Chapter 1

Making Networks Make Sense

In This Chapter

- Understanding network hardware and software
- Recognizing a network's anatomy
- Making sure that the network's running
- Sharing resources
- Following Windows networking trends into the new millennium

If you've ever used a cell phone or watched a TV show, you've used a network, perhaps without even realizing it. Much of the world's modern communications infrastructure, including wired and wireless telephones, cable and broadcast TV, and the Internet, depends on networks.

Windows Server 2003 needs a network, too. Because servers exist to provide file, print, directory, Web, security, and other services to clients across a network, using Windows Server 2003 without a network is like using a telephone that's not plugged into the wall. Although that phone may have some value as abstract art, its real value comes from its capability to connect you with other people or services. The same is true for Windows Server 2003.

In this chapter, we introduce you to the various components that make up a Windows Server 2003-based network and briefly discuss how each one works.

What's This about a Network?

A *network* requires at least two computers linked in a way that enables them to talk to each other. Most networks use electrical wires of some type to convey signals and data between computers. However, numerous types of networking media, including wireless technologies and fiber-optic cables, also support networked connections. In other words, you can get from here to there in many ways on modern networks!

A network's key ingredients always include some type of physical connection that allows computers to talk (and listen) to some kind of communications medium. Even if that network medium is wireless, something must physically connect computers to an antenna or to a similar device that allows those computers to broadcast and receive signals.

But there's more to networking than hardware. Although cables and connections are essential, they are purely decorative and can serve no useful purpose without software. In the following sections, you find out a bit more about the hardware and software that make networks work.

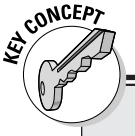
No hardware means no connections!

First and foremost, networking requires working connections to enable computers to communicate with each other. *Networking hardware* creates connections between computers and a network and defines the medium (or media) that allows information to flow from sender to receiver.

Networking hardware covers a broad range of devices, many of which you may find on your networks. In the first part of this book, we help you understand the roles and functions these devices play on a network.

From the most basic perspective, computers need the following hardware to talk to each other on a typical network:

- **A network interface card (NIC)** plugs into a computer and attaches to a network cable (or other medium, if something else is used). It turns computer bits into signals on the wire for outgoing stuff and turns incoming signals into bits for incoming stuff.
- **Connectors** make it possible to attach a network interface to the network medium. For wireless media, connectors attach antennas or other broadcast devices to interfaces. Connectors bring all the separate pieces of networking hardware together, so to speak.
- **Cables** convey signals from sender to receiver, using either electrical signals for wire cables or light pulses for fiber-optic cable. In the case of wireless media, the medium consists of the broadcast frequencies used to transmit information between senders and receivers.
- **Additional network devices** tie bigger, more complex networks together. These devices range from relatively simple hubs used to interconnect interfaces on star-wired networks (see Chapters 4 and 7) to repeaters used to link individual cable segments, as well as bridges, routers, and gateways (see Chapter 7). Hardware plays an important role in networking. Not only does it attach computers to a network, but it also interconnects multiple networks to manage how and when data flows from one network to another.



A simple view of networking

Networking boils down to these three critical requirements:

- **Connections** include the necessary hardware to connect a computer to a network, plus cables (called the *network medium*) that ferry messages between computers. The hardware that hooks a computer to a network is called a *network interface.* In most cases, attaching a PC to a network requires inserting an adapter board called a *network interface card (NIC).* Without a physical connection, a computer can't use the network.
- **Communications** define rules that computers must follow to exchange and interpret information. Because each computer may run different software, interconnected computers need a shared language to enable them to exchange messages and data. Without shared communications, computers can't exchange data, even though they may share a common network medium.
- **Services** are what computers talk about. In other words, services represent what computers do for each other, including sending or receiving files, messages, print jobs, and so on. Unless computers can perform services for each other across a network, a computer can't respond to requests from other computers, nor can it request things from other computers.

Without software, networks don't work

Software lets computers access and use hardware, whether that hardware is used for networking-related functions or for other purposes.

