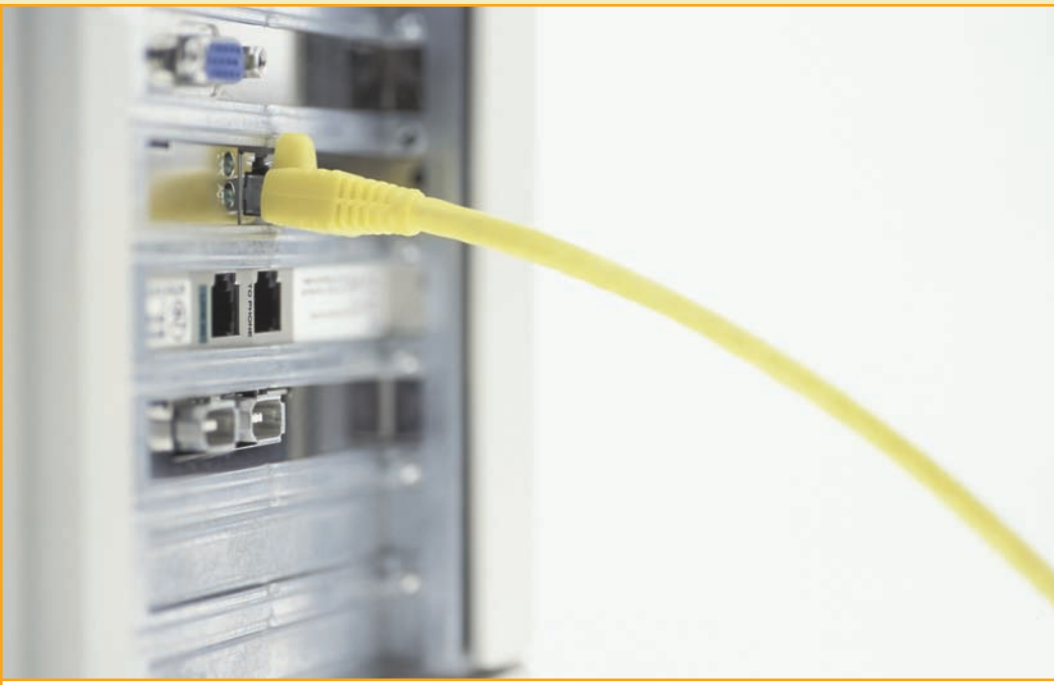
chapter 22

Local Area Networking

"I'm interested in upgrading my 28.8 kilobaud Internet connection to a 1.5 megabit fiberoptic T1 line. Will you be able to provide an IP router that's compatible with my token ring Ethernet LAN configuration?"

—COMIC BOOK GUY, *THE SIMPSONS*



In this chapter, you will learn how to

- **Install and troubleshoot structured cabling**
- **Explain the basics of TCP/IP**
- **Install and configure wired networks**
- **Troubleshoot wired networks**

Networks dominate the modern computing environment. A vast percentage of businesses have PCs connected in a small local area network (LAN), and big businesses simply can't survive without connecting their many offices into a single wide area network (WAN). Even the operating systems of today demand networks. Windows XP, Vista, and 7, for example, come out of the box *assuming* you'll attach them to the Internet just to make them work past 30 days (product activation), and they get all indignant if you don't.

Because networks are so common today, every good tech needs to know the basics of networking technology, operating systems, implementation, and troubleshooting. Accordingly, this chapter teaches you how to build and troubleshoot a basic network. First, let's move beyond the basic switch and UTP cable with RJ-45 connectors you saw in Chapter 5 and discover how real-world networks connect using alternatives to RJ-45, such as fiber. You'll see how professionals use a concept called "structured cabling" with wired networks to ensure their reliability and ease of use. I'll even show you the tools needed to make your own structured cable system.

The second part of this chapter gets down and dirty into TCP/IP and how Windows uses it in a typical network. I'll break down the TCP/IP protocol so you can appreciate how it works.

Next, we'll go through the process of setting up a small network from start to finish. This includes details on planning a network, installing and configuring NICs, setting up switches, configuring TCP/IP—everything you need so that Windows will enable you to share folders, printers, libraries, and so on.

The chapter closes with a popular topic: troubleshooting a network. Windows comes with plenty of powerful tools to help you when the network stops functioning. I'll show you the tools and combine that with a troubleshooting process that helps you get a network up and running again.

This chapter only covers local area networks, such as a group of computers in a single office. We'll save connecting to the Internet for Chapter 24. But be ready! You need to understand everything in this chapter before you can take the next step and connect to the Internet.

Both exam competencies discuss TCP/IP in detail, so this chapter covers both sets of objectives.

801/802

Beyond Basic Ethernet Cabling

Ethernet is the dominant networking technology, and unshielded twisted-pair (UTP) wired Ethernet networks using RJ-45 connectors are the most dominant form of Ethernet. Back in Chapter 5, you got a very basic exposure to an Ethernet network, so now we can take things a bit deeper and look at more network technologies, starting with alternatives to UTP, touring some of the more unique devices you might see in a network, and learning about proper cabling.

Know your cable types for the CompTIA A+ exams: STP, UTP, CAT 3, CAT 5, CAT 5e, and CAT 6. Recall the differences between plenum-grade cable and PVC-sheathed cables.

Alternative Connections

UTP is very popular, but Ethernet, as well as other types of networks, can use alternative cabling that you need to be able to identify. Every CompTIA A+ certified tech needs to know about fiber optic cabling and coaxial cable, so let's start there.

Fiber Optic

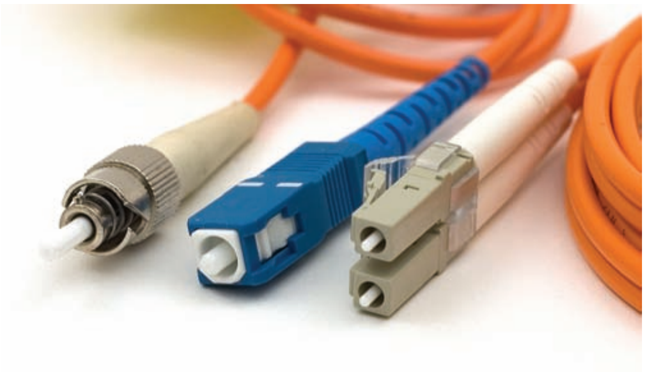
Fiber optic cable is a very attractive way to transmit Ethernet network frames. First, because it uses light instead of electricity, fiber optic cable is immune to electrical problems such as lightning, short circuits, and static. Second, fiber optic signals travel much farther, 2000 meters or more (compared with 100 meters on UTP). Most fiber Ethernet networks use *62.5/125 multimode* fiber optic cable. All fiber Ethernet networks that use this type of cabling require two cables. Figure 22.1 shows three of the more common connectors used in fiber optic networks. Square *SC* connectors are shown in the middle and on the right, and the round *ST* connector is on the left.

Like many other fiber optic connectors, the SC and ST connectors are half-duplex, meaning data flows only one way—hence the need for two cables in a fiber installation. Newer and higher-end fiber installations use connectors with names like LC or MT-RJ.

Tech Tip

Crossover Cables

You can hook two network cards directly together using a special UTP cable called a **crossover cable**. *A crossover cable is a standard UTP cable with one RJ-45 connector using the 568A standard and the other using the 568B standard. This reverses the signal between sending and receiving wires and thus does the job of a hub or switch. Crossover cables work great as a quick way to network two PCs. You can purchase a crossover cable at any computer store.*



• Figure 22.1 Typical fiber optic cables with connectors

Multimode and Single-Mode Light can be sent down a fiber optic cable as regular light or as laser light. Each type of light requires totally different fiber optic cables. Most network technologies that use fiber optics use light-emitting diodes (LEDs) to send light signals. These use *multimode* fiber optic cabling. Multimode fiber transmits multiple light signals at the same time, each using a different reflection angle within the core of the cable. The multiple reflection angles tend to disperse over long distances, so multimode fiber optic cables are used for relatively short distances.

Network technologies that use laser light use *single-mode* fiber optic cabling. Using laser light and single-mode fiber optic cables allows for phenomenally high transfer rates over long distances. Except for long-distance links, single-mode is currently quite rare; if you see fiber optic cabling, you can be relatively sure it is multimode.

Know fiber connector types and the difference between multimode and single-mode fiber.

There are close to 100 different Ethernet fiber optic cabling standards, with names like 1000BaseSX and 10GBaseSR. The major difference is the speed of the network (there are also some important differences in the way systems interconnect, and so on). If you want to use fiber optic cabling, you need a fiber optic switch and fiber optic network cards, and they're not cheap. The fiber optic cabling itself is delicate, expensive, and difficult to use, so it is usually reserved for use in data centers and is rarely used to connect desktop PCs.

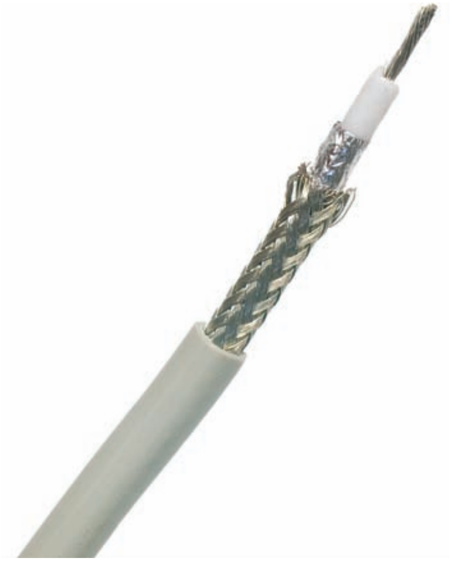
There are a number of Ethernet standards that use fiber optic cable instead of UTP.

Fiber networks follow the speed and distance limitations of their networking standard, so it's hard to pin down precise numbers on true limitations. Multimode overall is slower and has a shorter range than single-mode. A typical multimode network runs at 10, 100, or 1000 Mbps, though some can go to 10,000 Mbps. Distances for multimode runs generally top out at ~600 meters. With single-mode, speed and distance—depending on the standard—can blow multimode away. The record transmission speed in 2011, for example, was 100 *terabits* per second and that was over 100 *miles*!

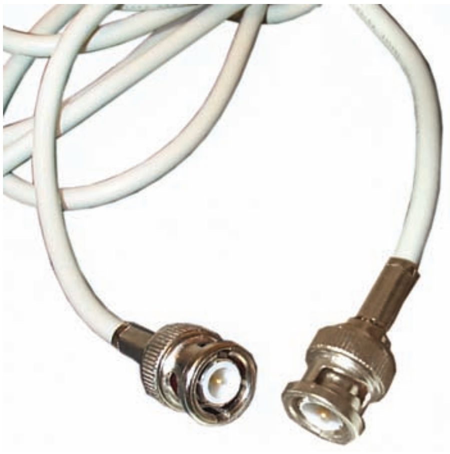
Coax/BNC

Early versions of Ethernet ran on **coaxial cable** instead of UTP. While the Ethernet standards using coax are long gone, coax lives on in the networking world, primarily for cable modems and satellite connections. Coax cable consists of a center cable (core) surrounded by insulation. This in turn is covered with a *shield* of braided cable (see Figure 22.2). The center core actually carries the signal. The shield effectively eliminates outside interference. The entire cable is then surrounded by a protective insulating cover.

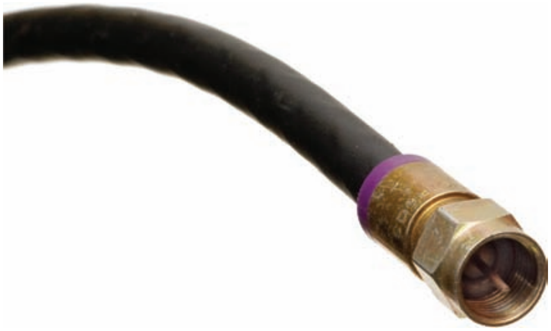
Coax cables are rated using an RG name. There are hundreds of RG ratings for coax, but the only two you need to know for the CompTIA A+ exams are RG-59 and RG-6. Both standards are rated by impedance, which is measured in ohms. Both RG-6 and RG-59 have a 75-ohm impedance. Both of these coax cables are used by your cable television, but RG-59 is thinner and doesn't carry data quite as far as RG-6. The RG rating is clearly marked on the cable.



