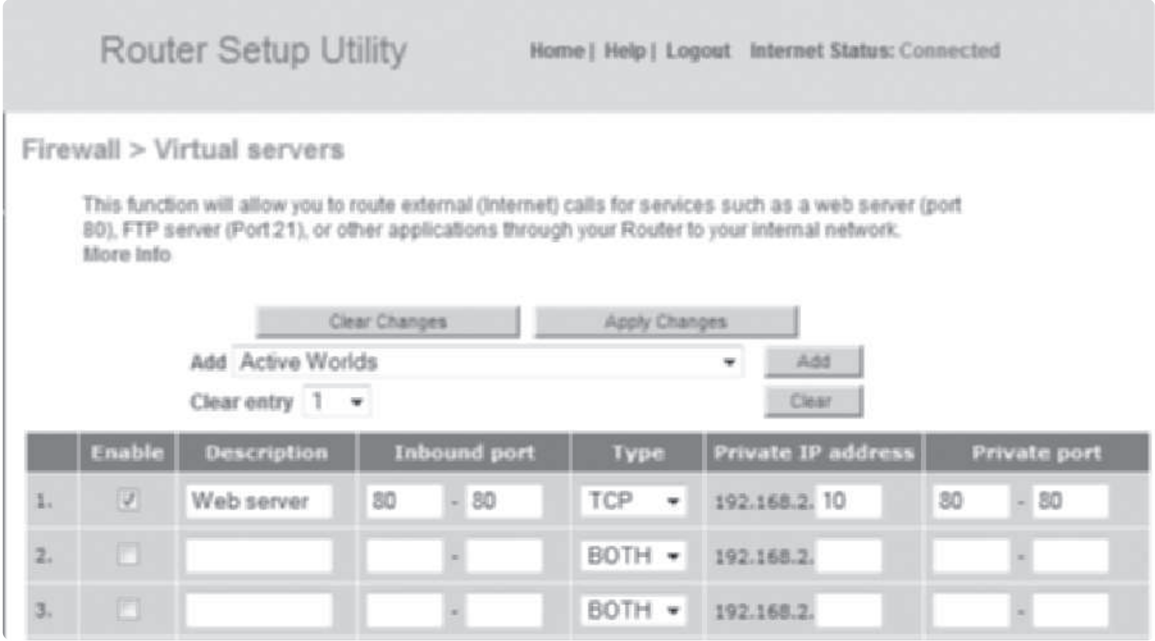
Figure 11-6 A network with a cable modem

Courtesy of Course Technology/Cengage Learning

In this type of network setup, the router is usually the network firewall, too. However, depending on your security needs, investing in a dedicated firewall that sits between the router and the switch might be worthwhile. In this configuration, the firewall stops any attacks before they reach the router. The router also usually plays the role of DHCP server and network address translator, handing out private IP addresses to internal computers and translating them via Port Address Translation (PAT) to the address the ISP provides when Internet requests are made. The router also gives each workstation a default gateway address (the router's address) and the DNS server addresses workstations need to translate domain names to IP addresses. The router usually acquires DNS server addresses from the ISP.

The type of router used in this situation is typically an inexpensive device (less than $100) with a Web browser interface for configuration. If a wireless network is set up, a router supporting both wired and wireless connections can be used. These devices can be purchased from computer retailers and office supply stores and are often billed as SOHO routers.

The default operation of these devices is to allow all packets through if an internal computer initiates the communication session. However, no unsolicited packets are allowed into the network from the outside. If communication needs to originate from the outside (for example, the business is running its own Web server), the router configuration can be changed to allow this communication. Figure 11-7 shows the virtual server configuration window for allowing this type of communication. The configuration option is sometimes called **port forwarding** because you're configuring the router to forward requests that apply to only certain TCP ports. In this figure, port 80 (the port for HTTP or Web communications) is being forwarded to an internal Web server at address 192.168.2.10.



This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network.

Add: Active Worlds

Clear entry: 1

	Enable	Description	Inbound port	Type	Private IP address	Private port
1.	☑	Web server	80 - 80	TCP	192.168.2. 10	80 - 80
2.	□		-	BOTH	192.168.2.	-
3.	□		-	BOTH	192.168.2.	-

Figure 11-7 Configuring port forwarding on a router

Courtesy of Course Technology/Cengage Learning

Of course, the company security policy should be taken into account when configuring access to the outside world because this type of connection is where most trouble originates. As soon as an Internet connection is established, equipping all servers and workstations with antivirus and antispyware software is doubly important.

VPN Remote Access A VPN remote access connection can be made as long as both parties are connected to the Internet. As discussed in Chapter 10, a VPN creates a private communication channel between two parties via the public Internet. Two VPN modes are available with most VPN devices:

- *Gateway-to-gateway*—In the **gateway-to-gateway VPN mode**, a VPN connection is established between two routers that support VPNs. No software needs to be installed on the computers using the VPN. This mode is used mostly between offices connected to the Internet through a router that supports VPNs. In this setup, all communication between the two offices is private, even though data travels across the public Internet.
- *Client-to-gateway*—The **client-to-gateway VPN mode** establishes a VPN connection between a single client computer and a VPN device. This mode requires configuring a VPN client on each computer participating in the VPN and a VPN device that clients connect to. This mode is best for providing private communication to the company network for employees working from home or employees who must connect to the network while traveling. In this setup, users connect to the Internet through their ISPs, and then run the VPN client software to create a private connection with their company network.

