Network Fundamentals

	NEWBIE	SOME EXPERIENCE	EXPERT
ETA	4 hours	2 hours	1 hour

This chapter takes you gently into the wonderful world of networking so that you can read the following chapters with some fundamental knowledge already in place. If you think you already have enough basic network experience, you can skip this chapter, but then again, a little refresher on the basics (*especially* the OSI seven-layer model) may not be a bad idea—and the chapter is not long!

Big or small, networks all serve the same purpose: to share things, whether it's disk space on a server, a printer, or an e-mail system. Networks enable more than one user to access shared resources. Back in the late 1980s, the average size of a network was often quoted to be eight users, and the main reason for the original growth in PC networking was to share expensive laser printers—sometimes just *one per company*! Today, we see networks that span the globe as well as humble two-machine setups for research purposes (otherwise known as death-match gaming). Every desktop operating system (such as Windows 9*x*/2000/XP) has built-in networking capabilities, which means that you can network nearly every PC today, without resorting to expensive software to make the network work.

So what's involved? Well, you'll probably need some equipment to link together, and since we're focusing on the Network+ exam, we'll do the same as the exam authors and concentrate on PC networking. Ready…?

Objective 1.01

Overview of Network Hardware

We need to begin with some hardware on our network (see Figure 1-1), the most obvious example of which is a PC. There's usually no problem linking together supposedly incompatible systems. For example, it's quite feasible to work on a PC running Windows 2000 while your data and programs are stored on a corporate minicomputer running a different operating system, such as UNIX or Linux or one of their close relatives. This is real corporate networking, and the fact that you are using a non-PC platform to store your data is handled by the networking software and hardware. All you see, for example, is another drive letter on your computer—maybe W: for word processing—and that's it!

Clients and Servers

Networks have two categories of computers: those that access the networked resources (clients) and those that provide the resources (servers).
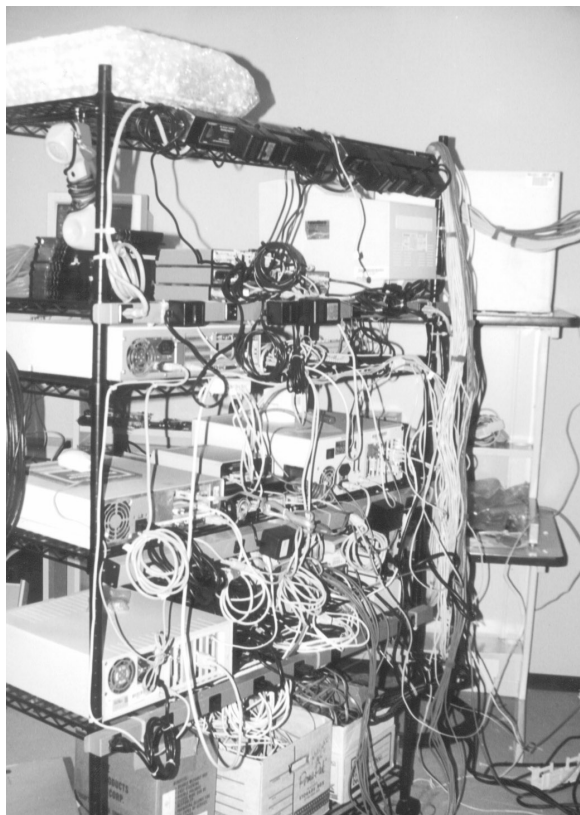
FIGURE 1-1   A typical pile of networked hardware

Clients

Any PC or other computer system that makes use of network resources is a *client*. In the old days, we might have called them workstations, but the correct, modern term is client. Some may say *terminal*, but that really refers to a screen and keyboard-only setup (no processing power, no Windows!) used for working with mainframes and minicomputers that do all the thinking for you.

Local Lingo
client   A computer system that makes use of shared network resources.
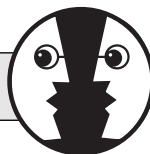
Almost any PC can be a client, provided that you can somehow attach it to the network and run the software needed to get it communicating. Networking a PC won't make it more powerful, but will allow it to use resources situated elsewhere in the building, or perhaps halfway round the world.

Servers

Servers manage the network's shared resources. A small network may have only one server, but a corporate setup may have dozens, each performing a specific task. For example, one server may hold the network's disk space, and another may manage the printer. A third server may provide access to the Internet while also acting as a firewall to keep out unwanted hackers trying to probe around your network. Ultimately, the number of servers on a network depends on the workload the network is going to face and whether one server can cope. Later chapters will discuss how networks behave under load and what can be done to keep things running smoothly.

Local Lingo

server   A computer system that provides and manages shared network resources.

Servers have a sense of duty and will try to protect your resources from unwanted access. Every major network operating system (NOS), such as Microsoft Windows NT Server, Novell NetWare, UNIX, Linux, and other variants will expect every user trying to access their resources to provide a valid user name and password. Other common features include the ability to restrict a specific user's network access to one or more machines or to only during certain days or times.