• Figure 22.2 Typical coax



• Figure 22.3 BNC connector



• Figure 22.4 F-type connector

Coax most commonly uses two different types of connectors. A BNC connector (see Figure 22.3) uses a quarter twist connector, and an F-type connector uses a screw connector. BNC is uncommon, but F-type is on the back of all cable modems and most televisions (see Figure 22.4).

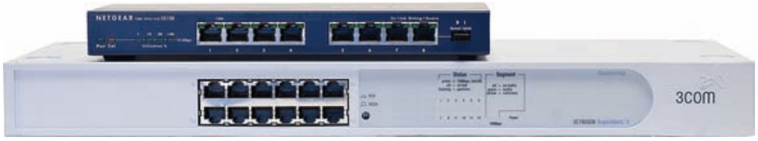
There is no hard limit to how fast coaxial cable can transmit data. Most cable broadband Internet implementations, however, top out at around 50 Mbps.

Network Devices

Back in Chapter 5 you read about hubs, switches, and routers. Let's do a quick review and add a few other devices.

Hubs

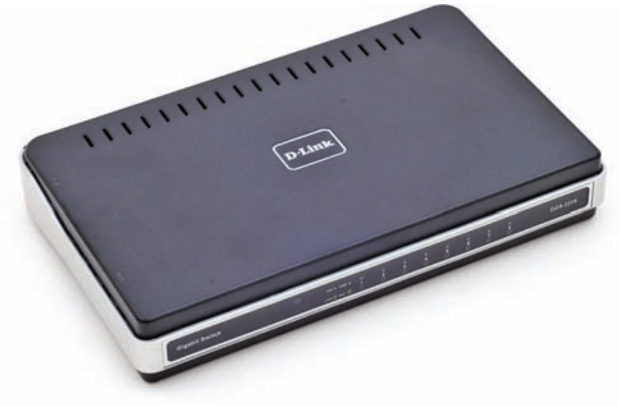
Hubs were the main interconnection for older Ethernet networks (see Figure 22.5). Any incoming signal on any port on a hub is re-created (repeated) and sent out on every connected port on the hub. The downside to hubs is that all connected devices have to share the total bandwidth. Hubs are extremely rare today, having been replaced by switches.



• Figure 22.5 Typical hubs

Switches

Switches are the current most common interconnection for Ethernet networks (see Figure 22.6). A **switch** looks like a hub, but a switch automatically creates point-to-point connections between any two computers. By separating every connection, each computer can use the full bandwidth of the switch.



• Figure 22.6 Typical switch

Bridges

If someone knows Morse code, it doesn't matter what medium you use to communicate the patterns of a coded method. You can blink a flashlight in his or her face, beat on a bongo drum, or tap into a telegraph machine: the person will understand the code. Ethernet functions similarly. The code for Ethernet is the same no matter what medium transfers that message. That means you can easily connect two Ethernet networks that use completely different media internally, such as UTP to fiber or maybe UTP to wireless. In these cases you need a device called a bridge. A **bridge** will always have two interfaces, one interface for each of the different media (see Figure 22.7).

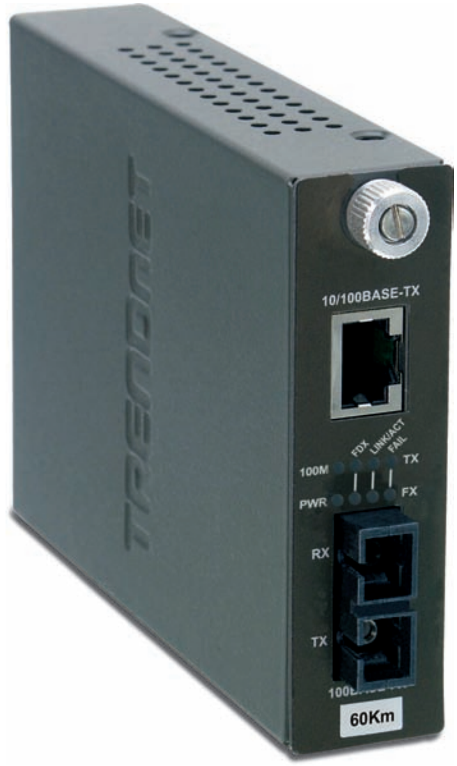
Networked Attached Storage (NAS)

You already know that networks enable you to share files and services with multiple PCs. In most cases, network administrators store files on a server system. This server might be a dedicated file server—a machine running Windows Server 2008 R2, for example—or it might just be someone's regular Windows machine with a shared folder. You can also use a *networked attached storage* (*NAS*) system. A NAS is basically a headless system (no monitor, no keyboard, and no mouse) that you plug into a network (Figure 22.8). A NAS is almost totally self-configuring, requiring only a name and network type (domain/workgroup).

We tend to use the term *network appliance* for any headless computer (that is, one with no direct interface) designed to do very specific duties. A NAS box is a perfect example of a network appliance.

Understand that a NAS only does one thing: share its hard drives. Almost all NAS devices use some form of Web interface for configuration, enabling you to control the NAS from a Web browser on any PC in the network.

There are hundreds of different NAS solutions to choose from. For most people, the big criteria are storage capacity, RAID options, and ease of configuration.

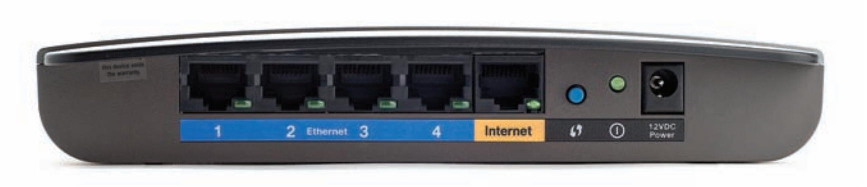


• **Figure 22.7** Typical bridge

• **Figure 22.8** Typical NAS

Routers

A **router** connects LANs together using the TCP/IP protocol. By definition, a router must have at least two connections—one into a network, and one out to another network. Some more powerful routers have many more connections. Figure 22.9 shows a typical home router.



• Figure 22.9 Typical home router

The CompTIA A+ exams assume you have a basic understanding of how routers work. To detail the process, I'll need to dive a bit deeper into TCP/IP. Check out the "TCP/IP" section later in this chapter.

The CompTIA A+ exams expect you to know the differences between hubs, routers, switches, bridges, and access points.

Structured Cabling

If you want a functioning, dependable, real-world network, you need a solid understanding of a set of standards collectively called **structured cabling**. These standards, defined by the Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA)—yes, the same folks who tell you how to crimp an RJ-45 onto the end of a UTP cable—give professional cable installers detailed standards on every aspect of a cabled network, from the type of cabling to use to standards on running cable in walls, even the position of wall outlets.

The CompTIA A+ exams require you to understand the basic concepts involved in installing network cabling and to recognize the components used in a network. The CompTIA A+ exams do not, however, expect you to be as knowledgeable as a professional network designer or cable installer. Your goal should be to understand enough about real-world cabling systems to communicate knowledgeably with cable installers and to perform basic troubleshooting. Granted, by the end of this section, you'll know enough to try running your own cable (I certainly run my own cable), but consider that knowledge extra credit.

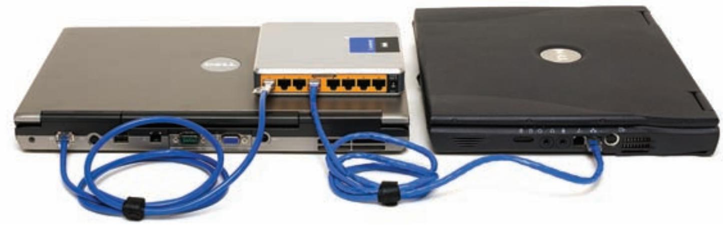
A structured cabling system is useful for more than just computer networks. You'll find structured cabling defining telephone networks and video conferencing setups, for example.

The idea of structured cabling is to create a safe, reliable cabling infrastructure for all of the devices that may need interconnection. Certainly this applies to computer networks, but also to telephone, video—anything that might need low-power, distributed cabling.

You should understand three issues with structured cabling. Cable basics start the picture, with switches, cabling, and PCs. You'll then look at the components of a network, such as how the cable runs through the walls and where it ends up. This section wraps up with an assessment of connections leading outside your network.

Cable Basics—A Star Is Born

Back in Chapter 5 we developed the idea of a LAN in its most basic configurations: a switch, some UTP cable, and a few PCs—in other words, a typical physical star network (see Figure 22.10).



• Figure 22.10 A switch connected by UTP cable to two PCs

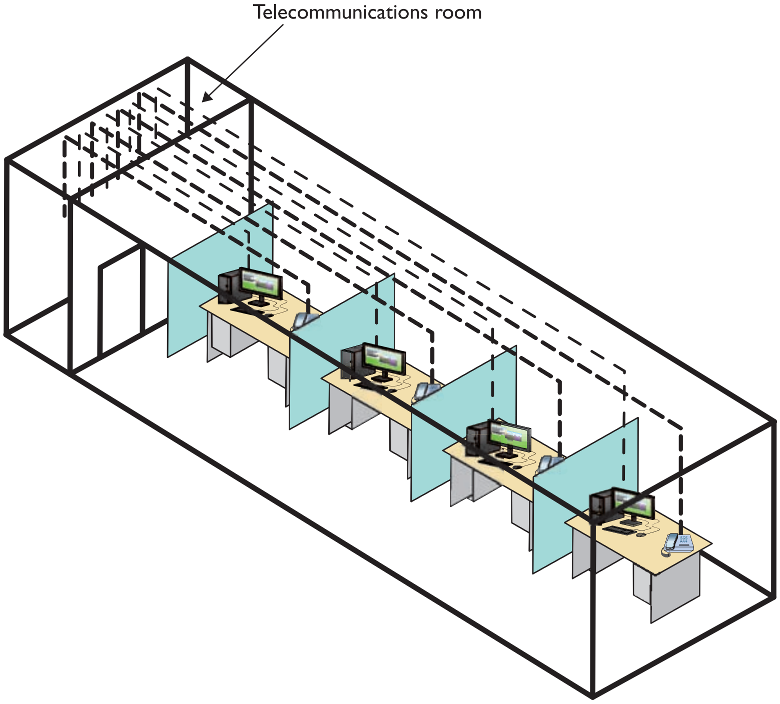
No law of physics prevents you from placing a switch in the middle of your office and running cables on the floor to all the computers in your network. This setup works, but it falls apart spectacularly when applied to a real-world environment. Three problems present themselves to the network tech. First, the exposed cables running along the floor are just waiting for someone to trip over them, giving that person a wonderful lawsuit opportunity. Simply moving and stepping on the cabling will, over time, cause a cable to fail due to wires breaking or RJ-45 connectors ripping off cable ends. Second, the presence of other electrical devices close to the cable can create interference that confuses the signals going through the wire. Third, this type of setup limits your ability to make any changes to the network. Before you can change anything, you have to figure out which cables in the huge rat's nest of cables connected to the switch go to which machines. Imagine *that* troubleshooting nightmare!

"Gosh," you're thinking (okay, I'm thinking it, but you should be, too), "there must be a better way to install a physical network." A better installation would provide safety, protecting the star from vacuum cleaners, clumsy coworkers, and electrical interference. It would have extra hardware to organize and protect the cabling. Finally, the new and improved star network installation would feature a cabling standard with the flexibility to enable the network to grow according to its needs and then to upgrade when the next great network technology comes along. That is the definition of structured cabling.

Cross Check

TIA/EIA Standards

You should remember the TIA/EIA 568 wiring standards from Chapter 5, but do you remember how to tell the difference between 568A and 568B?