Many SOHO equipment manufacturers, such as Linksys, NetGear, and D-Link, have fairly inexpensive VPN routers that support either VPN mode. Prices for this equipment range from under $100 for a VPN router that supports eight or fewer VPN connections to under $500 for a VPN router that supports as many as 30 or 40 connections. Be aware of terminology when purchasing a router for VPN connections. Some routers claim to support VPN "pass-through," which enables a VPN client to connect to a remote VPN device but doesn't actually create a VPN connection. This type of router is best for users who have a small network at home and want to connect to the company network by using client-to-gateway VPN mode. The home router doesn't participate in the VPN connection; it simply allows the VPN connection to pass through it.

When outfitting your business with a router that supports VPN connections from remote clients, look for one that supports VPN endpoints. The number of endpoints or tunnels the VPN router supports tells you how many VPN connections can be established. In client-to-gateway VPN mode, one VPN endpoint per user connection is required. In gateway-to-gateway VPN mode, in which a connection is made from LAN to LAN, one endpoint per LAN connection is required.

Identifying Requirements for Small-Business Applications

The application needs of small businesses range from ho-hum simple to quirky and complex. On the simple side, some businesses need only an office application suite, such as Microsoft Office. On the complex side, a business might use a custom program that has little or no support for networking and requires the network administrator to be creative in making it work with the office network. This chapter doesn't delve into industry-specific applications; instead, it concentrates on some standard business applications that have a place in many small businesses.

Before discussing specific types of software, two issues for network applications should be addressed. The first is that not all software is designed to operate over a network with multiple users accessing the data. Many applications, such as account and sales management software, sell both single-user and multiuser versions of their programs. It might be possible to network a single-user version, but you're usually limited to one user at a time accessing the data. If you know that multiple users need to access the application simultaneously, you probably need to purchase the multiuser version. The second issue is software licensing. Just because an application has been purchased doesn't necessarily mean it can be installed on the network or on multiple computers. The **end user license agreement** (**EULA**) should be consulted before purchasing any software for use by multiple users.

Accounting Software

Many accounting or bookkeeping applications are tailored to small businesses, such as QuickBooks by Intuit, AccountEdge, Sage Software's Simply Accounting, and Peachtree Accounting. A few free products are worth a look, such as Freshbooks and Outright. Most of these applications offer a choice of version, depending on the complexity of the company's needs. Typically, accounting packages come in basic versions to support common business needs, such as invoicing, check writing, inventory tracking, and payroll. For more complex needs, many packages have a professional or advanced version that supports multiple users, bill-of-materials handling, time and billing management, and other advanced features. As a network technician or administrator, your job isn't to support the function of these applications but to help ensure that the network is set up to run them adequately and make sure data is backed up. Some issues a network technician faces in supporting these applications include the following:

- Should the software be accessible by multiple users in the company? If so, should users be able to access the application and make changes to data simultaneously?
- How should the application be secured from users who shouldn't have access?
- Older software packages might not integrate with Windows well or support networking directly. You might need to use mapped drives to specify network locations or use printer redirection to print to network printers.
- How is the software and its data backed up? Some applications have their own backup program for data files. Whether you use a third-party backup program or the backup program included with the application, you must devise a scheme to support backing up and restoring data.

These issues are just a few of the many to consider in supporting accounting software. Because accounting is of utmost importance to a business's operation, care must be taken before performing any actions that might corrupt or destroy data. When possible, consult the application vendor's technical support when configuring or troubleshooting these applications.

Sales and Contact Management Software

Although many small business owners are aware of accounting software, they might not be familiar with sales and contact management software. Today's sales and contact management software offers features that are leaps and bounds ahead of yesterday's rolodex. Notes on customer conversations can be tracked and accessed by multiple users, promotional mailings can be targeted and automated, and even customers' birthdays and their pets' names can be tracked.

Products such as Goldmine from FrontRange Solutions, Maximizer by Maximizer Software, and ACT! by Sage Software have been industry standards in this area for years. These packages fall into the category of **customer relationship management** (**CRM**) and go far beyond simple electronic phone books. Shared calendars and to-do lists, sales forecasting, extensive client history management, and integration with smartphones are just a few features these packages offer. Many have versions targeted for specific industries, such as real estate and financial services.

CRM software has some of the same support issues you might encounter with accounting software. Again, although you might not want or even need to be an expert in this type of software, a network technician working with small businesses is often expected to be a jack-of-all-trades in computer and network support, including recommending and supporting small-business applications. Your knowledge of the products available for handling typical small-business tasks will help on the job, not to mention getting the job in the first place.

Windows Small Business Server

Although Windows Small Business Server (SBS) isn't a small-business application, it's bundled with many of the network services and add-on products a small business might need. SBS was designed with small businesses in mind and includes an administrative console with all main configuration options in one central user interface (see Figure 11-8).