Exam Tip

Purists may argue that UNIX and Linux are not network operating systems but multiuser operating systems—originally used via a dumb terminal and with centralized storage and printing—that now also happen to support network interconnectivity to client PCs and other servers. Fair enough, but they are certainly networkable and, especially in the case of Linux, can be configured to present themselves on a network as if they are servers.
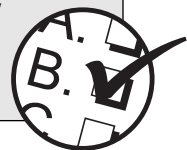
Client/Server Networks

For most medium to large business networks (it's difficult to give a figure but, say, a system with more than 10 clients), a dedicated server is usually the norm, giving us what's referred to as a *client/server* or *server-based* network (see Figure 1-2). The main point here is that the server has a specific role to play (it's a server!) and will be tucked away safely (maybe in a computer room) and left to get on with its job—you won't find someone sitting at the server running Microsoft Word or Quake III. The only time the server will see user activity at the keyboard is when an authorized person performs some administrative task, such as installing a program update, running a tape backup program, or perhaps checking the server's log files when an unexpected event occurs.

OK, so you have a PC on your desk; is it a client or a server? Ha, trick question! You can't tell just by looking—it could be either. Read on, and all will be revealed.
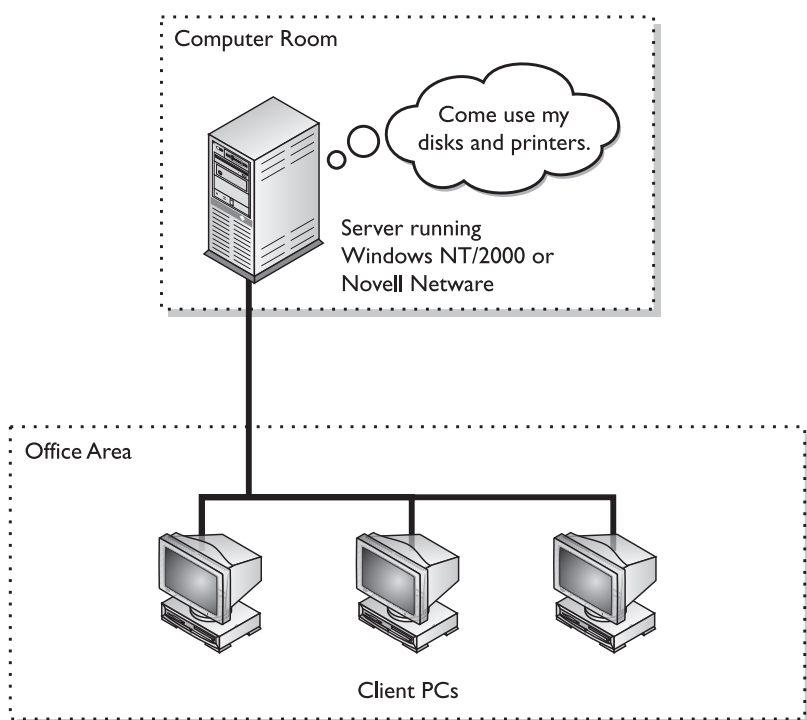

**FIGURE 1-2**   Some clients and a server

Peer–to–Peer Networks

Although traditional networking has always involved dedicated servers, you could almost always find specialized software to enable clients to share certain resources. Novell Personal NetWare, for example, enabled DOS-based clients to share disk space and printers. Since Microsoft introduced Windows for Workgroups, with its built-in server capabilities, all subsequent desktop computer operating systems—including Windows NT Workstation, 95, 98, 2000, ME, and XP—have supported some form of client-based sharing. These products enable machines to act as clients or servers, or as both at the same time. Every machine is the same in this respect, and we say that they are all peers (equals) because you don't need a dedicated server. Too good to be true? Yes and no!

So-called peer-to-peer networking (see Figure 1-3) is ideal for small offices or groups of people who need to share a printer or two (you can do this and still be part of a bigger client/server network), but running a PC as both a client and a server is hard work, and the system will slow down rapidly as other clients access its shared resources. There are other issues with peer-to-peer networking as well. What happens if someone switches off the PC at the end of the day while others are still accessing it? Security on such a network is not too great either. Although it is true that you can control access to your disk through the shared network connection, if your PC is in the middle of the office and someone wants your data, that person can just walk over and get it directly from your PC (if you haven't locked it). That's not so easy to do when you have a dedicated server in a secure computer room. Data control is another problem with peer-to-peer networking if you have several PCs all sharing their disk space. Since it's easy to lose track of where something has been saved, multiple copies of the same document or file are virtually inevitable. Using a dedicated server provides one central point for storage—and there's probably someone tasked with making regular backups, too.
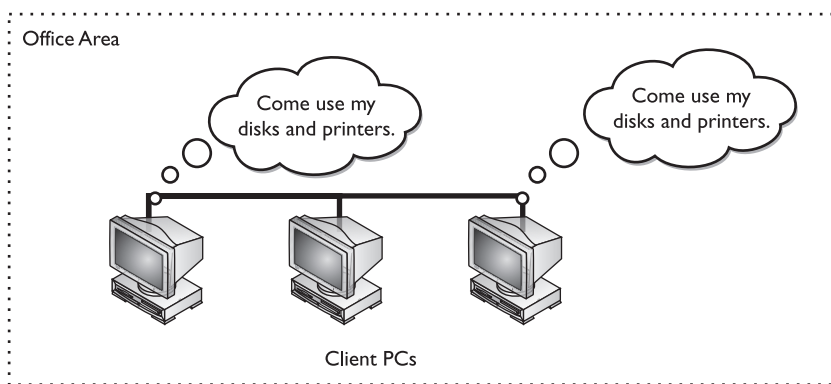
Exam Tip