By now, you should understand that hardware provides the necessary connections that make networking possible, and software supports the communications and services needed to access the hardware and the network to which the hardware is attached.

Many different types of software play a supporting role when networking modern computers. This software includes special-purpose programs called *device drivers,* which allow a computer to address a network interface and exchange data with that interface. The software collection also includes full-blown applications that can access data on a local computer or on a server across the network with equal aplomb. The software also includes a bunch of other stuff that sits between device drivers and applications.

Throughout this book, we show you how to recognize the various pieces of software involved in networking and how to best configure that software to work with Windows Server 2003 on a network.

Investigating Your Network's Facilities

If you tour an average network, you can't help but discover that many different types of equipment and a variety of related software are in use. If you inventory all the components in a network, you can use that data to figure out what's attached to your network and what functions various devices perform on your network.

The infrastructure that makes networking possible is made up of the equipment that hooks computers into a network, the cables or other networking media that ferry information between computers, and the hardware and software used to create and control a network. You may also call the collection of connections, cables, interfaces, and other equipment *glue* because these elements bind computers into a working network.

The three phases of networking

Network software falls into one of three categories: host/terminal, client/server, and peer-to-peer. Each category reflects a certain type of networked communication.

- **Host/terminal networks** are based on an old-fashioned model for networking, even if they don't use old-fashioned stuff. In this network's original version, users access information using a device called a *terminal,* which consists of nothing more than a screen, a keyboard, and a network connection. All the software runs on a powerful computer called a *host,* which resides elsewhere on the network. The lowly terminal doesn't do anything more than provide a way for users to access remote data and applications (which is why such devices are also known as *dumb terminals*). In more modern versions, PCs can act like terminals by using *terminal emulation software,* which the PC uses to access a host. The PC still provides some local smarts and access to local word-processing software, spreadsheets, and so on. In fact, Windows Server 2003 supports host/terminal capabilities through a facility called Terminal Server.
- A **client/server network** consists of a collection of smart machines. One or more of these machines acts as a server and has lots of storage space, a powerful processor, and networking software so it can handle requests for services from other machines. The other machines that interact with the server are called clients. Sometimes, client/server networks are also called *server-based networks* to emphasize the server's key role. Windows Server 2003 provides a foundation for the client/server network, which is the subject of this book. However, Novell NetWare and UNIX servers also play similar roles on modern networks.
- On a **peer-to-peer network**, any machine that can be a client can also act as a server. Unlike client/server networks, no special-purpose machine acts as a server. On a peer-to-peer network, all machines are more or less alike in capability and in the services they offer. If you use the built-in networking included in Windows XP Professional, Windows 2000 Professional, Windows NT Workstation, or Windows 95, 98, SE, or Me, you're using this type of networking software.

Workstations for everyone!

One of networking's primary advantages is that a network takes what you do at your desk — and we bet you usually call it "work" — and lets you do what you do more efficiently by allowing you to interact with remote resources and data. This means you can access a file on a server as if it's part of your own disk drive, send a job to a printer elsewhere on the network as if it were hooked directly to your machine, and so on. Sharing resources remains the most highly touted benefit of networking because it connects your desktop computer to file stores, printers, applications, and information resources that would otherwise be inaccessible or too expensive to add to every desktop computer.

The terms *network client, desktop computer,* and *workstation* are all used more or less synonymously in the networking world. No matter what you call them, these machines are where users do the bulk of their work (and perhaps some play at odd moments).

A *desktop* is also the area of a computer that displays the program icons and the wallpaper.

One of the key goals that drives networking is to interconnect all the desktops in an organization, whether they run a DOS, Windows, UNIX, Linux, or Macintosh operating system, so that they can communicate and share resources. Some of the resources shared by workstations include large disk arrays, expensive color or laser printers, CD-ROM jukeboxes, and high-speed Internet connections (all of which would be too expensive to connect to every desktop machine).

On most networks, the ratio of desktop machines to users is pretty close to one-to-one. In other words, each user has access to a workstation attached to the network, even if that user is not the only person who works on that machine. Because workstations are where requests for services originate, such machines are known as network clients, or more simply, as *clients*.