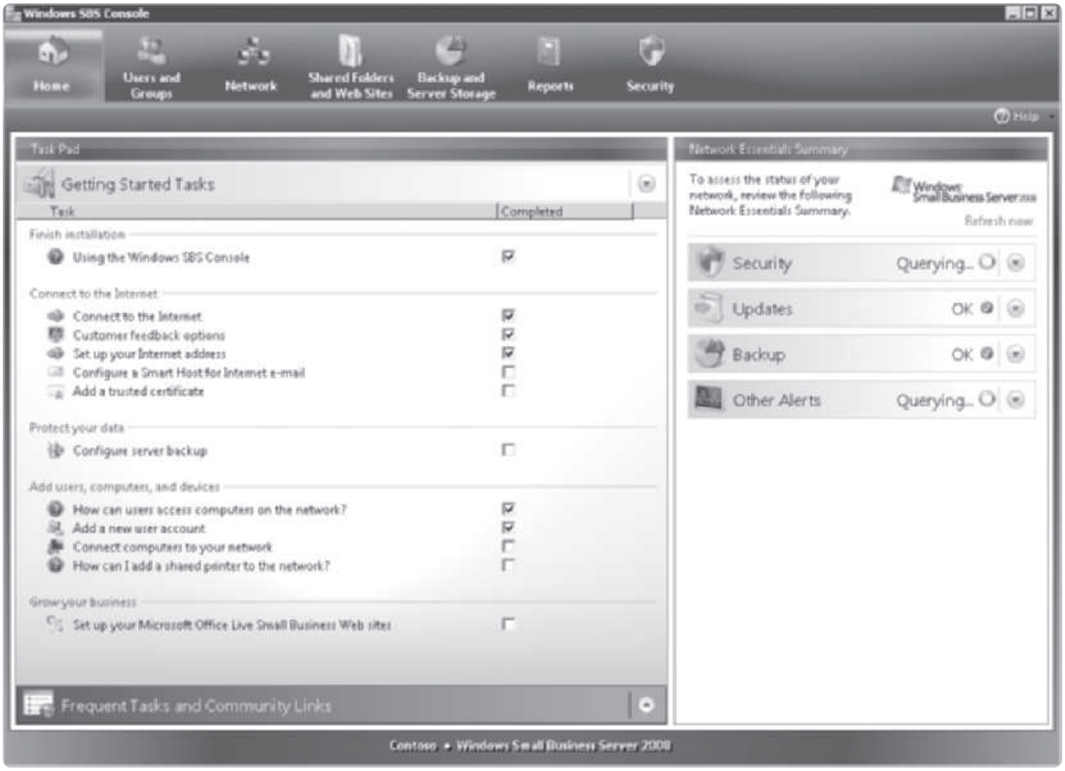
SBS offers the following application features beyond the Windows Server 2008 OS:

- *E-mail server*—Microsoft Exchange Server 2007 comes standard with SBS 2008.
- *Shared calendar*—It includes Microsoft Exchange Server's calendaring functions.
- *Intranet resource sharing*—Sharepoint Services is available to organize documents and collaborate with colleagues.
- *E-mail security*—Microsoft Forefront Security is included to protect e-mail from viruses, worms, and spam.
- *Database*—Microsoft SQL Server comes with SBS 2008 Premium Edition.

SBS provides support for up to 75 users and is designed to be run by employees who don't have an extensive IT background. For larger networks, Windows Essential Business Server supports up to 300 users and has most of the same features as SBS plus security and network management options. However, networks of that size and complexity usually require onsite IT staff. Windows SBS is a good alternative to standard Windows Server editions if you know your business needs its built-in services and you want to be able to manage most services by using in-house employees instead of hiring IT consultants.

Hosted Applications

An alternative to installing and supporting business applications on servers and desktops is using hosted applications, which are one component of cloud computing (discussed more in Chapter 12). Google Apps, for example, provides a full suite of office applications, e-mail,


Windows SBS Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Help
Task Pad
Frequent Tasks and Community Links
Network Essentials Summary
Windows Small Business Server 2008
Refresh now
Contoso • Windows Small Business Server 2008

Getting Started Tasks

Task	Completed
Finish installation	
Using the Windows SBS Console	☑
Connect to the Internet	
Connect to the Internet	☑
Customer feedback options	☑
Set up your Internet address	☑
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	
Configure server backup	□
Add users, computers, and devices	
How can users access computers on the network?	☑
Add a new user account	☑
Connect computers to your network	□
How can I add a shared printer to the network?	□
Grow your business	
Set up your Microsoft Office Live Small Business Web sites	□

To assess the status of your network, review the following Network Essentials Summary.

Security	Querying...
Updates	OK
Backup	OK
Other Alerts	Querying...

Figure 11-8 The Small Business Server 2008 administrative console

Courtesy of Course Technology/Cengage Learning

document collaboration, and calendaring that can be accessed through a Web interface. The Standard Edition is free and suitable for fewer than 50 users in environments where storage and security needs are modest. The Premier Edition has a nominal yearly fee for unlimited accounts, secure access, support, and considerable storage space. Using hosted applications is a viable alternative for businesses with fast, reliable Internet connections that don't need the advanced features of office suites, such as Microsoft Office, and don't want to support them.