Peer-to-peer networking is ideal for small workgroups, but offers limited security and is easily disrupted by computer shutdowns.
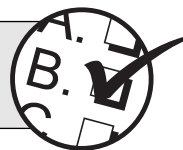
Local Lingo

peer-to-peer networking   Sharing resources among networked client systems which can also act as servers, so no dedicated server is needed.

FIGURE 1-3   A peer-to-peer network

Linking It All Together

Our network will not work very well unless we have some way of getting data from the server to the clients. We need a communication channel and a way of connecting our computers to it—in essence, the core network components themselves. Later chapters will elaborate, but the basics are as follows.

Network Wiring (and the Rest)

The vast majority of the network that you see will be in the form of copper cabling, snaking from the back of your PC down the back of the desk to a socket in the floor or wall, or perhaps just on into the distance somewhere. There are a number of network wiring types, each with its own characteristics, speed, length limitations, and restrictions. You may find that your network uses one type of wiring in one area and something completely different in another area, depending on the age of the installation and the cable type chosen to match the requirements at the time. Networks can also use other forms of "wiring" such as optical fiber, infrared, and wireless, for starters. Clearly, some of these wiring types don't use wire at all, so we use the term *network media* to encompass all varieties. Figure 1-4 shows one type of network wiring called unshielded twisted pair, or UTP. There's more about network media in Chapter 2.

Network Interface Cards (NICs)

A NIC is the plug-in (or built-in) interface between your computer system and the network media. Every client and server must have at least one NIC (yes, a system
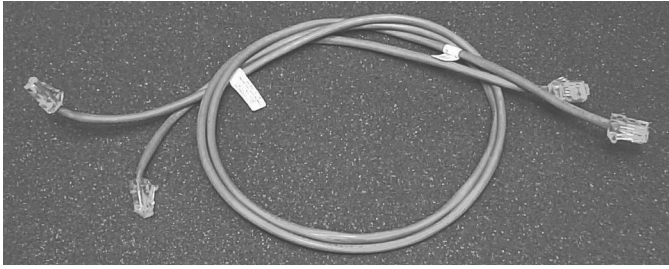
FIGURE 1-4   UTP wiring (patch leads)

can have more than one under some circumstances), and the NIC must be compatible with your computer system, the network media, and the way in which the network passes information. If it isn't, your PC isn't going to do much networking! Although some modern PCs have built-in NICs, you still may need a regular, plug-in NIC if, for example, the onboard NIC develops a fault, and it's too expensive to have the whole system board repaired or replaced. Figure 1-5 shows a typical NIC.

Network Equipment

A network often needs to grow beyond one or more limiting factors. For example, some network cable types can support only a certain number of machines on a single length of cable, or only a certain length of cable per network segment. Or maybe you need to join your network to another network at a remote site. For
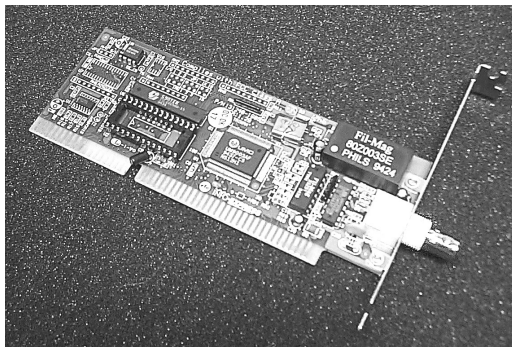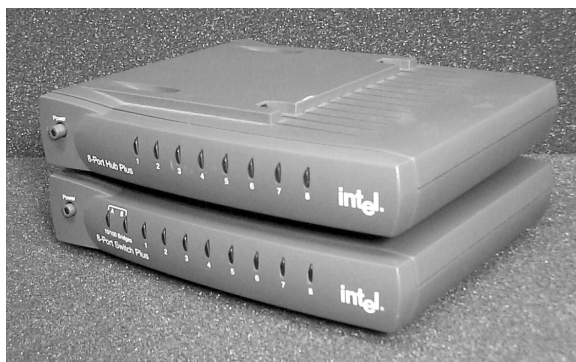

FIGURE 1-5   A typical NIC

A network hub and switch

most problems of this type, the solution usually involves adding modules or pieces of equipment that enable your network to handle more machines or greater distances. These devices have names such as repeater, hub, switch (see Figure 1-6), bridge, and router. As you'll see in Chapter 4, you can choose among many devices to help solve your problems, but there will always be one that's more suitable than the others (probably for cost reasons). We'll explore later what these devices are and what they do.