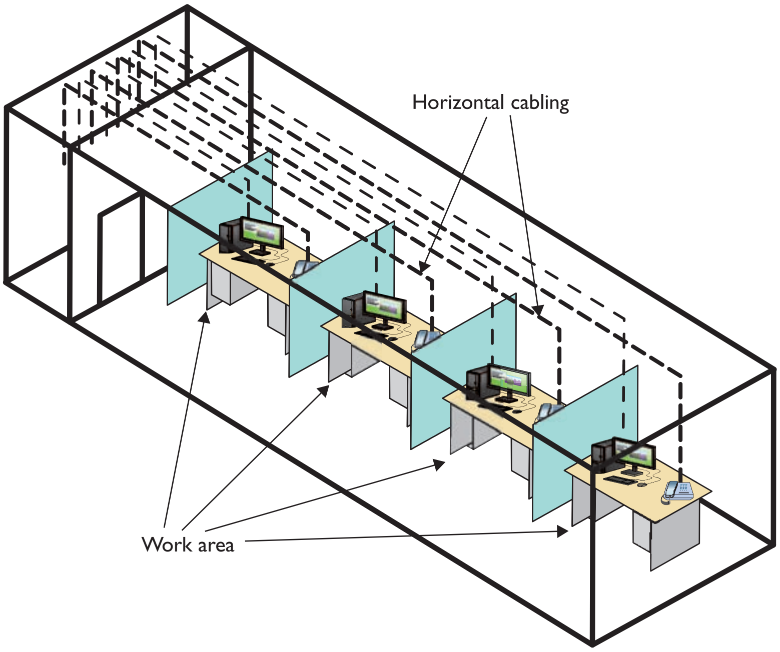
• Figure 22.11 Telecommunications room

Structured Cable Network Components

Successful implementation of a basic structured cabling network requires three essential ingredients: a telecommunications room, horizontal cabling, and a work area. Let's zero in on one floor of a typical office. All the cabling runs from individual PCs to a central location, the **telecommunications room** (see Figure 22.11). What equipment goes in there—a switch or a telephone system—is not the important thing. What matters is that all the cables concentrate in this one area.

All cables run horizontally (for the most part) from the telecommunications room to the PCs. This cabling is called, appropriately, **horizontal cabling**. A single piece of installed horizontal cabling is called a **run**. At the opposite end of the horizontal cabling from the telecommunications room is the work area. The **work area** is often simply an office or cubicle that potentially contains a PC and a telephone. Figure 22.12 shows both the horizontal cabling and work areas.

Each of the three parts of a basic star network—the telecommunications room, the horizontal cabling, and the work area(s)—must follow a series of strict standards designed to ensure that the cabling system is reliable and easy to manage. The cabling standards set by TIA/EIA enable techs to make sensible decisions on equipment installed in the telecommunications room, so let's tackle horizontal cabling first, and then return to the telecommunications room. We'll finish up with the work area.



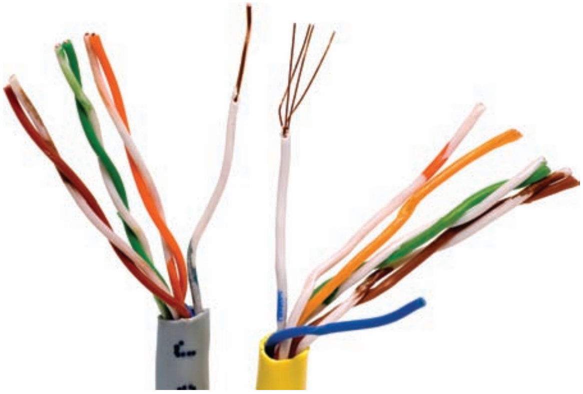
• Figure 22.12 Horizontal cabling and work area

Horizontal Cabling A horizontal cabling run is the cabling that goes more or less horizontally from a work area to the telecommunications room. In most networks, this cable is a CAT 5e or better UTP, but when you move into structured cabling, the TIA/EIA standards define a number of other aspects of the cable, such as the type of wires, number of pairs of wires, and fire ratings.

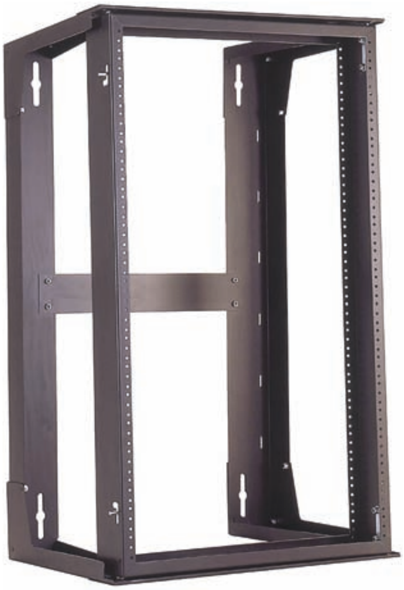
A single piece of cable that runs from a work area to a telecommunications room is called a *run*. In most networks, this cable is CAT 5e or better UTP.

Solid Core Versus Stranded Core All UTP cables come in one of two types: solid core or stranded core. Each wire in **solid core** UTP uses a single solid wire. With **stranded core**, each wire is actually a bundle of tiny wire strands. Each of these cable types has its benefits and downsides. Solid core is a better conductor, but it is stiff and will break if handled too often or too roughly. Stranded core is not quite as good a conductor, but it will stand up to substantial handling without breaking. Figure 22.13 shows a close-up of solid and stranded core UTP.

TIA/EIA specifies that horizontal cabling should always be solid core. Remember, this cabling is going into your walls and ceilings, safe from the harmful effects of shoes and vacuum cleaners. The ceilings and walls enable you to take advantage of the better conductivity of solid core without the



• Figure 22.13 Solid and stranded core UTP risk of cable damage. Stranded cable also has an important function in a structured cabling network, but I need to discuss a few more parts of the network before I talk about where to use stranded UTP cable.



• Figure 22.14 A short equipment rack

Equipment racks evolved out of the railroad signaling racks from the 19th century. The components in a rack today obviously differ a lot from railroad signaling, but the 19-inch width has remained the standard for well over 100 years.

The Telecommunications Room

The telecommunications room is the heart of the basic star. This room is where all the horizontal runs from all the work areas come together. The concentration of all this gear in one place makes the telecommunications room potentially one of the messiest parts of the basic star. Even if you do a nice, neat job of organizing the cables when they are first installed, networks change over time. People move computers, new work areas are added, network topologies are added or improved, and so on. Unless you impose some type of organization, this conglomeration of equipment and cables decays into a nightmarish mess.

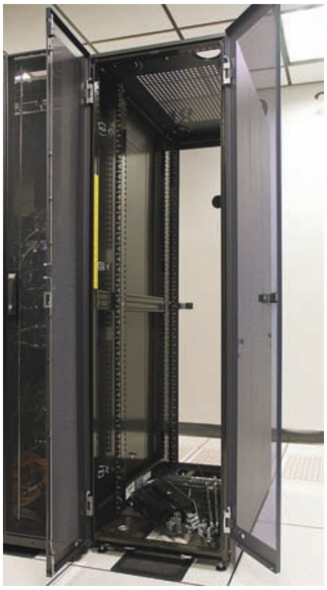
Fortunately, the TIA/EIA structured cabling standards define the use of specialized components in the telecommunications room that make organizing a snap. In fact, it might be fair to say that there are too many options! To keep it simple, we're going to stay with the most common telecommunications room setup and then take a short peek at some other fairly common options.

Equipment Racks The central component of every telecommunications room is one or more equipment racks. An **equipment rack** provides a safe, stable platform for all the different hardware components. All equipment racks are 19 inches wide, but they vary in height from two- to three-foot-high models that bolt onto a wall (see Figure 22.14) to the more popular floor-to-ceiling models (see Figure 22.15).

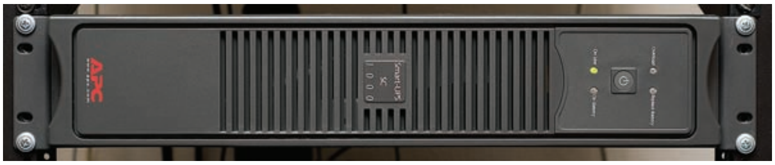
You can mount almost any network hardware component into a rack. All manufacturers make rack-mounted switches that mount into a rack with a few screws. These switches are available with a wide assortment of ports and capabilities. There are even rack-mounted servers, complete with slide-out keyboards, and rack-mounted uninterruptible power supplies (UPSs) to power the equipment (see Figure 22.16).

All rack-mounted equipment uses a height measurement known simply as a **U**. A U is 1.75 inches. A device that fits in a 1.75-inch space is called a 1U; a device designed for a 3.5-inch space is a 2U; and a device that goes into a 7-inch space is called a 4U. Most rack-mounted devices are 1U, 2U, or 4U. The rack in Figure 22.15 is called a 42U rack to reflect the total number of Us it can hold.

Patch Panels and Cables Ideally, once you install horizontal cabling, you should never move it. As you know, UTP horizontal cabling has a solid core, making it pretty stiff. Solid core cables can handle some rearranging,



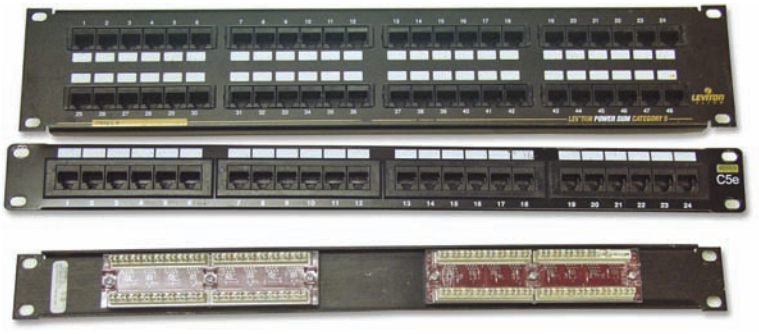
• Figure 22.15 A floor-to-ceiling rack



• Figure 22.16 A rack-mounted UPS

but if you insert a wad of solid core cables directly into your switches, every time you move a cable to a different port on the switch, or move the switch itself, you will jostle the cable. You don't have to move a solid core cable many times before one of the solid copper wires breaks, and there goes a network connection!

Luckily for you, you can easily avoid this problem by using a patch panel. A **patch panel** is simply a box with a row of female connectors (ports) in the front and permanent connections in the back, to which you connect the horizontal cables (see Figure 22.17).



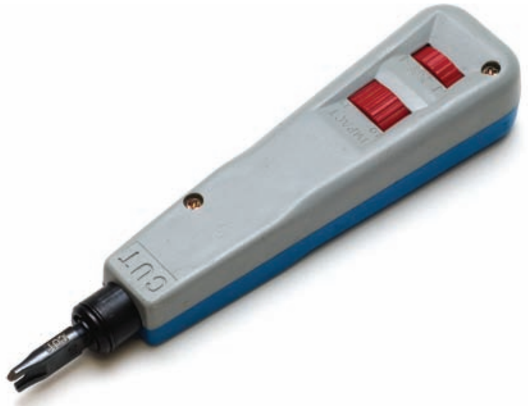
• **Figure 22.17** Typical patch panels

The most common type of patch panel today uses a special type of connecter called a **110 block**, or sometimes a *110-punchdown block*. UTP cables connect to a 110 block using a **punchdown tool**. Figure 22.18 shows a typical punchdown tool, and Figure 22.19 shows the punchdown tool punching down individual strands.