Is Linux a Viable Desktop Alternative to Windows?

Much has been written about Linux in the workplace, with most of it focused on using Linux as a server OS. However, Linux has made inroads into desktops, too. Using an open-source Linux distribution is certainly less expensive than Windows or Mac OS in software costs. The biggest questions about using a Linux desktop are **total cost of ownership (TCO)** and application support. TCO is the cost when you factor in intangibles, such as support costs and productivity gain or loss. Linux has come a long way since the early 1990s, when only the savviest computer technician was willing to take on its difficult installation and configuration. Today, Linux installation for most distributions is no more difficult than a Windows installation. Although postinstallation configuration can still be challenging, Linux is definitely a viable option as a base OS.

In application support, Linux-based Web browsers and e-mail clients are similar to those in Windows and Mac OS, and powerful (and often free) office application suites are available. OpenOffice.org (*www.openoffice.org*) is an open-source office application suite that runs on Windows, Linux, Sun Solaris, and Mac OS. It's available as a free download and consists of a word-processing program, a spreadsheet program, presentation software, a database application, and a drawing and diagramming application. OpenOffice has good compatibility with Microsoft files. KOffice (*www.KOffice.org*) includes a full-featured word-processing program, a spreadsheet program, presentation software, a database application, and many other add-on applications. It runs on Linux and some UNIX versions and offers some Microsoft Office compatibility. A quick look at the Ubuntu Linux desktop and Applications folder (see Figure 11-9) shows that Linux is making good progress toward being your next desktop OS.

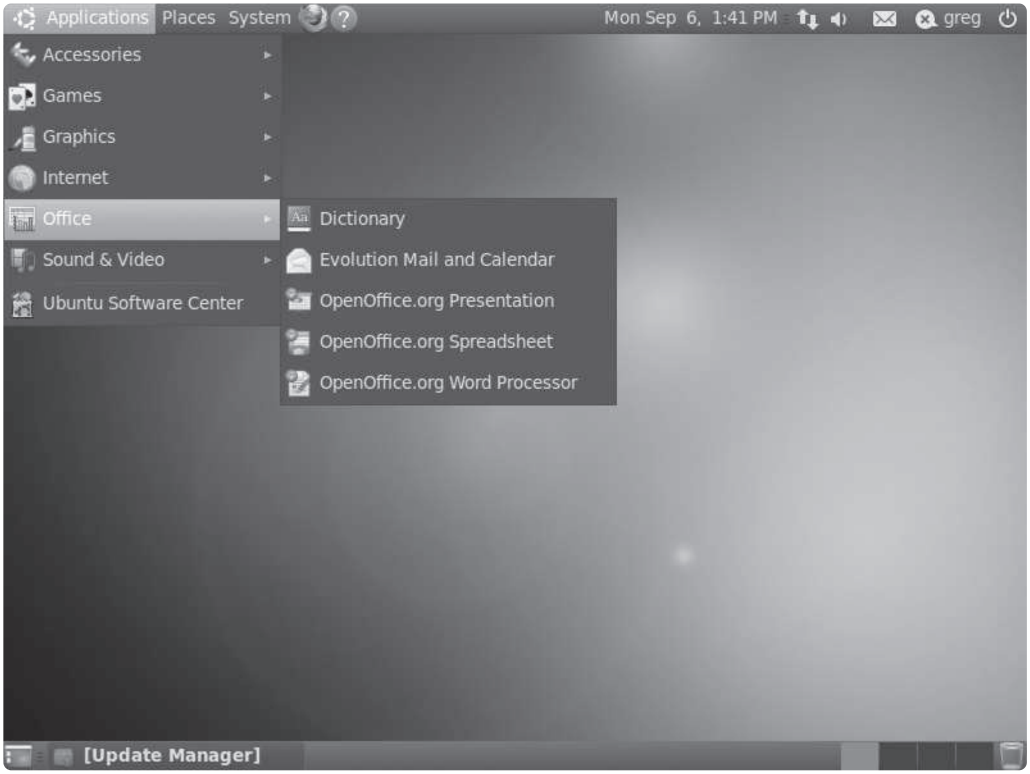


Figure 11-9 The Applications folder in Ubuntu Linux

Courtesy of Course Technology/Cengage Learning

Although Linux has a number of office productivity packages, support for industry-specific applications is lacking. If a small business simply needs what an office productivity suite includes, Linux is a viable option, particularly if support is available from the company's network technician. However, if the company needs to run industry-specific applications, you must find out whether Linux is supported. If a business is sold on Linux because of its open-source licensing and improved security over some competitors, there are solutions for running Windows applications in Linux. Windows Emulation (WINE) is one that's available free for all Linux distributions when a Windows environment is simulated, allowing an application to run as though it were running on Windows. VMware and VirtualBox, discussed in Chapter 8, are virtualization environments that enable you to run Windows on a Linux OS and vice versa. So if Linux sounds attractive but a critical application requires Windows, you can have the best of both worlds by using virtualization. Linux has come a long way, but its suitability for desktops depends on the expertise of the technicians who set it up and the compatibility of applications the business needs to run.