Objective 1.02

Overview of Network Software

O K, the network's in place, and you've bought the hardware and installed the network cabling. Now you're reaching for the software…

We've already mentioned the mainstream, server-based networking products such as Microsoft Windows NT Server and Novell NetWare, and we've told you about the peer-to-peer functionality built into most desktop operating systems. This section expands on these discussions and describes the component parts that must be installed and configured correctly to make your computer system work properly on a network, whether it's as a client, a server, or a peer-to-peer machine. In many cases, the basic installation of these software components is automatic, and everything you need is actually supplied with your operating system. For example, Windows 9*x* or 2000/XP can detect that you've added a NIC and install all the right drivers—the amount of input required from you may be minimal.

NIC Driver

Nothing's going to happen if you can't send and receive data through the network. The NIC is connected to the network media, and the server or client software probably comes supplied with suitable drivers. If it doesn't, just reach for the disk supplied with the NIC or perhaps visit the manufacturer's web site to download a suitable driver. A visit to the web site is generally a good idea in any case, just to make sure that you are using the latest driver.

Protocol Driver

Once you have the right NIC driver installed, you need to consider the language—or *protocol*—that the network will use to convey the data. Over the years, various protocols have been developed, and you need to ensure that the client and server PCs (yes, and peer-to-peer systems) all speak the same language. If they don't, you won't be able to see some or all of the resources potentially available on the network. To complicate matters, you may need to ensure that the systems support more than one protocol—this is true when you have a mix of systems services on the network, and there's no common protocol that fits them all. The main communication protocols referred to on the Network+ exam are NetBEUI, IPX/SPX, and TCP/IP, and there's much more about these in Chapter 5.

> **Local Lingo**
>
> **protocol**   A standardized way of performing a specific action, such as communicating across a network or exchanging information.

Client and Server Software

If you're installing one of the major network operating systems (NOSs), then a lot of the files copied from the installation CD represent parts of the core NOS—the *server software*. On the other hand, if you're working on a client PC running, say, Windows 98 SE, then the client and server software services are actually just modules that need to be enabled and configured using the Network applet in the Control Panel. And, as we said before, you might find that most of this is done automatically anyway. Did you notice that we mentioned "Windows 98 SE" and

then "server software"? Surely Windows 98 SE is used for *client* PCs and not servers? True, but don't forget that to be a peer-to-peer machine, a client PC also needs to act as a server, so Windows 98 SE (and 95, 2000, ME, and so on) comes with a *File and Printer Sharing* service module.

Redirector

One important role played by the client software is to provide an interface between the resources of the network and the functions of the host PC's operating system. This means, for example, enabling a network storage location to appear as a driver letter (say, W:), or a shared network printer to be accessed from a PC by printing to LPT2, even if the PC doesn't actually have a physical second parallel port. In networking terms, this feature is called *redirection* (Novell also uses the term "requester"). You simply refer to a resource by a drive letter or port that's not alien to the operating system, and before the OS has a chance to realize that W: or LPT2 doesn't actually exist, the client software has already stepped in and redirected the request to the relevant network resource.

Exam Tip

Client software is also known as redirector or requestor software.
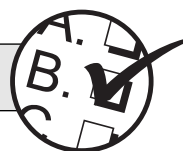
Now That We Are Whole...

To summarize, there are three main software components that must be installed and configured correctly to enable a PC to run on a network (see Figure 1-7):

- NIC driver
- Protocol driver(s)
- Client/server services

Once you have these core components in place, the operating system and applications can make use of (or provide, in the case of a server) network resources.

If you look at what's been covered to this point, you'll notice that the focus has moved from the media, to the network card, to protocols, to the client/server software, and then to the operating system and applications—a clear progression in layers of functionality.
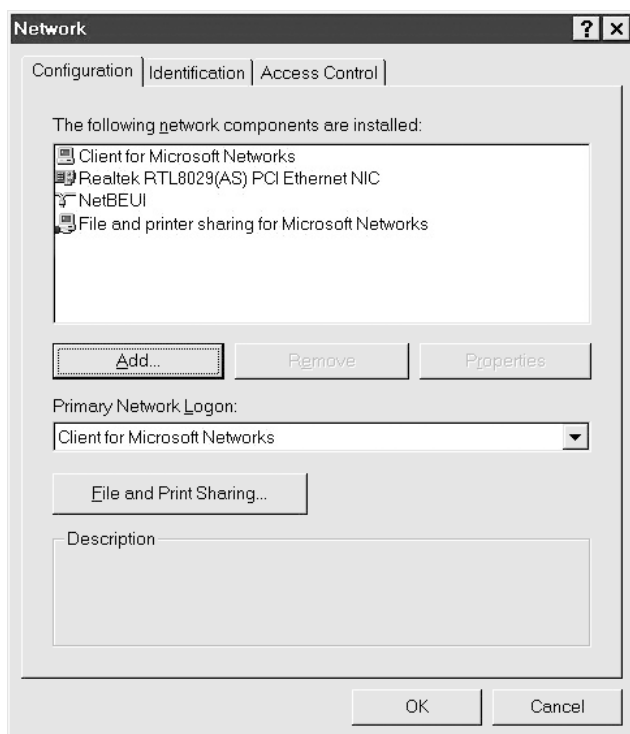
FIGURE 1-7   A Windows 9*x* machine with a client driver, NIC driver, protocol, and file and printer sharing service installed