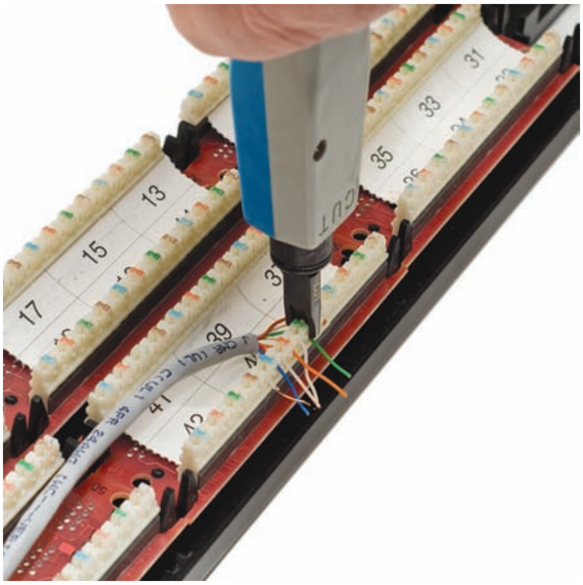
The CompTIA A+ exams expect you to know that a punchdown tool is used for securing UTP connections to a punchdown block. It's not until you go for CompTIA Network+ certification that you'll be expected to know how to use these tools.

The punchdown block has small metal-lined grooves for the individual wires. The punchdown tool has a blunt end that forces the wire into the groove. The metal in the groove slices the cladding enough to make contact.

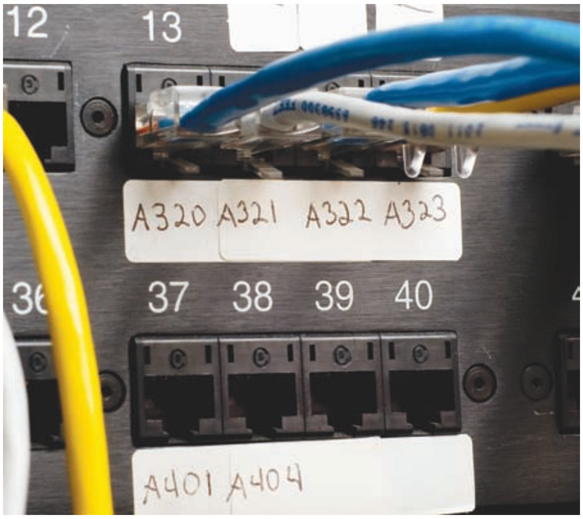
Not only do patch panels prevent the horizontal cabling from being moved, but they are also your first line of defense in organizing the cables. All patch panels have space in the front for labels, and these labels are the network tech's best friend! Simply place a tiny label on the patch panel to identify each cable, and you will never have to experience that sinking feeling of standing in the telecommunications room of your nonfunctioning network, wondering which cable is which. If you want to be a purist, there is an official, and rather confusing, TIA/EIA labeling methodology called TIA/EIA 606, but a number of real-world network techs simply use their own internal codes (see Figure 22.20).



• **Figure 22.18** Punchdown tool



• **Figure 22.19** Punching down a 110 block



• Figure 22.20 Typical patch panels with labels

Patch panels are available in a wide variety of configurations that include different types of ports and numbers of ports. You can get UTP, STP, or fiber ports, and some manufacturers combine several different types on the same patch panel. Panels are available with 8, 12, 24, 48, or even more ports.

UTP patch panels, like UTP cables, come with CAT ratings, which you should be sure to check. Don't blow a good CAT 6 cable installation by buying a cheap patch panel—get a CAT 6 patch panel! A higher-rated panel supports earlier standards, so you can use a CAT 6 or even CAT 6a rack with CAT 5e cabling. Most manufacturers proudly display the CAT level right on the patch panel (see Figure 22.21).

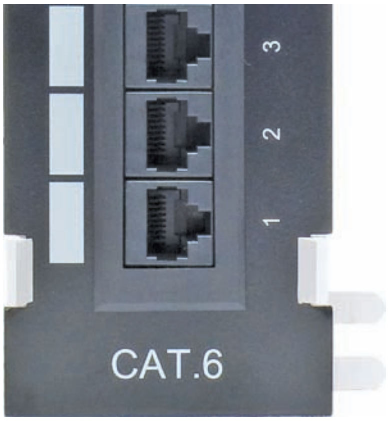
Once you have installed the patch panel, you need to connect the ports to the switch through **patch cables**. Patch cables are short (typically two- to five-foot) UTP cables. Patch cables use stranded rather than solid cable, so they can tolerate much more handling. Even though you can make your own patch cables, most people buy premade ones. Buying patch cables enables you to use different-colored cables to facilitate organization (yellow for accounting, blue for sales, or whatever scheme works for you). Most prefabricated patch cables also come with a reinforced (booted) connector specially designed to handle multiple insertions and removals (see Figure 22.22).

The CompTIA A+ exams expect you to know that a cable tech uses a crimper or crimping tool to attach an RJ-45 to the end of a UTP cable.

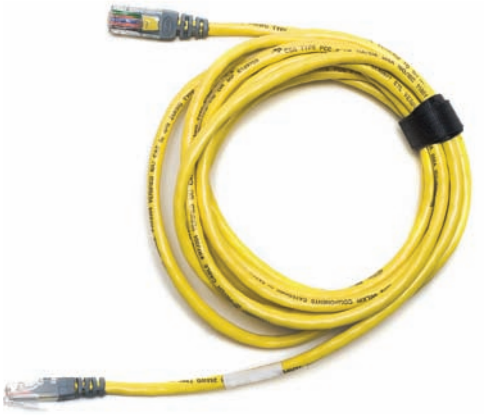
Making Your Own Patch Cables Although most people prefer simply to purchase premade patch cables, making your own is fairly easy. To make your own, use stranded UTP cable that matches the CAT level of your horizontal cabling. Stranded cable also requires specific crimps, so don't use crimps designed for solid cable. Crimping is simple enough, although getting it right takes some practice.

Figure 22.23 shows the two main tools of the crimping trade: an RJ-45 crimper with built-in wire stripper and a pair of wire snips. Professional cable installers naturally have a wide variety of other tools as well.

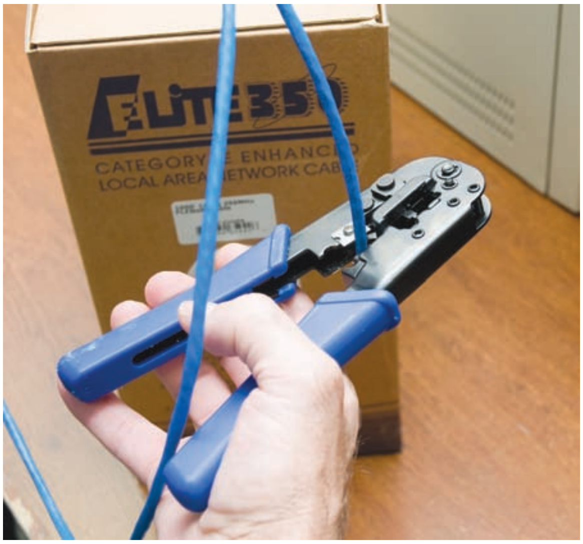
Here are the steps for properly crimping an RJ-45 onto a UTP cable. If you have some crimps, cable, and a crimping tool handy, follow along!



• Figure 22.21 CAT level on patch panel



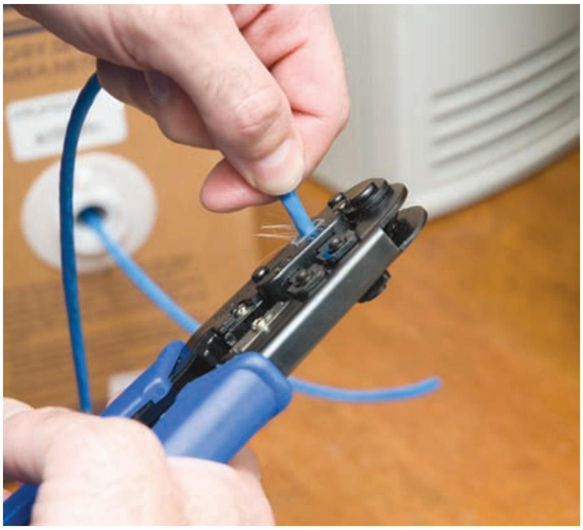
• Figure 22.22 Typical patch cable



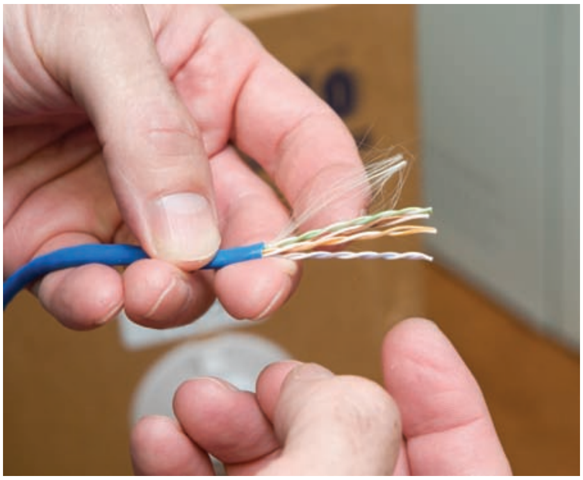
• **Figure 22.23** Crimper and snips

1. Cut the cable square using RJ-45 crimpers or scissors.
2. Strip off one-half inch of plastic jacket from the end of the cable (see Figure 22.24).
3. Slowly and carefully insert each individual wire into the correct location according to either TIA/EIA 568A or B (see Figure 22.25). Unravel as little as possible.
4. Insert the crimp into the crimper and press (see Figure 22.26). Don't worry about pressing too hard; the crimper has a stop to prevent you from using too much pressure.

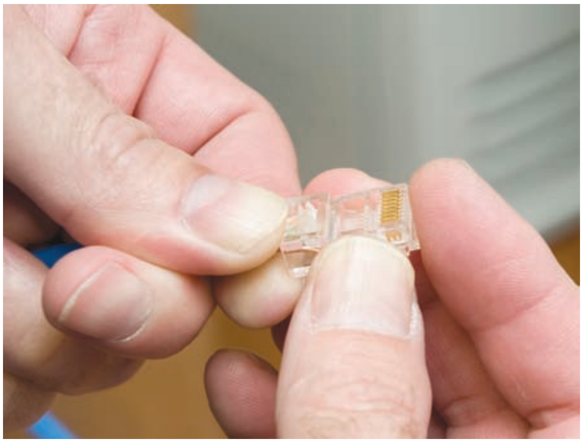
Figure 22.27 shows a nicely crimped cable. Note how the plastic jacket goes into the crimp.



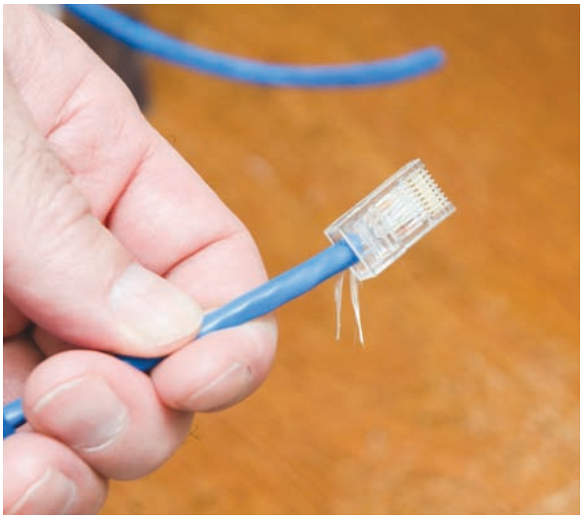
• **Figure 22.26** Crimping the cable



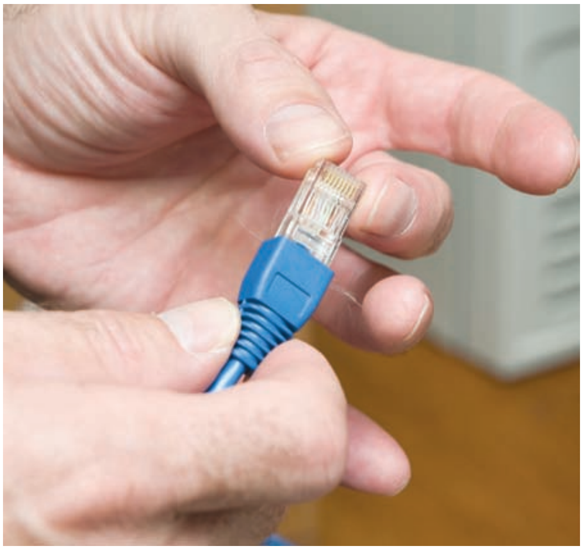
• **Figure 22.24** Properly stripped cable



• **Figure 22.25** Inserting the individual strands



• **Figure 22.27** Properly crimped cable



• Figure 22.28 Adding a boot

A good patch cable should include a boot. Figure 22.28 shows a boot being slid onto a newly crimped cable. Don't forget to slide each boot onto the patch cable *before* you crimp both ends!