Supporting a Small Business

The job of supporting small businesses in their IT needs can sometimes be more difficult than supporting a large business because small businesses rarely have in-house specialized expertise. Large businesses might have a technician who specializes in supporting the network infrastructure, another who supports servers, one who supports desktop OSs, and still another who supports specialized applications; small businesses usually count on their hired consultant to do it all. This is where you, the entrepreneur, come in.

Entrepreneurs Wanted

Although it's true that many equipment manufacturers have started catering to small businesses, many computer consulting companies still have a large-business mentality. They're used to large jobs with large budgets, and their job is to install the network and leave the rest to the internal staff. Small businesses don't have large budgets or internal staff to support a network after it's installed. If you decide you want to specialize in working with small businesses, you need to understand their needs and be able to explain what technology can do for them. That's why knowing the choices available to these businesses for accounting software, CRM software, and office suites is important. You also have to understand and respect the way companies do business yet be able to gently nudge them toward solutions you know will make sense for them when they understand their options. Working with small businesses can be financially rewarding and create a sense of achievement because you can make a difference in a company's success by helping it use technology to increase and maintain its business. Before you can start working with small businesses, however, you must convince small-business owners to place their information technology in your hands.

Getting the Job Most small-business owners who are looking for a computer or network consultant usually request proposals from multiple vendors. If you're called on to develop a proposal, the most important thing you can do is listen to the company's requirements. Find out what kind of business a company is in, how it's currently managing day-to-day information, and where it wants to be in the next several years. Talk not only to the owner or manager, but also to the people actually using the computers, working with customers, handling accounting, and so forth. The more you know about how the business works, the more tailored and detailed you can make your proposal.

Most small businesses are customer friendly, and they expect the same from their vendors. Typically, they delve into technology cautiously because they don't have internal expertise and are hesitant to place the future of their business in a consultant's hands. So above all, be responsive when customers or potential customers call you. They need to know they can count on you to be available when they need you. Large businesses often don't expect to talk to a live person when they call for support because they often use call automation. If a small-business owner gets your voicemail or an automated answering service, you might lose that company as a customer.

When developing a proposal for a consulting job, be detailed about what's included in the price you quote. Many businesses want to have choices, so give them multiple quotes when appropriate, and spell out the advantages of the higher-priced option. Each line item of a proposal should specify what need it fills. That way, owners don't have to wonder whether they really need what you're quoting and whether all their needs are addressed adequately.

Securing a Small-Business Network

One aspect of your proposal to a small business that you shouldn't neglect is security. Spell out in your proposal how you plan to secure the network and data. First, you need to determine what type of security will work best with the business: an open security policy, for example, or a highly restrictive policy. When discussing a business's needs, be sure to emphasize the trade-offs between an open policy and a more secure policy. A more secure policy safeguards data better but at the expense of requiring more user training and perhaps lowering productivity. You must factor in how this company currently does business and whether tight security is truly a requirement for its business.

Passwords and Backup Don't automatically assume that every business should have password policies that require frequent changes and complex passwords—or any passwords, for that matter. Some businesses simply don't need or want this level of security. Perhaps all that's required is antivirus and antispyware software, an easy-to-follow backup scheme, and a simple disaster recovery plan. It's the consultant's job to make technology work for a business, not against it. As long as you explain the ramifications of an open security policy, and it's what the business wants, you just need to carry it out. If, on the other hand, a business does want a secure network, it's your job to know how to construct it. Chapter 10 covers many security issues you should be aware of and tools for setting up security measures.

Regardless of the security policy, one of the first security-related items on your agenda should be an easy-to-use backup strategy. Every business needs a backup scheme, and unless you're going to be available every night to run a backup, the process should be clear and concise so that any of the business's users can do it. Tape backup is still a favorite method for backing up large amounts of data, especially when hundreds or thousands of gigabytes must be backed up regularly. However, in a small business, tape backup might be unnecessary and unnecessarily complicated. Depending on the amount of data to back up, using removable media, such as DVD-RWs, might make sense; if there's more data, USB hard drives are a good solution. Some USB hard drives have a one-touch backup solution. For data on users' computers, document files can be backed up to a network hard drive, which can be backed up periodically to removable media for offline storage, if needed. The OS and applications don't usually require regular backup. One convenient method of backing up a user's OS and applications is creating a drive image of the computer's hard drive periodically and backing up the image to a network location. Many software packages are available to create an image of a hard drive, such as Symantec Ghost and Acronis True Image. A drive image allows you to recover from drive failure simply by restoring the image to a new drive. The user's computer is then returned to the same state it was in when the image was last recorded.

Microsoft's Backup utility in Windows Vista, Server 2008, and later can create a drive image, as can a free utility called Disk2VHD, available from Microsoft's Web site at *http://technet.microsoft.com/en-us/sysinternals/default.aspx*.

However you decide to back up, one essential step that many IT technicians skip is testing the backup and restore process to ensure that the backup scheme is actually working and data can be restored when disaster strikes.

Security from the Outside World Antivirus/antispyware software, as mentioned in Chapter 10, is a must for any computer with an Internet connection. Beyond that, a firewall should be in place for most businesses that share a connection to the Internet, such as through a cable or DSL modem. If a Windows computer is used to share an Internet connection, Windows Firewall is in place, but a dedicated router is preferable because it offloads extra traffic from a workstation and usually has more firewall features.