Strangely enough (almost as if we'd planned it!), there is an industry standard way of describing how networks and their hardware and software function with reference to a model that has seven layers of generic functionality: the so-called OSI seven-layer model, which will be discussed in this book quite soon. But first…

Objective 1.03   Data Packets

The fundamentals of computing are all about data: moving data, storing data, processing data, and transmitting and receiving data. Networks rely on data, too, and so, before we move on, we need to talk about the facts of (data) life.

Consider a data file: it can be small, like a 200-byte text file, or big, like a 20-megabyte database. In either case, we want to be confident that when we click Save, our data makes its way safely to the server. In addition to application data, our networked PC is also going to send data codes with special meaning to our servers—instructions such as: "Log me in, my user name is…," "Here's my password…," "Send this to SALES_LASER02." (In reality, these requests won't be encoded in plain English, but in binary data sequences that are understood by the NOS.)

We know that all of this data is going to travel through our network media, but we need to understand a little about *how* this is accomplished for various other principles in this book to make sense. So here's a breakdown of how it works:

- **Networks carry data in packets**   The data in our 20-megabyte database is just a series of binary ones and zeroes. If we just throw all this data onto the network, no other machine is going to know what it is, where it came from, or where it needs to go. We need order—we need *packets*!

    A packet (or *frame*) contains some or all of the data we want to send across our network. If we're sending only a few bytes, such as our 200-byte text file, then it might all fit in one packet, but our database certainly won't. Because of the way that networks operate, they can carry only data packets that are between certain sizes, with typical packet sizes ranging from 1,500 to 4,000 bytes, according to the network technology being used.

    Think of a packet as an envelope into which you can stuff just so much paper. It's a carrying mechanism in a standardized format that's recognizable by every device on the network.

- **Packets need addresses**   You probably wouldn't post a letter without writing an address on the front of the envelope, and we certainly won't put a packet of data on a network without stating where it's supposed to go. In fact, a data packet contains both the recipient's and the sender's addresses so that the recipient knows where the packet came from, or in case there's a problem, how to contact the sender.

- **How big is that packet?**   A packet can contain any amount of data within predefined limits. Every data packet includes a note of how much data it actually contains. Among other things, this aids in error checking because the recipient can determine whether the packet that has just been received is complete.

- **What protocol is this packet using?**   We already know the names of three network protocols: NetBEUI, IPX/SPX, and TCP/IP. Every basic network packet includes a protocol ID field to help devices on the net-

work determine how to decode and understand the contents of the packet. This field also makes it easier for network devices to pay attention only to packets formatted using a protocol they support.

- **That packet looks unwell!**   It's a hard slog through all the media from your PC to the destination device, and data packets can be corrupted along the way by electrical interference, loose connectors, power glitches, and a host of other events. To help detect dodgy data packets, each packet includes a cyclic redundancy check (CRC) value that's computed by the sending device using the data in the packet. The CRC value is the result of a complex binary mathematical calculation on the data that is performed by both the sender and the recipient of the packet. If the CRC in the packet and the locally generated CRC don't match, then something's wrong, and the recipient will ask for the packet to be resent.

Figure 1-8 shows the format of a basic data packet.

Packet Summary

Data packets contain important pieces of information. The main ones are listed here:

- The sender's address
- The recipient's address
- A protocol ID
- A data length field
- The data
- A CRC value

> **Exam Tip**
>
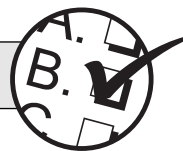> Data is carried around networks in packets (frames).

Source Address	Dest. Address	Protocol ID	Length	DATA	CRC

FIGURE 1-8   A basic data packet

The OSI Seven–Layer Model

Objective 1.04

This is the part of the course that strikes fear into many a network technician, but we're pretty confident that when you finish this section, you'll wonder what all the fuss is about! Honest!

The Open Systems Interconnect (OSI) seven-layer model was developed by a standards organization called ISO. Contrary to popular belief, ISO is not an abbreviation—it's derived from the Greek word for equal.

ISO wanted a framework into which the major network hardware and software components and protocols could be placed to give every item a common reference point: a means of relating the components and their functionality to each other and a way of standardizing some of the components and protocols.