After making a cable, you need to test it to make sure it's properly crimped. We use a handy cable tester (a kind of multimeter), available in any good electronics store, to verify all the individual wires are properly connected and in the correct location (see Figure 22.29).

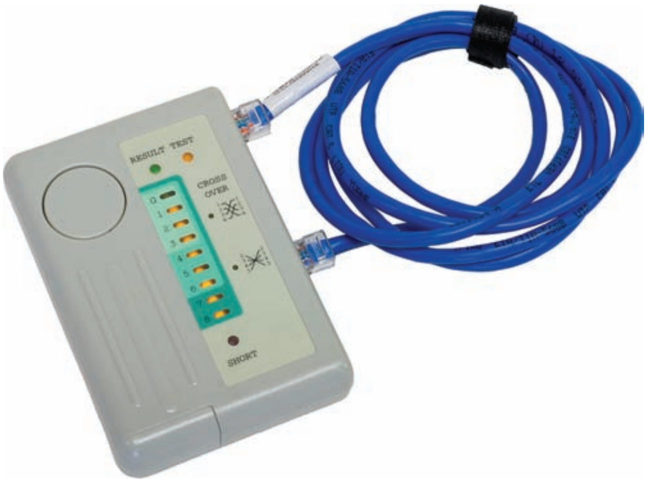
The Work Area

From a cabling standpoint, a work area is nothing more than a wall outlet that serves as the termination point for horizontal network cables: a convenient insertion point for a PC and a telephone. (In practice, of course, the term "work area" includes the office or cubicle.) A wall outlet itself consists of one or two female jacks to accept the cable, a mounting bracket, and a faceplate. You connect the PC to the wall outlet with a patch cable (see Figure 22.30).

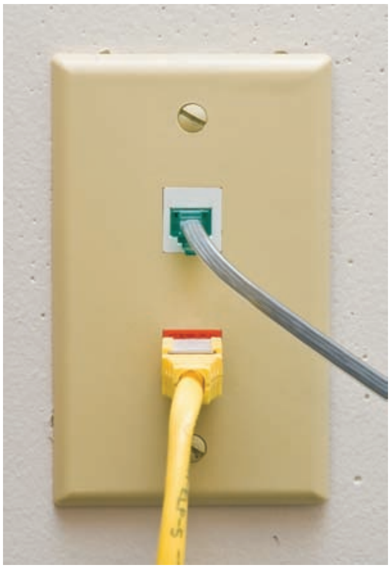
The female RJ-45 jacks in these wall outlets also have CAT ratings. You must buy CAT-rated jacks for wall outlets to go along with the CAT rating of the cabling in your network. In fact, many network connector manufacturers use the same connectors, often 110 punchdowns, in the wall outlets that they use on the patch panels (see Figure 22.31). These modular outlets significantly increase the ease of installation.

The last step is connecting the PC to the wall outlet. Here again, most folks use a patch cable. Its stranded cabling stands up to the abuse caused by moving PCs, not to mention the occasional kick.

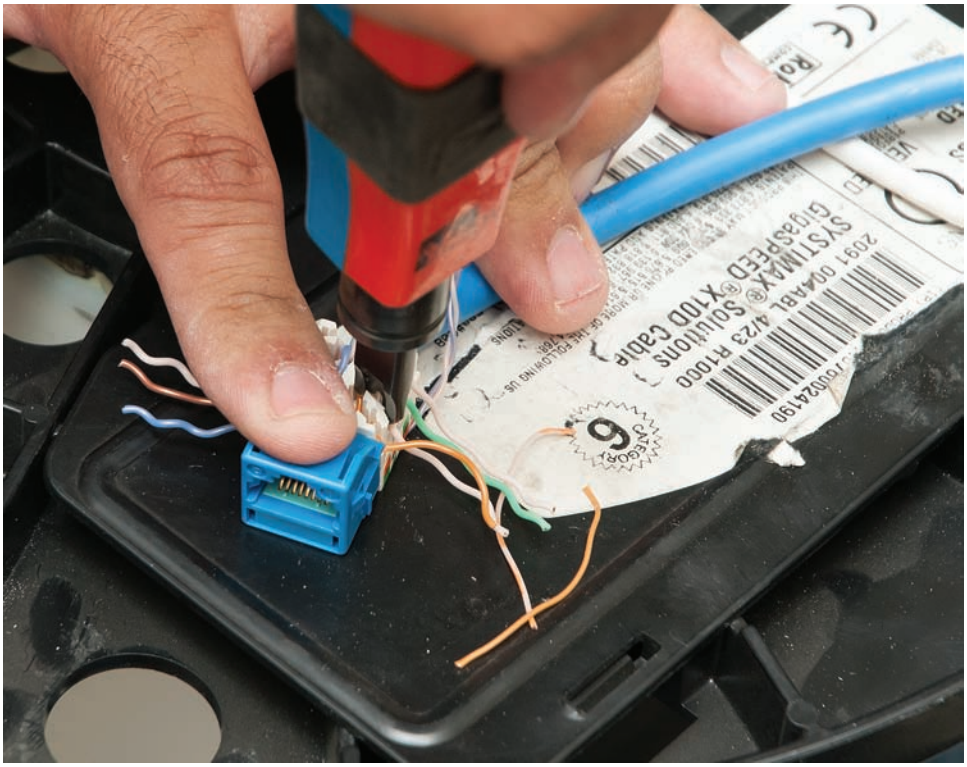
The work area may be the simplest part of the structured cabling system, but it is also the source of most network failures. When a user can't access the network and you suspect a broken cable, the first place to look is the work area.



• Figure 22.29 Typical tester



• Figure 22.30 Typical work area outlet



• Figure 22.31 Punching down a modular jack

TCP/IP

The **Transmission Control Protocol/Internet Protocol (TCP/IP)** is the primary protocol of most modern networks, including the Internet. For a PC to access the Internet, it must have TCP/IP loaded and configured properly. TCP/IP has become so predominant that most network folks use it even on networks that do not connect to the Internet. Although TCP/IP is powerful, it is also a bit of a challenge to set up. So whether you are installing a modem for a dial-up connection to the Internet or setting up 500 computers on their own private *intranet*, you must understand some TCP/IP basics. You'll go through the following basic sections of the protocol and then you'll look at specific steps to install and configure TCP/IP.

Network Addressing

Any network address must provide two pieces of information: it must uniquely identify the machine and it must locate that machine within the larger network. In a TCP/IP network, the IP address identifies the PC and the network on which it resides. If you look at an IP address, it's not apparent which part of the address identifies the network and which part is the unique identifier of the computer. Let's review IP addresses and then see how they identify PCs and networks.

IP Addresses

In Chapter 5, you learned that TCP/IP networks don't identify PCs by name but by IP address. The **IP address** is the unique identification number for your system on the network. IP addresses consist of four sets of eight binary numbers (octets), each set separated by a period. This is called *dotted-decimal notation*. So, instead of a computer being called SERVER1, it gets an address like so:

202.34.16.11

Written in binary form, the address would look like this:

```
11001010.00100010.00010000.00001011
```

To make the addresses more comprehensible to users, the TCP/IP folks decided to write the decimal equivalents:

```
00000000 = 0
00000001 = 1
00000010 = 2
...
11111111 = 255
```

Subnet Mask

Part of every IP address identifies the network (the network ID), and another part identifies the local computer (the host ID, or host) on the network. A NIC uses a value called the **subnet mask** to distinguish which part of the IP address identifies the network ID and which part of the address identifies the host. The subnet mask blocks out (or masks) the network portion of an IP address.

Let's look at a typical subnet mask: 255.255.255.0. When you compare the subnet mask to the IP address, any part that's all 255s is the network ID. Any part that's all zeros is the host ID. Look at the following example:

IP address: 192.168.4.33

Subnet mask: 255.255.255.0

Because the first thee octets are 255, the network ID is 192.168.4 and the host ID is 33.

Every computer on a single LAN must have the same network ID and a unique host ID. That means every computer on the preceding network must have an IP address that starts with 192.168.4. Every computer on the network must have a unique IP address. If two computers have the same IP address, they won't be able to talk to each other, and other computers won't know where to send data. This is called an *IP conflict*.

You can never have an IP address that ends with a 0 or a 255, so for the preceding example, we can have addresses starting at 192.168.4.1 and ending at 192.168.4.254: a total of 254 addresses. But what if you have more than 254 computers? Well, you just take a 255 out of the subnet mask like this:

255.255.0.0

If the IP address is 192.168.4.33, then we now have a network ID of 192.168 and a host of 4.33. We can have addresses ranging from 192.168.0.1

to 192.168.255.254. (Notice the 0 and the 255? You can have 0s and 255s in an IP address, just not at the end of the IP address.)

So how many addresses can you have now? Well, let's count them out:

192.168.0.1

192.168.0.2

…

192.168.0.254

192.168.1.1

192.168.1.2

…

192.168.255.253

192.168.255.254

You would have a total of 65,534 addresses on your network. So with a subnet mask of 255.255.255.0, you get 254 addresses and a network ID of 192.168.4; and with a subnet mask of 255.255.0.0, you get 65,534 addresses and a network ID of 192.168. That just leaves one big question: who picks the network ID?

Class Licenses

The folks who organized IP addressing way back in the 1970s came up with a way to pass out network IDs using something called *class licenses*. IP addresses are divided into class licenses that correspond with the potential size of the network: Class A, Class B, and Class C. Class A licenses were intended for huge companies and organizations, such as major multinational corporations, universities, and governmental agencies. Class B licenses were assigned to medium-size companies, and Class C licenses were designated for smaller LANs.

Class A networks use the first octet to identify the network address and the remaining three octets to identify the host. Class B networks use the first two octets to identify the network address and the remaining two octets to identify the host. Class C networks use the first three octets to identify the network address and the last octet to identify the host. Table 22.1 lists range (class) assignments.

You'll note that the IP address ranges listed in Table 22.1 skip from 126.x.x.x to 128.x.x.x. That's because the 127 address range (i.e., 127.0.0.0–127.255.255.255) is reserved for network testing (loopback) operations. (We usually just use the address 127.0.0.1 for loopback purposes and call it the *localhost* address, but any address that starts with *127* will work just as well.) That's not the only reserved range, either! Each network class has a specific IP address range reserved for *private* networks—traffic from these networks doesn't get routed to the Internet at large. Class A's private range goes from 10.0.0.0 to 10.255.255.255. Class B has two private address ranges: 172.16.0.0 up to 172.31.255.254 for private

Table 22.1 Class A, B, and C Addresses

Network Class	Address Range	No. of Network Addresses Available	No. of Host Nodes (Computers) Supported
A	1–126	129	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

Pinging the loopback is the best way to test whether a NIC is working properly. To test a NIC's loopback, the other end of the cable must be in a working switch or you must use a loopback device such as a loopback adapter/plug.

Private IP addresses are very commonly used on LANs. But if private IP addresses are blocked by routers, how can we use them if we want to get on the Internet? It's a neat little trick called NAT, which you'll learn about in Chapter 24.

addresses and 169.254.0.0 to 169.254.255.254 to accommodate the **Automatic Private IP Addressing (APIPA)** function (discussed later in the chapter). Class C's private addresses range from 192.168.0.0 to 192.168.255.254.