When you call such a machine a *workstation,* you emphasize its capability to support an individual user more or less independently. When you call such a machine a *client,* you focus on its connection to the network. Whatever you call it, it's a machine that sits on your desk and is connected to a network.

A server is always at your service

Networking is about obtaining access to shared services. Because networks are useless unless you can do something with them, access to services is what networking is all about.

On modern networks, servers provide the capabilities necessary to obtain access to resources or to do things. For example, when you send a print job to a networked printer, you can assume that, somewhere in the background, a print server is handling the job. Likewise, when you request a file from a network drive, a file server is probably involved. When you poke around in the network directory — you guessed it! — a directory server is pulling the strings. For every service, some type of server handles and responds to requests. Sometimes, a single server provides many services; at other times, a server provides only a single service.

Computers that provide services to clients are generically called *servers.* A server's job is to listen for requests from clients for whatever service or services it offers, and to satisfy any valid requests for its services. In fact, validating service requests is an important part of what servers do — you wouldn't want just anyone to be able to print the salaries for everyone in your company just because a user asks a print server to do so. You want that server to verify that Bob is *allowed* to access that file before you let him print it! Throughout this book, you find out more about such validations and other key aspects of what it takes for a server to provide services.

The common path of networking

A common pathway must exist between any computer that requests services and any computer whose job it is to satisfy such requests. Just as you need a highway to drive from one city to another, you need a pathway over which your computer can send and receive data. On a network, that's the job of the media that tie all the various pieces together.

Look around and observe the types of cables and connections used on your network. Get a sense of the structure of your network so you can tell which highways the users use — from the side roads that only the folks in the accounting or shipping department use to the main road that all users use.

When you observe how all the pieces fit together — workstations, servers, and media — you get a reasonably complete view of your network. Figure 1-1 depicts a simple network diagram that shows these purely physical elements of a network. Notice that clients (desktop machines) outnumber servers, and that media tie all the pieces together. Networking follows the law of supply and demand, so the more clients you have, the more (or bigger) servers you'll need — and the more work will get accomplished!

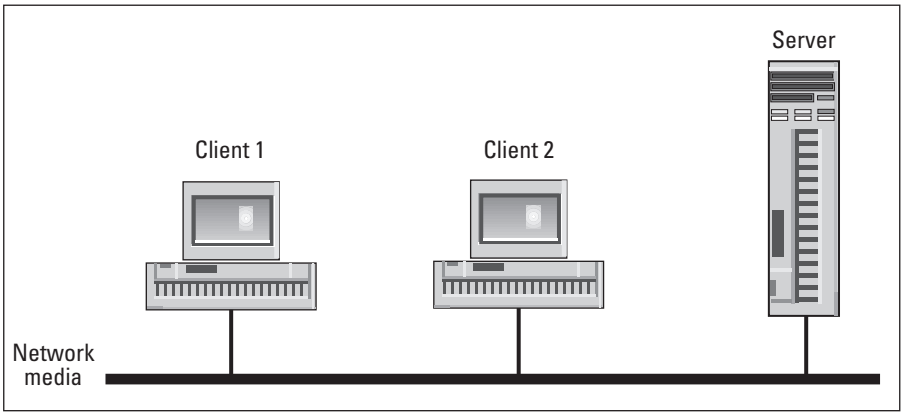


Figure 1-1: A typical network with clients, a server, and infrastructure (or network media).

What Is the Sound of a Working Network?

Figuring out whether a network is functioning is both easy and hard, and most observers, including novices and experts alike, agree that telling when a network's *not* working is easier than telling when it is! A client must know how to ask for services from the network and must state precisely what it's requesting. Likewise, a server must know how to recognize and evaluate incoming requests for its services and how to respond appropriately. Only then can a network work correctly.

Understanding how this constant stream of requests and replies works means looking a little deeper into how clients state their requests and how servers satisfy them. In the following sections, we examine the mechanics of this give-and-take.