Exam Tip

The Network+ exam expects you to know the layers by name (especially layers 1 through 4), how they function in relation to each other, and what they represent.
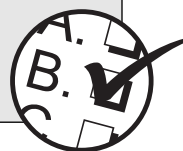
Each layer of the model represents a particular aspect of network functionality. For example, layer 1—the Physical layer—represents electrical signals, connectors, and media types and the way that data is placed on the network media.

For a simple example of how layers work, imagine that you're designing your own range of NICs, and you've gotten to the stage where you're choosing what connector type to use for the media and card interface. Off you trot to your local electronics store, where a simple, four-pin audio connector catches your eye. You finish your card design and send it to the manufacturer, but when the product hits the stores, it doesn't sell. That's because no one else uses that four-pin connector type on their NIC or media, and so no one can hook your cards onto their network. In addition, those who have tried to interface to your card were a bit shocked (literally!) to discover that your data signals use a 120-volt reference for binary 1 (in the real world, data signals on a network cable are a fraction of a volt).

What went wrong? You should have used a media connector type and an electrical signaling system that conform to the relevant OSI physical layer standards. Also, don't be surprised if you get sued by that technician with the smoking screwdriver and singed hair!

As well as helping to standardize the design elements of network components, the OSI model helps position and standardize network protocols with reference to one another. As you'll see, this is important because more than one protocol or action is needed to get your data onto a network (or, indeed, to do the reverse and pick up data from a network). For example, the "protocol" TCP/IP, in fact, refers to two protocols, TCP and IP, and these two protocols don't work alone. What do they do? Chapter 5 is where you'll find out.

To summarize, the OSI seven-layer model is a theoretical representation of how a networked device functions and helps us understand the interrelationships among hardware, software, protocols, and applications. Many network technicians refer to network devices by their positions in the model; for example, a repeater (a device mentioned earlier) is a layer 1 (Physical layer) device.

The Layers and What They Represent

Here's a run through the layers and an overview of their tasks and responsibilities. Figure 1-9 summarizes the layers and their functions.

Layer 1: Physical Layer

Layer 1 is responsible for defining the network standards relating to electrical signals, connectors, and media types and the way that data is placed on the network media.

Layer 2: Data Link Layer

Layer 2 is responsible for gathering together and completing all of the elements that make up a data packet and putting the whole thing together so that it can be passed to a Physical layer device and on to the network. The Data Link layer assembles outgoing packets and generates the CRC. For incoming packets, it checks the data for validity by comparing its locally generated CRC value with that sent in the packet. The Data Link layer also determines whether it is possible or permissible at any instant to try and send data to the network. At any instant, another computer

Layer	Functionality
7. Application	Network services, authentication
6. Presentation	Translation, encryption
5. Session	Connections, sessions
4. Transport	Fragmentation, defragmentation, reliable data delivery, error correction/management, flow control
3. Network	Addressing, routing
2. Data Link	Packets/Frame, CRC generation/checking, network access
1. Physical	Media, connectors, electrical signals

FIGURE 1-9   The OSI seven-layer model

may already be using the network. If you transmit data at the same time, both packets will become corrupted.

Layer 3: Network Layer

Layer 3 understands addressing—how to find the ultimate destination address for a data packet—and routing, to make sure the packet ends up in the right place.

Layer 4: Transport Layer

If the data being sent is bigger than the allowable packet size, the Transport layer breaks the data into smaller, manageable chunks that will fit inside two or more packets. Breaking up data into smaller chunks is also known as *fragmentation*. The Transport layer is also responsible for confirming whether transmitted packets have reached their destination intact (or at all) and retransmitting them if they haven't (error correction/management). For incoming packets, the Transport layer reassembles the fragmented data (performs defragmentation), carefully ensuring that received packets are processed in the right order. The Transport layer also

manages the flow of data to ensure that packets are sent at a pace that's suitable for the receiving device and for general network conditions. Sending data too quickly is like speaking too fast: you may have to keep repeating yourself to get the message understood, which is actually counterproductive.

Layer 5: Session Layer

Layer 5 sets up, manages, and terminates the data connections (called *sessions*) between networked devices. These sessions enable networked systems to exchange information.

Layer 6: Presentation Layer

Layer 6 is responsible for managing and translating information by catering to differences in the ways some computer systems store and manage their data. Presentation layer protocols are also responsible for data encryption.

Layer 7: Application Layer

Layer 7 represents the network-related program code and functions running on a computer system. This program code provides network support for the main applications being run, such as the redirector software discussed earlier, allowing a shared network location to appear on a machine as drive W: and providing services such as login authentication. Some application layer functions do exist as user-executable programs. Some file transfer and e-mail applications, for example, exist entirely on this layer.