The default subnet mask for Class A addresses is 255.0.0.0; for Class B, it's 255.255.0.0; and for Class C, 255.255.255.0. For example, in the Class B IP address 131.190.4.121 with a subnet mask of 255.255.0.0, the first two octets (131.190) make up the network ID, and the last two (4.121) make up the host ID.

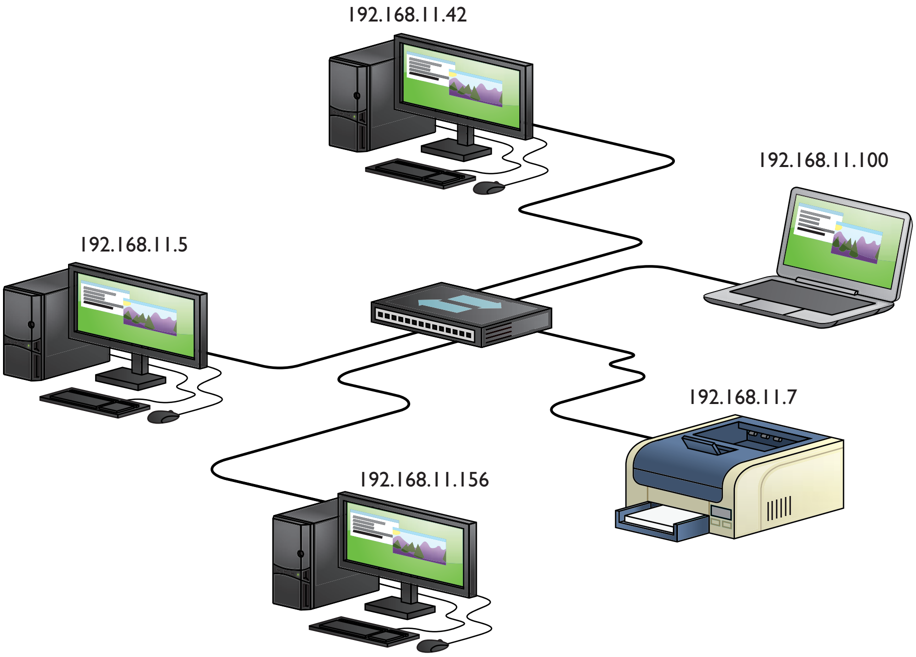
Interconnecting Networks with Routers

Now that you have a basic understanding of IP addressing, let's go back and watch a router in action. Let's take a look at a typical network: four computers and a networked printer all connected to a single switch (see Figure 22.32).

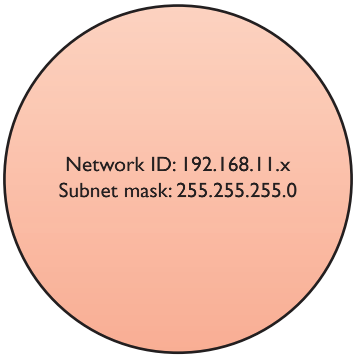
When network nerds draw out a network, they tend not to draw every device. Instead, they make a circle with the network ID and the subnet mask, as shown in Figure 22.33.

If you have two networks, just make two circles. Routers read IP addresses of incoming traffic and forward the traffic to the proper port. Since routers interconnect network IDs, we draw routers as boxes between networks, as shown in Figure 22.34

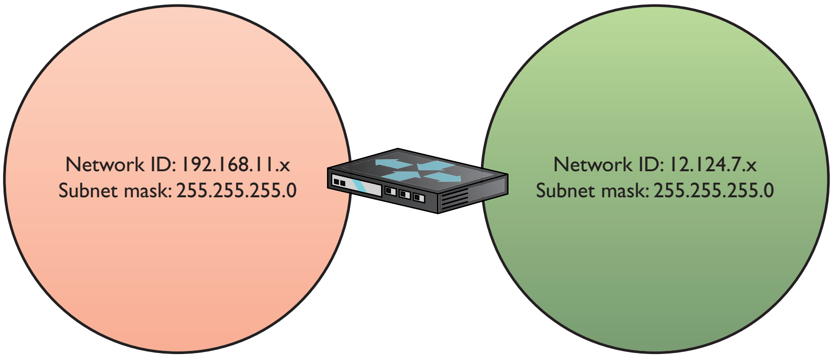
To make a router connect two networks requires a configuration process. There are a lot of different routers out there, from cheap home routers to multimillion-dollar routers that connect the big pipes of the Internet. The CompTIA A+ exams only test on a few basic settings on simple home routers. While we'll save the real configuration of routers for Chapter 24, there's one thing that's very important to understand now: every port on



• Figure 22.32 Typical network

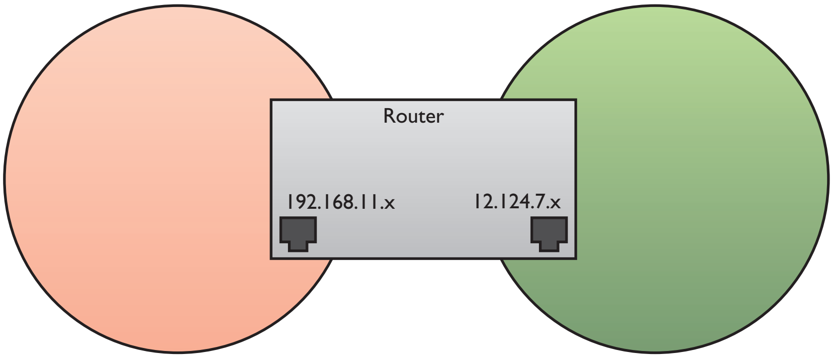


• **Figure 22.33** Same network shown as a circle



• **Figure 22.34** Router between two networks

a router is a member of a different network ID. Let's zoom in on the router in Figure 22.34 and see how the ports are set up, as shown in Figure 22.35. Note that each router gets the first address in the network ID. This isn't a law of physics, just good manners. Keep in mind that the IP address for the router is usually the default gateway for all the computers for that network.



• **Figure 22.35** Router graphic in detail

TCP/UDP

When moving data from one system to another, the TCP/IP protocol suite needs to know if the communication is connection-oriented or connectionless. When you want to be positive that the data moving between two systems gets there in good order, use a connection-oriented application. If it's not a big deal for data to miss a bit or two, then connectionless is the way to go. The connection-oriented protocol used with TCP/IP is called the *Transmission Control Protocol* (*TCP*). The connectionless one is called the *User Datagram Protocol* (*UDP*).

Let me be clear: you don't *choose* TCP or UDP. The people who developed the applications decide which protocol to use. When you fire up your Web browser, for example, you're using TCP because Web browsers use a protocol called HTTP. HTTP is built on TCP.

Over 95 percent of all TCP/IP applications use TCP—that's why we call the protocol suite "TCP/IP" and not "UDP/IP." TCP gets an application's data from one machine to another reliably and completely. As a result, TCP comes with communication rules that require both the sending and receiving machines to acknowledge the other's presence and readiness to send and receive data.

UDP is the "fire and forget" missile of the TCP/IP protocol suite. UDP doesn't possess any of the extras you see in TCP to make sure the data is received intact. UDP works best when you have a lot of data to send that doesn't need to be perfect or when the systems are so close to each other that the chances of a problem occurring are too small to bother worrying about.

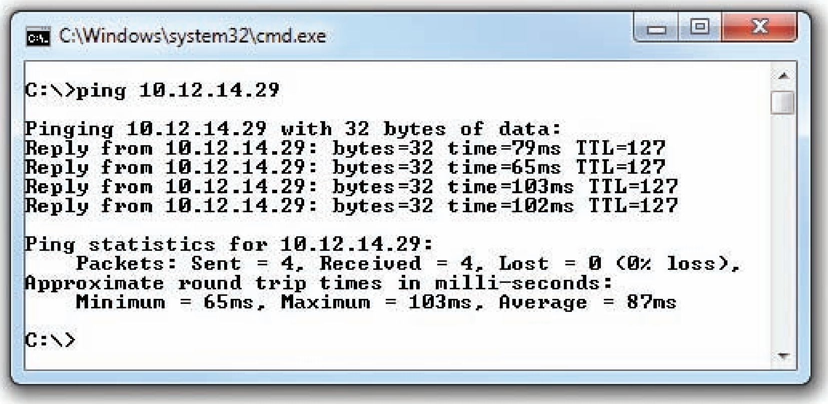
Besides the physical ports on your computer and router, a networking *port* is also a 16-bit number (between 0 and 65,535) assigned to a TCP/IP session (or connection). The port number determines the software protocol used and how to handle the data packet. You'll learn more about ports in Chapter 24.

The CompTIA A+ exams expect you to know about other TCP/IP protocols for accomplishing other goals. They're all covered in Chapter 24.

A few dropped frames on a Voice over IP call, for example, won't make much difference in the communication between two people. So there's a good reason to use UDP: it's smoking fast compared to TCP.

TCP/IP Services

TCP/IP is a different type of protocol. Although it supports File and Printer Sharing, it adds a number of unique sharing functions, lumped together under the umbrella term **TCP/IP services**. The most famous TCP/IP service is called *Hypertext Transfer Protocol* (*HTTP*), the language of the World Wide Web. If you want to surf the Web, you must have TCP/IP. But TCP/IP supplies many other services beyond just HTTP. By using a service called Telnet, for example, you can access a remote system as though you were actually in front of that machine.

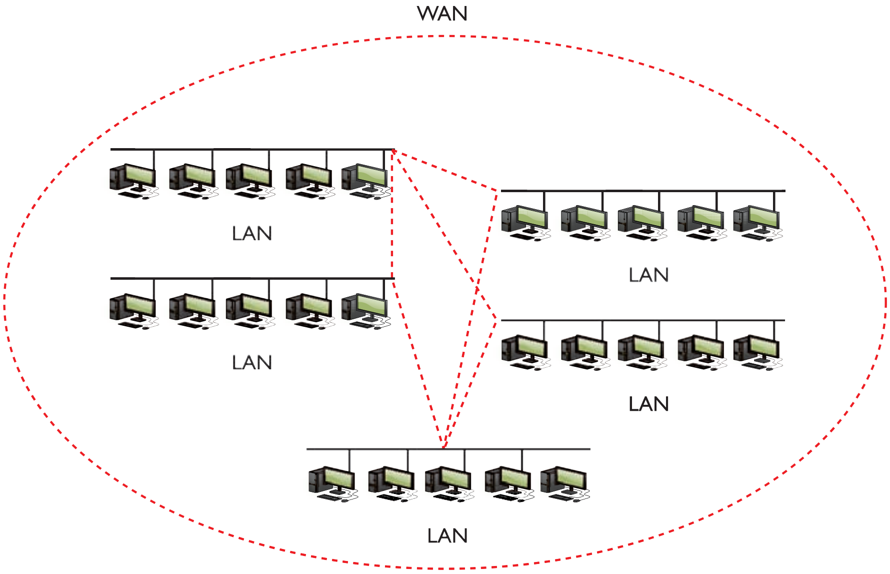


```
C:\>ping 10.12.14.29

Pinging 10.12.14.29 with 32 bytes of data:
Reply from 10.12.14.29: bytes=32 time=79ms TTL=127
Reply from 10.12.14.29: bytes=32 time=65ms TTL=127
Reply from 10.12.14.29: bytes=32 time=103ms TTL=127
Reply from 10.12.14.29: bytes=32 time=102ms TTL=127

Ping statistics for 10.12.14.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 103ms, Average = 87ms

C:\>
```

• Figure 22.36 The ping command in action

Another example is a handy utility called ping. The **ping** command enables one machine to check whether it can communicate with another machine. Figure 22.36 shows an example of ping running on a Windows 7 system. Isn't it interesting that many TCP/IP services run from a command prompt? Good thing you know how to access one! I'll show you other services in a moment.