Knowing how to ask is where the game begins

Knowing how to ask for network services requires some ability to distinguish between what's available locally on a client machine and what's available remotely from the network. Determining what's local and what's remote is the key to handling network access correctly. This determination depends on specialized software to handle the job in the background, so users don't necessarily have to know the difference.

A computer's main control program is called its *operating system (OS)* because it defines the software environment that lets a computer operate and run the applications and system services that get things accomplished on a machine. Most modern operating systems include built-in networking capabilities to augment their control over local resources and devices.

Certain modern operating systems can be called *network operating systems (NOSs)* when they create network server environments. Their built-in networking capabilities include a range of network services as part and parcel of the underlying operating system. Windows Server 2003 certainly fits this bill because it offers a broad range of powerful, flexible networking capabilities.

Right out of the box, Windows Server 2003 understands the differences between local and remote resources. The same is true for most modern desktop operating systems, including Windows XP Professional, Windows 2000 Server and Professional, Windows NT Server and Workstation, Windows 9*x,* the Macintosh OS, as well as that old (but still modern) warhorse, UNIX.

In Windows Server 2003, Windows XP Professional, Windows 2000, Windows NT, Windows 9*x,* Macintosh, and UNIX operating systems, and through add-ons to DOS and Windows 3.*x,* a special piece of software known as a *redirector* keeps track of what's local and what's remote when users or applications request resources. The redirector takes generic requests for services and sends any that can't be satisfied locally to the appropriate service provider elsewhere on the network (in other words, to the appropriate server). Therefore, if you ask for a file that resides on a server elsewhere on the network, the redirector hands your request off to that machine and makes sure that the results of that request are delivered properly.

What's on today's menu?

For a computer to use network services, the computer must know how to ask for them. That's what a *requester* does. But knowing what to ask for is as important as knowing how to ask. In most cases, applications supply the necessary information about network services that they want to access, either through information supplied from a requester or through knowledge built directly into an application itself.

E-mail clients and Web browsers represent good examples of applications with sophisticated, built-in networking capabilities. On the other hand, file system access tools, such as Windows Explorer, My Computer, and My Documents, rely on the redirector to furnish them with views of (and access to) shared files and printers elsewhere on the network.

Please note that applications with built-in networking knowledge offer *transparent* access to network services because the applications know how to ask for services and, often, what to ask for on the user's behalf. Programmers design such computer applications to be transparent to keep the applications out of sight and out of mind; therefore, the user remains blissfully unaware of cumbersome networking details and trivia. File managers, printer controls, and other tools with access to both local and remote resources, however, require users to be able to tell the difference between what's local and what's remote. In fact, such tools usually force users to request access to remote resources explicitly and directly.

Increasingly, finding out which services a network can provide is becoming more and more implicit. This is why all editions of Windows Server 2003 support a set of directory services to catalog and describe the services that the network can deliver to its users. Likewise, Windows Server 2003 supports the Distributed File System that allows directories on multiple machines all around a network to appear as a single network drive to users. Therefore, users don't have to know where individual files or folders reside.

Such sophisticated mechanisms make it easier than ever before for users to request and access resources implicitly without having to know how to request those resources or having to determine exactly where they reside. Nevertheless, some explicit knowledge about such things is necessary if you want to make the most of Windows Server 2003's networking capabilities.

It's All about Sharing Resources

The mechanics of requesting resources depend on having access to the right software tools to determine when network requests are necessary. The software delivers the request to a server whose job is to listen for such requests and to satisfy all legitimate ones. Ultimately, a server's job is to make resources available to all authorized users. This feature makes sharing possible and helps explain the most powerful benefit of networking — namely, to provide a single, consistent way for multiple users to obtain secure and managed access to files, printers, scanners, data, applications, and more.

The secret to sharing is to find a way to make sure that everyone can obtain access to a shared resource. For example, for access to print services, a temporary storage space must hold incoming print jobs until each one's turn to be printed comes up. Therefore, sharing a printer means not only providing access to the device itself, but also keeping track of who's in line, providing a place where pending jobs can reside, and sometimes notifying users when a print job has been successfully completed. All these mechanisms make sharing work easier and explain why servers are so important to any network.