Using the Seven-Layer Model

The seven-layer model is only a theoretical representation of how networks function. Although knowing it inside out won't change your life, it should help you pass the Network+ exam. The conceptual use of the model assumes that an event on one computer system (for example, a user pressing ENTER on a login screen) creates some data that sets off a chain of events. The data runs down through the layers on the sending machine and then leaves the system in a data packet, which travels across the network and then up through the layers on the receiving machine, until the data arrives intact at the application layer and causes something to happen. Later chapters in this book point out where certain key protocols and

hardware fit into the model, and this can be useful stuff to know for both the Network+ exam and real life. Be prepared for a shock, however, because some network arrangements and protocols don't fit exactly into the model and, under some circumstances, not all of the layers are actually used. Does this matter? Well, as long as your data gets from point A to point B successfully, probably not.
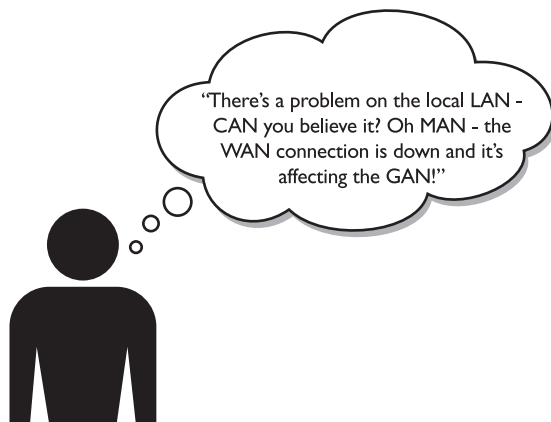
Objective 1.05 # Real–World Networking

Enough theory! Let's get back to the real world. You've a few more terms to absorb before you're ready to be let loose on the next chapter.

Network Size

You may have heard the terms LAN and WAN before, but did you know that there's a whole bunch of other *AN abbreviations that also describe the general size of a network (see Figure 1-10)? This section lists the main ones in order of size, with the smallest first.

By the way, network technicians often refer to every network they mention as either a LAN or a WAN. In practice this doesn't really matter unless you feel like correcting them just to see how they react.

"There's a problem on the local LAN - CAN you believe it? Oh MAN - the WAN connection is down and it's affecting the GAN!"

FIGURE 1-10 Terms to describe network sizes

Local Area Network (LAN)   A LAN is a single network confined to one building or area of a building. There may be links to other locations at the same site, but these will be very localized.

Campus Area Network (CAN)   CAN is a fairly new term, used to describe a group of interconnected LANs within a small geographical area, such as a school campus, university, hospital, or military base.

Metropolitan Area Network (MAN)   The term *MAN* is usually applied to networks that have a sociopolitical boundary; such as a network of district authority offices in a town or city. Sites on a MAN are usually interconnected using fiber-optic cable or some other high-speed digital circuit (rather than standard phone lines, for example), and the MAN itself may well carry voice as well as data traffic.

Wide Area Network (WAN)   A WAN is two or more interconnected LANs spread over a large geographic area, even on different continents. The Internet is the largest WAN in existence.

Global Area Network (GAN)   A GAN is a single network with connection points spread around the world. GANs are used mostly by large corporate organizations and consist of a series of networked, orbiting satellites. Note the subtle difference between a WAN and a GAN: the latter is a single network, not a number of interconnected networks.

Solar System Area Network (SSAN)   A SSAN is a series of interconnected GANs connecting all the habitable planets and planetoids in a single solar system…err…. Well, we'll see one someday!

> **Travel Advisory**
>
> These terms don't exist as official standards, but their use and definitions have become generally accepted over time.

Network Performance

Many factors affect network performance, but here we want to talk about just the basic speed of a standard network, how network speed is measured, and some of the terms related to performance.

Bandwidth

Network data speeds are measured in megabits per second—sometimes abbreviated Mbps. That lowercase *b* is important, because an uppercase *B* would imply mega*bytes*. For a standard corporate network, the speed at which data travels between networked systems will typically range between 4 and 100 Mbps, depending on the network standard used. In real terms, this means that a network link could easily work at about the same pace as a quad-speed CD-ROM drive—hardly blazing a trail, but this illustrates one key point about networking: it's not always about speed; it's about the ability to access shared resources.

So where does this word *bandwidth* come in? Well, the data signal traveling through the network media (usually some form of copper wire) is an electrical signal that's changing voltage rapidly to represent a string of binary data (remember our packets?). Any signal that changes in this cyclic way has a frequency associated with it—measured in Hertz (Hz)—which is known as its *bandwidth*. Your network media is designed to operate across a certain range of frequencies, or bandwidths, and if you try to push data through the network at a faster rate (exceeding your bandwidth), you will quickly discover that the laws of physics are not negotiable!

The bandwidth of the network is closely related to its maximum theoretical speed. So network technicians will often say things like "our network has a bandwidth of 10 megabits per second," when they really mean "our network has a top speed of 10 megabits per second," or "the bandwidth of our network provides a throughput of 10 megabits per second." For the purposes of the Network+ exam, all of these variations are considered to be correct and to mean the same thing.

Local Lingo

bandwidth   A term used to refer to the performance (speed) of a network.