If a router is used to provide Internet access to multiple computers, it should be equipped with a firewall. Most inexpensive commercial routers are designed to block incoming traffic unless it's part of an existing conversation with an internal computer. However, for more complete protection, opt for a router described as a firewall router. These routers have firewall features that protect a network from external threats, such as DoS attacks and IP spoofing. They can also be set up to filter Web sites based on URLs and block cookies and scripting languages that can install spyware on company computers. In addition, these firewalls can be set up to allow Internet access only during certain times of the day and block unproductive bandwidth-heavy content, such as streaming media and peer-to-peer file sharing.

If you're running a wireless network, take extra care to ensure that wardrivers can't break into your wireless network and gain free reign of its resources. The wireless security precautions discussed earlier in this chapter and in Chapter 10 should be used. In addition, using an AP that allows adjusting the signal strength might be worthwhile. With some APs, you can adjust the wireless signal's strength so that only devices in close proximity can hear the signal. You can adjust the strength so that all your wireless devices receive the signal, but someone walking by outside can't.

Managing a Small-Business Network

Unlike a large business with its own IT staff, a set-it-and-forget-it approach doesn't usually work for a small-business network. There are hard drives to defragment, virus scanners to update, OS patches to install, and many other tasks. For this reason, working out a maintenance schedule and contract is usually a good idea. Some tasks can be automated, but others, such as software updates and disk cleanup, aren't as easy to automate. Setting up a weekly or monthly visit for maintenance keeps you in front of the small-business owner, inspiring confidence as well as making you the prime choice of vendor when more work needs to be done.

In managing a small-business network, there's nothing like personal contact. However, sometimes onsite visits are impractical or unnecessary. In these situations, remote access might be the best way to solve a problem quickly and easily. The following list describes some ways to set up remote access to a network:

- *VPN*—If the business is connected to the Internet through a broadband connection, a VPN is probably the best method for accessing and supporting the network remotely. You can connect to the company network securely from wherever you have an Internet connection and establish a remote desktop session with servers and workstations or monitor and update devices on the network. Windows has a built-in remote desktop application for remote control of a computer's desktop. Virtual Network Computing (VNC; *www.realvnc.com*) is another remote control/remote desktop application that works across several platforms, including Linux, UNIX, and Windows.
- *Dial-up*—Dial-up access is another option for accessing a network remotely, although it's less convenient. You can use Windows Server 2008 to configure remote dial-up access to a Windows network, or third-party products can be used on servers or desktops. Dial-up is sometimes used as a last resort when the network is down and VPN access isn't possible. If the situation warrants, having dial-up access to a network as a backup can save you a long trip.
- *Telnet*—Telnet is one way to gain command-line access to a computer or network device. It should be used when a secure connection has already been established, such as through a VPN. Telnet isn't a secure protocol, so usernames and passwords are sent across the network in unencrypted plaintext. Telnet is best used to access Linux or UNIX systems and command-line-based routers and switches. In a pinch, Telnet can also be used to manage a Windows system.
- *Secure Shell (SSH)*—SSH is a secure method of gaining command-line access to a computer or network device, and when it's supported, it should be used in place of Telnet because communication is encrypted. SSH is available for Windows and Linux systems.
- *Windows Remote Assistance*—For user help, Windows Remote Assistance is an option that doesn't require a VPN, as access to the user's computer is by invitation only. In addition, the user must be sure remote control is enabled. Remote control is enabled by default when Remote Assistance is enabled, and you can configure it in the Remote tab of the System Properties dialog box. The company firewall must also be configured to allow connections to the remote desktop port, which is 3389 by default.

However remote access to the network is set up, it must be done securely. Even a business following an open security policy shouldn't apply the policy to remote connections.

The technology needs of small businesses can be varied and complex. Like the people who own the business, each has its own quirks and requirements. Rarely can you devise a one-size-fits-all solution for a small-business network, but if you're prepared for something new every time you visit a new business, you'll soon have an arsenal of tools, tips, and tricks that make supporting small-business networks easier and help make the businesses you support more successful.

Chapter Summary

- Most small businesses have modest network requirements that don't require advanced WAN technologies, data encryption, or highly restrictive security policies.
- A server-based solution is often the best solution, but a peer-to-peer network is an option. Either way, it's best to design the simplest file-sharing solution that meets the organization's requirements.