The goal of TCP/IP is to link any two hosts (remember, a *host* is just a computer in TCP/IP lingo), whether the two computers are on the same LAN or on some other network within the WAN. The LANs within the WAN are linked together with a variety of connections, ranging from basic dial-ups to dedicated high-speed (and expensive) data lines (see Figure 22.37). To move traffic between networks, you use routers (see Figure 22.38). Each host sends traffic to the router only when that data is destined for a remote network, cutting down on traffic across the more expensive WAN links. The host makes these decisions based on the destination IP address of each packet.



• Figure 22.37 WAN concept

TCP/IP Settings

TCP/IP has a number of unique settings that you must configure correctly to ensure proper network functionality. Unfortunately, these settings can be quite confusing, and there are several of them. Not all settings are used for every type of TCP/IP network, and it's not always obvious where you go to set them.

In Windows, you can configure network settings from the appropriate networking applet. To open Network Connections in Windows XP, either right-click on My Network Places and select Properties or open the Control Panel and select Network Connections (see Figure 22.39). In Windows Vista and Windows 7, either right-click on Network and select Properties or open the Control Panel and select Network and Sharing Center. In Windows Vista, you'll also need to click the *Manage network connections* link, and in Windows 7, you'll need to click *Change adapter settings*.

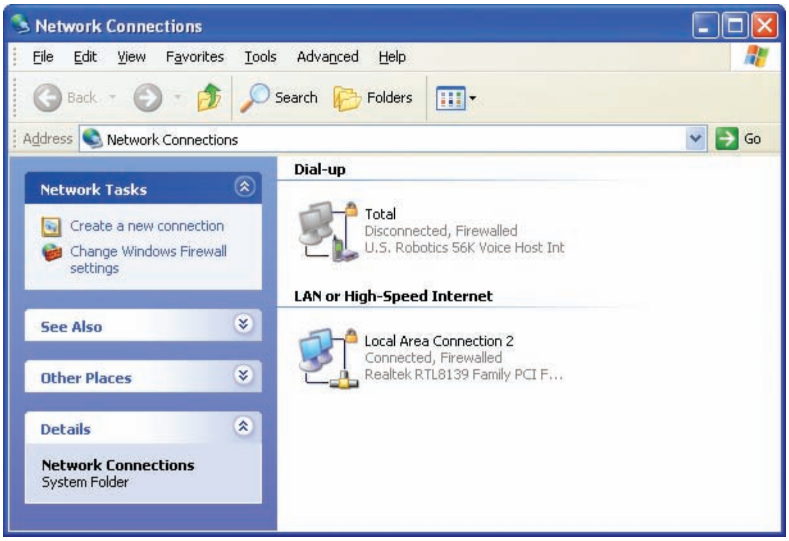
The CompTIA A+ certification exams assume that someone else, such as a tech support person or some network guru, will tell you the correct TCP/IP settings for the network. Your only job is to understand roughly what those settings do and to know where to enter them so the system works. I already discussed default gateways and DNS back in Chapter 5, so the last big thing to cover is DHCP.

• **Figure 22.38** Typical router

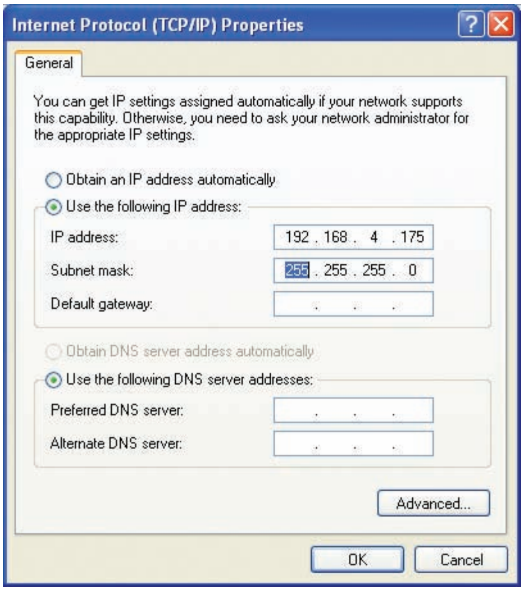
The CompTIA A+ certification exams have a rather strange view of what you should know about networking. Take a lot of time practicing how to get to certain network configuration screens. Be ready for questions that ask, "Which of the following steps will enable you to change a particular value?"

DHCP To understand the **Dynamic Host Configuration Protocol (DHCP)**, you must first remember that every machine must be assigned an IP address, a subnet mask, a default gateway, and at least one DNS server. These settings can be added manually by using the TCP/IP Properties dialog box. When you set the IP address manually, the IP address will not change and is called a **static IP address** (see Figure 22.40).

DHCP enables you to create a pool of IP addresses that are given temporarily to machines. DHCP is especially handy for networks of a lot of laptops that join and leave the network on a regular basis. Why give a machine that is on the network for only a few hours a day a static IP address? For that reason, DHCP is quite popular. If you add a NIC to a Windows system, the default TCP/IP settings are set to use DHCP. When you accept those



• **Figure 22.39** Network Connections showing dial-up and LAN connections



Internet Protocol (TCP/IP) Properties

General

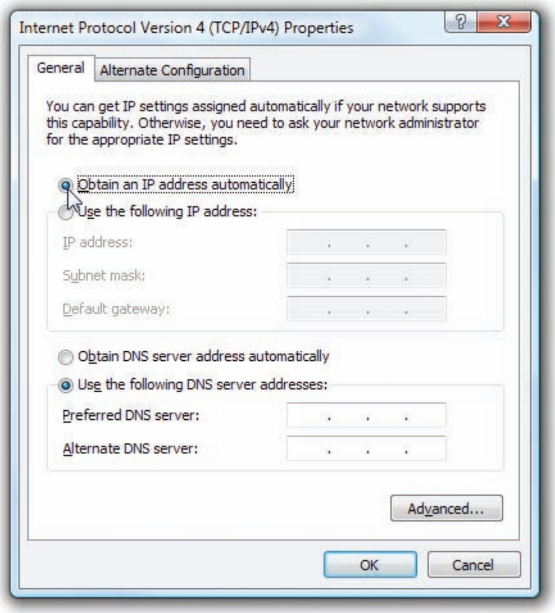
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 4 . 175
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

• **Figure 22.40** Setting a static IP address automatic settings, you're really telling the machine to use DHCP (see Figure 22.41).

To use DHCP you need a DHCP server. A DHCP server can be a program running on any computer in your network, but most commonly it's a feature added to routers.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

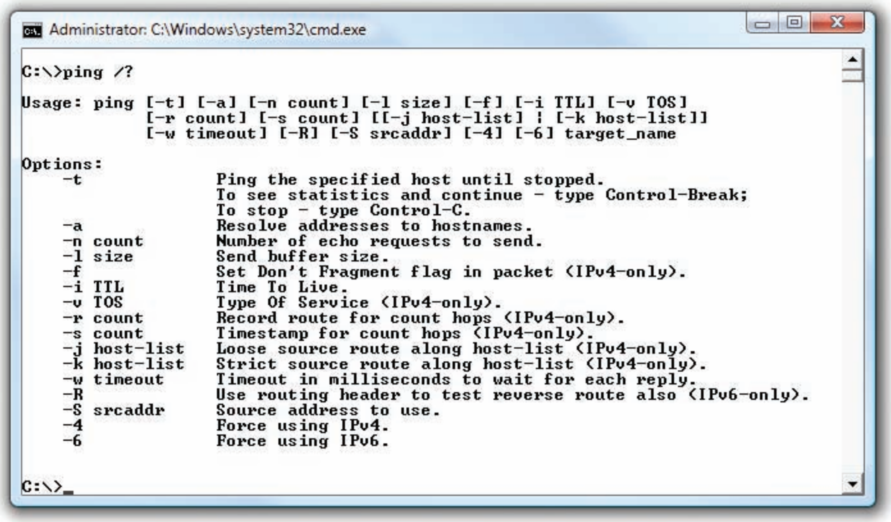
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

• Figure 22.41 Automatically obtaining an IP address

TCP/IP Tools

All versions of Windows come with handy tools to test and configure TCP/IP. Those you're most likely to use in the field are ping, ipconfig, nslookup, and tracert. All of these programs are command-line utilities. Open a command prompt to run them; if you just place these commands in the Run or Search dialog box, you'll see the Command Prompt window open for a moment and then quickly close!

ping You've already encountered ping, a really great way to see if you can talk to another system. Here's how it works. Get to a command prompt and type **ping** followed by an IP address or by a DNS name, such as **ping www.chivalry.com**. Press the ENTER key on your keyboard and away it goes! Figure 22.42 shows the common syntax for ping.



```
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.

C:\>_
```

• Figure 22.42 The ping command's syntax

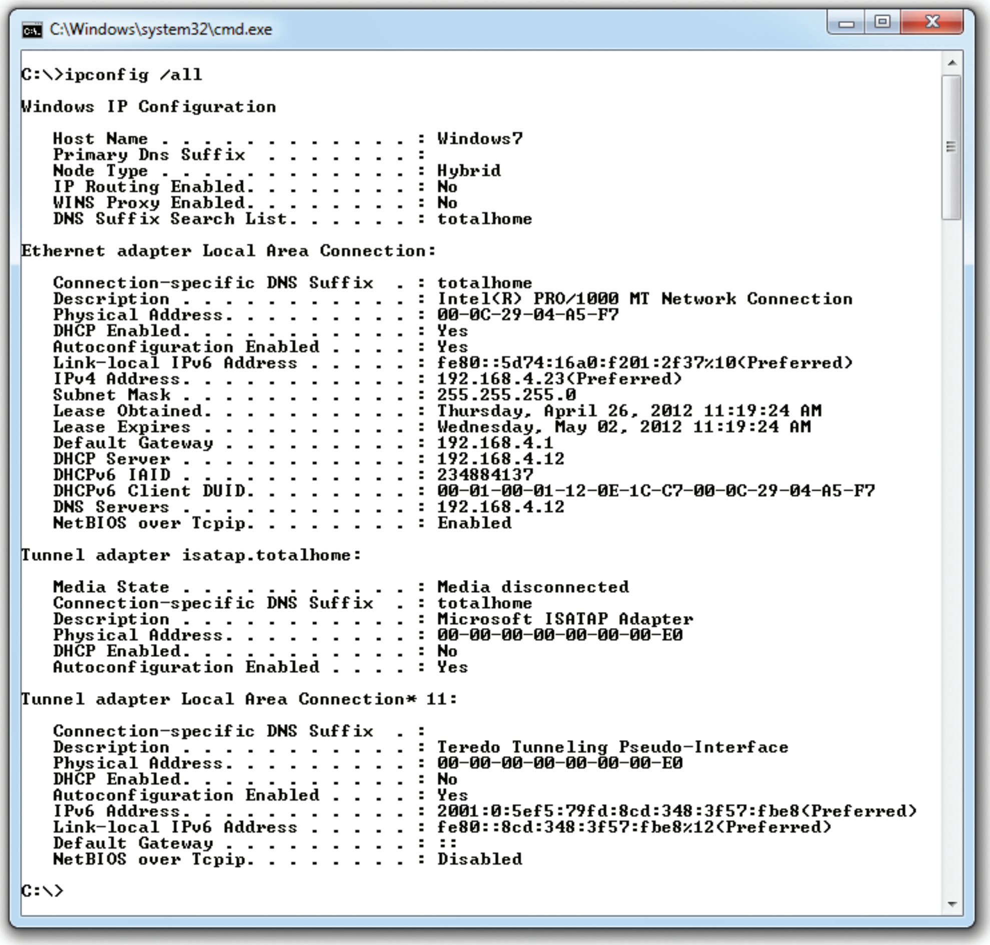
The ping command has a few useful options beyond the basics. The first option is the –t switch. If you use the –t switch, ping continuously sends ping packets until you stop it with the break command (CTRL-C). The second option is the –l switch, which enables you to specify how big a ping packet to send. This helps in diagnosing specific problems with the routers between your computer and the computer you ping.

ipconfig Windows offers the command-line tool **ipconfig** for a quick glance at your network settings. From a command prompt, type **ipconfig/ all** to see all of your TCP/IP settings (see Figure 22.43).