CHECKPOINT

✔ **Objective 1.01: Overview of Network Hardware**   The most obvious pieces of network hardware are the computers on the network. These are divided into client and server systems unless they are desktop systems that are sharing resources, in which case they are known as peer-to-peer systems.

Corporate networks generally use dedicated servers because they offer higher performance, greater stability, and better security than peer-to-peer options. Your network won't be complete without some media such as copper wiring, fiber optics, wireless, or infrared to interconnect your systems, and a Network Interface Card (NIC) to connect your system to the media. Other devices on the network—such as repeaters, hubs, bridges, and routers—enable you to expand the system locally or to other sites.

✔ **Objective 1.02: Overview of Network Software**   The major software components of a network are the network operating system (NOS), NIC drivers, protocol drivers, and client/server services. Most of the components needed to get a network up and running are supplied as standard with your NOS or as part of your client operating system (Windows NT/9*x*/2000/ME/XP, Linux, and so on).

✔ **Objective 1.03: Data Packets**   To send a piece of data across a network, it has to be placed in a standard, formatted structure known as a packet or frame. These packets also state the source and destination addresses of the data, the protocol being used, and the amount of data being sent. A cyclic redundancy check (CRC) value is also added to the packet to enable the receiving device to check the packet for errors. If the packet looks faulty, the recipient will ask for it to be resent.

✔ **Objective 1.04: The OSI Seven-Layer Model**   The OSI seven-layer model describes how data flows from one networked system to another—it's a theoretical model into which many of the standards, components, and functions of a network fit. The model promotes the use of recognized network standards and helps ensure compatibility between network hardware and software from different manufacturers.

✔ **Objective 1.05: Real-World Networking**   Networks come in all shapes and sizes, and there are a number of de facto abbreviations that can be used to describe different types of networks, from small LANs to worldwide GANs. One of the key features of a network is its performance at the desktop (that is, the speed at which the client machines can send and receive data), which is usually measured in megabits per second. Accessing data across a network is not necessarily that fast compared to accessing the same data from a local hard disk, but this is far outweighed by the benefits of being able to share data and resources, such as printers, with a large number of clients. The term bandwidth is often used interchangeably with speed, although the two are not quite the same thing.

REVIEW QUESTIONS

1. What name is given to a computer that can act as both a client and a server? (Select one answer.)

    A. A multitasking computer
    B. A mainframe computer
    C. A peer-to-peer computer
    D. A LAN computer

2. Which of the following statements are *not* true? (Select all that apply.)

    A. A peer-to-peer server is the best choice for a large corporate network.
    B. Client/server networks are more robust that peer-to-peer networks.
    C. Novell NetWare is an example of a peer-to-peer NOS.
    D. Windows 98 SE does not support peer-to-peer networking.

3. You have configured a new client PC and connected it to your LAN. You can see some of the servers on the network, but not all of them. What is the most likely cause? (Select one answer.)

    A. A faulty NIC
    B. Faulty media
    C. A faulty OSI layer
    D. A missing protocol driver

4. Which of the following items is *not* part of a data packet? (Select one answer.)

    A. Media identifier
    B. Data length
    C. Protocol ID
    D. CRC

5. Which layer of the OSI model is responsible for addressing and routing? (Select one answer.)

    A. Transport
    B. Network
    C. Session
    D. Application

6. Which layer of the OSI model can translate data from one format to another? (Select one answer.)

   A. Application
   B. Presentation
   C. Session
   D. Transport

7. At which layer of the OSI model is error correction performed? (Select one answer.)

   A. Data Link
   B. Physical
   C. Transport
   D. Session

8. Layer 3 is the _____ layer of the OSI model. (Select one answer.)

   A. Session
   B. Application
   C. Data Link
   D. Network

9. Which of the following takes place at the Data Link layer? (Select all that apply.)

   A. Packet fragmentation
   B. Data framing
   C. CRC checking
   D. Encryption

10. Which of the following are not common network protocols? (Select two answers.)

   A. IPBEUI
   B. IPX/SPX
   C. NetBEUI
   D. NET/IP

REVIEW ANSWERS

1. **C** A desktop PC acting as a client and a server is said to be a peer-to-peer system.

2. **A** **C** **D** Only statement B is true. Client/server networks are more robust than peer-to-peer networks.

3. **D** We know that we're on the network because we can see *some* resources, so the NIC (A) and media (B) must be okay. Answer C is just meaningless. Because we can't see *some* resources, we probably don't have the required protocol installed—answer D.

4. **A** There's no such field as "media identifier" in a data packet, but all the others are present.

5. **B** The Network layer provides addressing and routing functionality.

6. **B** The Presentation layer (answer B) can translate data.

7. **C** Error correction is performed by the Transport layer.

8. **D** Layer 3 is the Network layer.

9. **B** **C** The Data Link layer puts everything together in a packet and checks incoming CRC information.

10. **A** **D** Only IPX/SPX and NetBEUI (B and C) are true protocols; the others are made-up names.