- Windows 7 has a new simple file-sharing option called HomeGroup, which is used to create a password-protected file and printer sharing network without needing to set up user accounts and permissions on each computer in a homegroup.
- The two most common choices for file sharing in a Linux environment are Samba and NFS. Samba is compatible with Windows file sharing; NFS works best when most computers run Linux or UNIX.
- Most computer manufacturers maintain small-business solution centers offering equipment that focuses on the needs of small businesses. When purchasing servers, buy as much hardware as the budget allows that will meet needs for the next two to three years.
- When choosing network equipment, you need to decide between a wired and wireless network. In most cases, a wired solution works best for stationary systems, and wireless can be used for laptops and mobile users. In either case, selecting from the hardware vendor's SMB products is best.
- Internet connections and remote access usually require a broadband connection and a router. Some routers have built-in VPN capability.
- Small-business application requirements can range from simple and straightforward to very complex. Both single-user and multiuser versions are available for many applications.
- Typically, small businesses need office suites, accounting software, and sales and contact management software. Windows Small Business Server is a good alternative to Windows Server because it includes built-in e-mail, calendaring, and database applications as well as security features. Linux can be an alternative to Windows desktop OSs if there are no Windows-specific applications that all employees must run.
- Working with small businesses requires excellent communication skills and the ability to make proposals that business owners can understand. Security shouldn't be neglected, and devising a reliable backup scheme is a must.
- To manage a small business, remote control options should be considered, including Remote Desktop through a VPN connection, dial-up, Telnet or SSH, and Windows Remote Assistance.

Key Terms

client-to-gateway VPN mode This VPN mode establishes a VPN connection between a single client computer and a VPN device.

customer relationship management (CRM) A category of software designed to help businesses manage customers and sales prospects.

end user license agreement (EULA) A license that governs how an application can be used. It specifies how many users are allowed to use an application, how many times it can be installed, and whether the software can be copied, among other things.

gateway-to-gateway VPN mode This VPN mode establishes a connection between two routers that support VPNs.

homegroup A peer-to-peer networking feature introduced in Windows 7 that simplifies sharing files and printers between computers.

port forwarding The process by which a router forwards a request for a TCP or UDP port to a specified computer.

total cost of ownership (TCO) The cost of a product or service when intangibles, such as support costs and productivity gains or losses, are factored in.

Review Questions

1. Which of the following is one of the most important aspects of supporting a small business?
   a. Finding the most inexpensive solution
   b. Using a "canned" solution you can apply to all small businesses
   c. Listening to the company's requirements and designing a solution
   d. Using your experience to tell the business what it needs
2. Which of the following is a possible problem with a peer-to-peer network solution? (Choose all that apply.)
   a. Users can unknowingly sever access to shared files or printers.
   b. A failure on one computer could cause the network to crash.
   c. Sensitive data could be made available to unauthorized users.
   d. The centralized server could cause security leaks.
3. Which of the following is true of the HomeGroup feature?
   a. Homegroups are password-protected.
   b. The network type can be Work or Home.
   c. A Public network joins a homegroup automatically.
   d. New user accounts must be created on each machine.

4. Which is true about sharing files in a Windows domain?
   a. The user database is distributed among all domain members.
   b. At least two domain controllers are required.
   c. The user database is centralized.
   d. All computers except the server are workgroup members.
5. Which of the following is true about an NAS? (Choose all that apply.)
   a. It usually has its own user interface.
   b. It works only in a Windows domain.
   c. Users and groups can be created on an NAS.
   d. Most NASs are too big for small-business networks.
6. Which is true about Windows SBS? (Choose all that apply.)
   a. It includes an e-mail server.
   b. It requires more IT support than server OSs.

c. It supports 300 users.

d. It provides intranet functionality.

7. Which of the following is true about using Linux as a desktop OS? (Choose all that apply.)

a. Office applications are available that are compatible with Microsoft Office.

b. Virtualization can be used to run Windows applications.

c. It's difficult to install.

d. Open-source licensing makes it more expensive than Windows.

8. A domain controller simplifies resource management by doing what?

a. Distributing account creation

b. Providing larger hard drives

c. Eliminating the need to log on

d. Centralizing accounts

9. What are the most common options for sharing files in a Linux environment? (Choose all that apply.)

a. NetBIOS

b. NFS

c. TCP

d. Samba

10. Which of the following is a common fault-tolerant disk configuration for servers?

a. RAID 0 for the OS and RAID 1 for the data

b. RAID 5 for the OS and RAID 3 for the data

c. RAID 1 for the OS and RAID 5 for the data

d. RAID 3 for the OS and RAID 0 for the data

11. Which of the following is a consideration when purchasing a switch? (Choose all that apply.)

a. Switch speed

b. Support for multiple media types

c. Support for multiple Network-layer protocols

d. Whether it's managed or unmanaged

12. Which of the following is a consideration when selecting wireless network equipment? (Choose all that apply.)

a. Support for the 802.5 protocol

b. Category 6 cable connections for gigabit transfers

c. Security standards supported

d. Interference from other wireless devices

13. To run a Web server on a network protected by a SOHO router, you must enable what feature?

    a. Address translation

    b. Port forwarding

    c. Port filtering

    d. Address filtering

14. Which of the following is a VPN mode? (Choose all that apply.)

    a. Client-to-endpoint

    b. VPN-to-router

    c. Gateway-to-gateway

    d. Client-to-gateway

15. What legal document should be read carefully before purchasing software for multiple users to run?

    a. ELAN

    b. EULA

    c. Readme file

    d. User's manual

16. Which of the following describes the cost of a product when intangibles are factored in?

    a. CRM

    b. VPN

    c. TCO

    d. EULA

17. Which network remote access method provides a secure connection over the Internet?

    a. Dial-up

    b. Telnet

    c. UDP

    d. VPN

18. Which of the following is a feature a firewall router provides? (Choose all that apply.)

    a. Protection against DoS attacks

    b. Web site filtering

    c. Cookie blocking

    d. Protection against IP spoofing

Challenge Labs

Challenge Lab 11-1: Creating a Peer-to-Peer Small-Business Network

Time Required: 1 to 2 hours or more

Objective: Create a small-business network according to specifications.