Because servers bring services and data together in a single machine, servers provide a natural point of control and maintenance for the important devices, services, and data on a network, which are, of course, the things that everybody wants to share.

Windows Networking Trends

Microsoft is leaping into a new era in which local networking and Internet access is integrated unlike ever before. Windows Server 2003 is Microsoft's next step toward a goal of end-to-end communication structures that enable companies and individuals to electronically communicate easily, efficiently, and securely. Windows Server 2003 is built on technology from Windows 2000, which in turn was built on technology from Windows NT. The Windows Server 2003 family embraces several types of servers, including the following:

- **Windows Server 2003, Web Edition:** A server system optimized for Web serving and hosting. This edition supports up to four processors and 2GB of RAM per computer.
- **Windows Server 2003, Standard Edition:** A server designed to replace Windows 2000 Server. It can be used as a member server or as a domain controller on small to medium-sized networks. The Standard Edition supports up to four processors and 4GB of RAM per computer. It is also the subject of this book.
- **Windows Server 2003, Enterprise Edition:** You can think of the version as Windows Server 2003, Standard Edition with lots of bells and whistles. This souped-up version allows you to use up to eight CPUs (processors) and up to 32GB of RAM on a single server (which helps improve performance). Windows Server 2003, Enterprise Edition supports up to eight-node clustering (combining two or more computers in such a way that they all share the workload to support a single, large application or network service).
- **Windows Server 2003, Datacenter Edition:** This is a high-end Windows operating system that supports even more CPUs and RAM than Windows Server 2003, Enterprise Edition (up to 64 CPUs and 64GB of RAM). It has the same features as the Enterprise Edition, plus more. Windows Server 2003, Datacenter Edition can support more than 10,000 simultaneous users in certain situations and up to eight-node clustering.

There are also versions of Windows Server 2003, Enterprise Edition and Windows Server, Datacenter Edition designed for the Intel 64-bit Itanium CPU.

Although these versions vary, they're more alike than different. Therefore, this book can help you master the basics for any of these types of Windows Server 2003 products.

Based on the capabilities of Windows Server 2003, we see the following trends emerging for Windows networking in this millennium:

- **Use of Active Directory:** Active Directory is Microsoft's name for the directory services supported by Windows Server 2003. Active Directory makes it easier for users to identify and access network resources and for applications to use such resources directly and automatically. Currently, you can't see much evidence of this capability, but it will change the way we use Windows — and networks — in the future.
- **Access to dynamic disk storage:** Windows Server 2003 supports a variety of sophisticated directory-sharing technologies. Dynamic disk storage enables network administrators to define collections of files and directories gathered from multiple servers around a network and present them to users as if the files and directories reside on a single network drive. This makes creating, identifying, and accessing collections of shared files easier.
- **Consistent naming services:** Part of locating resources on a network is knowing their names (or how to find them). Windows Server 2003 uses a single enhanced method to translate human-intelligible names for network resources into computer-intelligible network addresses, which makes managing and interacting with network resources far simpler.
- **Web-based management console:** In Windows Server 2003, a single Microsoft Management Console (MMC) plays host to management tools (called *MMC snap-ins*) for all system services, resources, and facilities. This console makes the Windows Server 2003 interface simpler and its many capabilities more visually consistent and therefore easier to learn and manage. In fact, this capability works on any computer with a suitable Web browser (and an administrative password).
- **Simplified Web content creation and delivery:** One of the primary goals of the Windows Server 2003 family is to bring high-end, high-profit Web services and applications to end users (that is, customers) in an efficient manner. Through the use of optimized Web tools, new programming language structures, and content development architectures, Windows Server 2003 is poised to revolutionize how enterprise Web sites are created, deployed, and maintained.

As all these capabilities are used, the trends in Windows networking should be clear:

- Easier, more straightforward access to network resources
- Simplified administration and management of such resources
- More sophisticated tools and technologies to describe, deliver, and control network resources

Get used to it!