Required Tools/Equipment: Four computers with a Windows desktop and/or Linux OS installed, one printer, and a wireless router/AP

Description: This lab can be done in groups. Set up a peer-to-peer small-business network for a company named SmallBiz. Three computers are wired, and one is wireless. If possible, one computer should run a Linux OS, such as Ubuntu. The network should look similar to Figure 11-10. One computer will run a Web server that should be accessible from the outside. Build this network to meet these requirements:

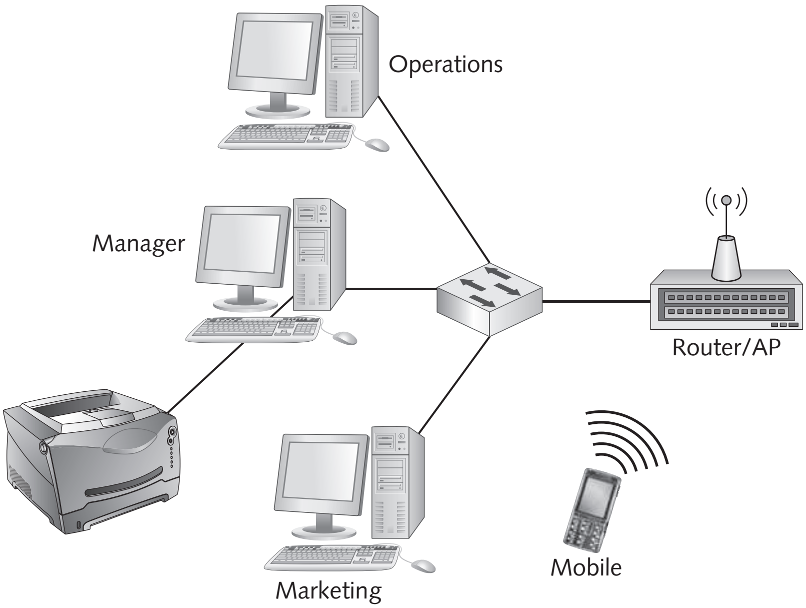


Figure 11-10 The Challenge Lab network layout

Courtesy of Course Technology/Cengage Learning

- The HomeGroup feature can’t be used.
- Name these computers Marketing, Manager, Operations, and Mobile (the wireless computer).
- The wireless computer doesn’t share any files.

- IP addressing should be static, and you can choose a suitable addressing scheme.
- The three wired computers have a dedicated folder set up to share files. The shares should be named appropriately.
- Users should be created as follows: MktUser, MgrUser, OpsUser, and MobUser.
- The shared documents on each computer should have at least read/write access by the user who uses the computer. For example, MktUser might be assigned Full Control access to the Marketing files. The other users should have Read access to the shared files. An Administrator account has Full Control access to all shared files.
- The router should be configured so that a Web site on the Marketing computer can be accessed from the outside.
- The wireless network should be secure and use an appropriate SSID.
- A printer should be configured on the Manager computer and shared. All other computers should be able to print to this printer.
- Develop a backup scheme stating how backup should be done. (You don't need to set up the Backup utility.)

Write a report documenting the network that could be used by an outside consultant who might need to troubleshoot or expand the network. In addition, write a paragraph or two stating whether a domain-based or other centralized server-based (such as an NAS) network might be a better solution.

Case Projects

Case Project 11-1

This project can be done in groups. You're going into business as a computer networking consultant, and you want to be sure all your potential clients get the same service. Devise a questionnaire that you and your other employees can use when interviewing a client about computer and networking requirements. Be sure to cover as many bases as you can think of, including but not limited to number of users, security, resource sharing, Internet access, applications, budget, existing cabling and equipment, and support needs. Save your questionnaire for use in the next project.

Case Project 11-2

Your instructor will concoct a fictitious small business for the purposes of this project. Each group should use the questionnaire designed in Case Project 11-1 to interview the instructor about the business's networking requirements. After the interview, each group should develop a proposal to submit to the business. The proposal should specify only solutions to the business's requirements and shouldn't include pricing yet. Each proposal should be presented to the entire class. Groups can revise their proposals based on feedback from the class and the instructor's suggestions. A final proposal should then be submitted to the instructor.

Case Project 11-3

Based on the final proposal submitted in Case Project 11-2, each group should create a detailed quote for equipment and services. Good sites to find information on pricing include *www.tigerdirect.com*, *www.newegg.com*, *www.lanshack.com*, and *www.cyberguys.com*, but your group can use other resources to determine costs. Be sure to include labor costs at $65 per hour (to keep labor rates consistent for all proposals). All items in the quote must be tied to the proposal submitted in Case Project 11-2. All quotes and final proposals should be presented to the class. The instructor will select a vendor based on the proposal's completeness and the price quote.