When you have a static IP address, ipconfig does little beyond reporting your current IP settings, including your IP address, subnet mask, default gateway, DNS servers, and WINS servers. When using DHCP, however, ipconfig is also the primary tool for releasing and renewing your IP address. Just type **ipconfig /renew** to get a new IP address or **ipconfig /release** to give up the IP address you currently have.

nslookup The **nslookup** command is a powerful command-line program that enables you to determine exactly what information the DNS server is

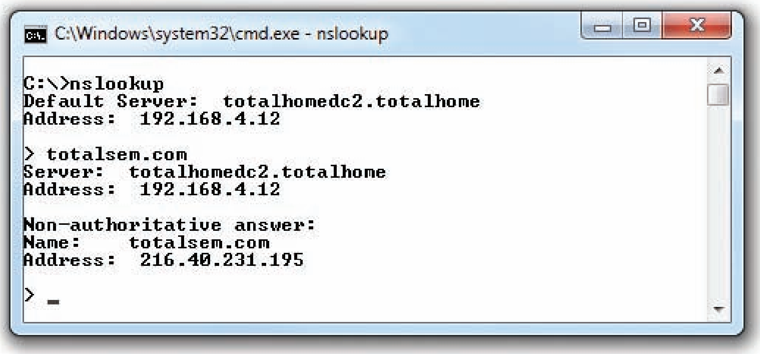
You can do some cool stuff with nslookup, and consequently some techs absolutely love the tool. It's way outside the scope of CompTIA A+ certification, but if you want to play with it, type **help** at the nslookup prompt and press ENTER to see a list of common commands and syntax.



```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Windows7
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : totalhome

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : totalhome
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-04-A5-F7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d74:16a0:f201:2f37%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.4.23(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, April 26, 2012 11:19:24 AM
   Lease Expires . . . . . . . . . . : Wednesday, May 02, 2012 11:19:24 AM
   Default Gateway . . . . . . . . . : 192.168.4.1
   DHCP Server . . . . . . . . . . . : 192.168.4.12
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-12-0E-1C-C7-00-0C-29-04-A5-F7
   DNS Servers . . . . . . . . . . . : 192.168.4.12
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.totalhome:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : totalhome
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fd:8cd:348:3f57:fbe8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::8cd:348:3f57:fbe8%12(Preferred)
   Default Gateway . . . . . . . . . : ::
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\>
```

• **Figure 22.43** An ipconfig /all command on Windows 7

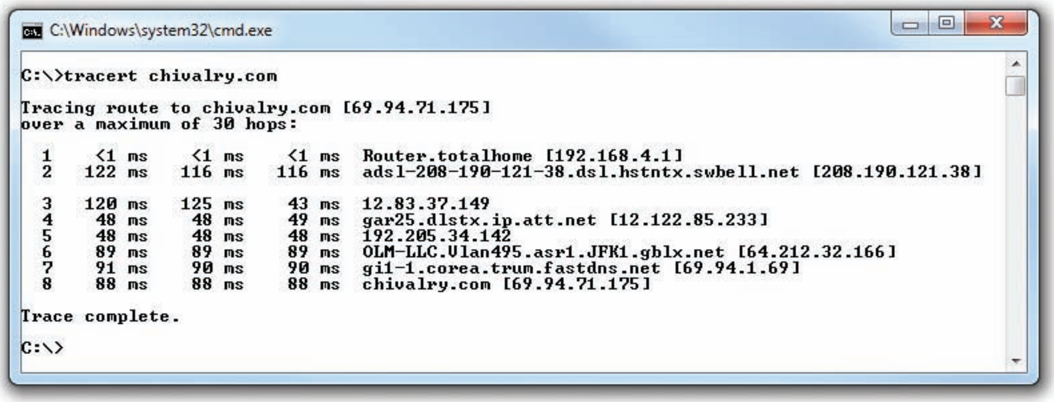
giving you about a specific host name. Every version of Windows makes nslookup available when you install TCP/IP. To run the program, type **nslookup** from the command prompt and press the ENTER key (see Figure 22.44). Note that this gives you a little information and that the prompt has changed. That's because you're running the application. Type **exit** and press the ENTER key to return to the command prompt.



```
C:\>nslookup
Default Server:  totalhomedc2.totalhome
Address:  192.168.4.12

> totalsem.com
Server:  totalhomedc2.totalhome
Address:  192.168.4.12

Non-authoritative answer:
Name:    totalsem.com
Address:  216.40.231.195

> _
```

• **Figure 22.44** The nslookup command in action

tracert The **tracert** utility shows the route that a packet takes to get to its destination. From a command line, type **tracert** followed by a space and an IP address or URL. The output describes the route from your machine to the destination machine, including all devices the packet passes through and how long each hop between devices takes (see Figure 22.45). The tracert command can come in handy when you have to troubleshoot bottlenecks. When users complain of difficulty reaching a particular



```
C:\>tracert chivalry.com

Tracing route to chivalry.com [69.94.71.175]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Router.totalhome [192.168.4.1]
  2   122 ms   116 ms   116 ms  adsl-208-190-121-38.dsl.hstntx.swbell.net [208.190.121.38]

  3   120 ms   125 ms    43 ms  12.83.37.149
  4    48 ms    48 ms    49 ms  gar25.dlstx.ip.att.net [12.122.85.233]
  5    48 ms    48 ms    48 ms  192.205.34.142
  6    89 ms    89 ms    89 ms  OLM-LLC.Vlan495.asr1.JFK1.gblx.net [64.212.32.166]
  7    91 ms    90 ms    90 ms  gi1-1.corea.trum.fastdns.net [69.94.1.69]
  8    88 ms    88 ms    88 ms  chivalry.com [69.94.71.175]

Trace complete.

C:\>
```

• Figure 22.45 The tracert command in action

destination by using TCP/IP, you can run this utility to determine whether the problem exists on a machine or connection over which you have control, or if it is a problem on another machine or router. Similarly, if a destination is completely unreachable, tracert can again determine whether the problem is on a machine or router over which you have control.

Try This!

Running tracert

Ever wonder why your e-mail takes *years* to get to some people but arrives instantly for others? Or why some Web sites are slower to load than others? Part of the blame could lie with how many hops away your connection is from the target server. You can use tracert to run a quick check of how many hops it takes to get to somewhere on a network, so Try This!

1. Run tracert on some known source, such as www.microsoft.com or www.totalsem.com. How many hops did it take? Did your tracert time out or make it all of the way to the server?
2. Try a tracert to a local address. If you're in a university town, run a tracert on the campus Web site, such as www.rice.edu for folks in Houston, or www.ucla.edu for those of you in Los Angeles. Did you get fewer hops with a local site?

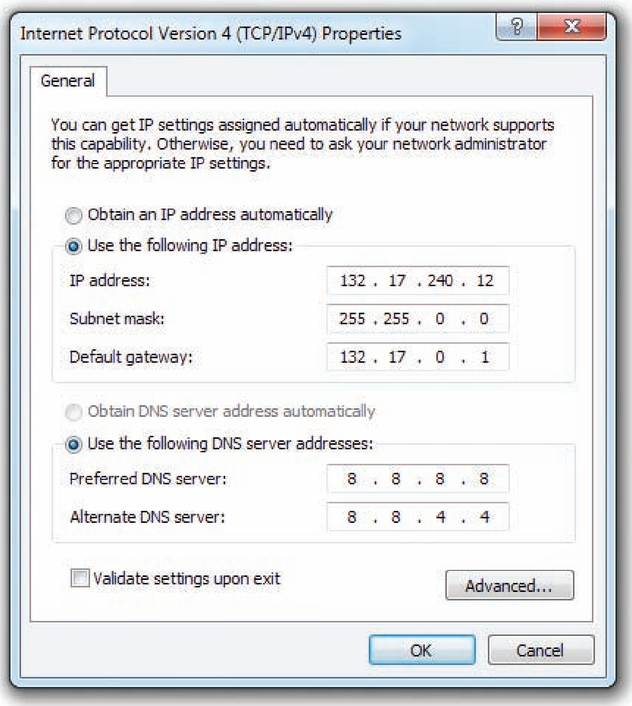
Configuring TCP/IP

By default, TCP/IP is configured to receive an IP address automatically from a DHCP server on the network (and automatically assign a corresponding subnet mask). As far as the CompTIA A+ certification exams are concerned, Network+ techs and administrators give you the IP address, subnet mask, and default gateway information and you plug them into the PC. That's about it, so here's how to do it manually:

1. In Windows XP, open the Control Panel and double-click the Network Connections applet. Double-click the Local Area Connection icon. In Windows Vista/7, open the Control Panel and go to the Network and Sharing Center applet. In Windows Vista, click the *Manage network connections* link, and in Windows 7, click *Change adapter settings*. After that, double-click the Local Area Network icon.
2. Click the Properties button, highlight Internet Protocol (TCP/IP), and click the Properties button. In Windows Vista/7, you should highlight Internet Protocol Version 4 (TCP/IPv4), as opposed to

IPv6, which you'll learn about later in this chapter.

3. In the Properties dialog box (see Figure 22.46), click the radio button next to *Use the following IP address*.
4. Enter the IP address in the appropriate fields.
5. Press the TAB key to skip down to the Subnet mask field. Note that the subnet mask is entered automatically, although you can type over this if you want to enter a different subnet mask.
6. Optionally, enter the IP address for a default gateway.
7. Optionally, enter the IP addresses of a primary DNS server and a secondary DNS server. (Figure 22.46 uses the Google DNS servers.)
8. Click the OK button to close the Properties dialog box.
9. Click the Close button to exit the Local Area Connection Status dialog box.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 132 . 17 . 240 . 12

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 132 . 17 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

□ Validate settings upon exit

• Figure 22.46 Setting up IP

Automatic Private IP Addressing

Windows supports a feature called Automatic Private IP Addressing (APIPA) that automatically assigns an IP address to the system when the client cannot obtain an IP address automatically. The Internet Assigned Numbers Authority, the nonprofit corporation responsible for assigning IP addresses and managing root servers, has set aside the range of addresses from 169.254.0.1 to 169.254.255.254 for this purpose.

If the computer system cannot contact a DHCP server, the computer randomly chooses an address in the form of 169.254.*x.y* (where *x.y* is the computer's identifier) and a 16-bit subnet mask (255.255.0.0) and broadcasts it on the network segment (subnet). If no other computer responds to the address, the system assigns this address to itself. When using APIPA, the system can communicate only with other computers on the same subnet that also use the 169.254.*x.y* range with a 16-bit mask. APIPA is enabled by default if your system is configured to obtain an IP address automatically.

A computer system on a network with an active DHCP server that has an IP address in this range usually indicates a problem connecting to the DHCP server.

IPv6

When the early developers of the Internet set out to create an addressing or naming scheme for devices on the Internet, they faced several issues. Of course they needed to determine how the numbers or names worked, and for that they developed the Internet Protocol and IP addresses. But beyond that, they had to determine how many computers might exist in the future, and then make the IP address space even bigger to give Internet naming longevity. But how many computers would exist in the future?

Keep in mind that TCP/IP development took place back in the early 1970s. There were fewer than 1000 computers in the entire *world* at the time, but that didn't keep the IP developers from thinking big! They decided to go absolutely crazy (as many people considered it at the time) and, in 1979, created the **Internet Protocol version 4 (IPv4)** 32-bit IP address space, creating approximately 4 billion IP addresses. That should have been fine for the foreseeable future!

It wasn't. First, the TCP/IP folks wasted huge chunks of IP addresses due to classful addressing and an easygoing method of parceling out IP addresses. Second, the Internet reached a level of popularity far beyond the original developers' imaginations. By the mid-1980s, the rate of consumption for IP addresses started to worry the Internet people and the writing was on the wall for IPv4's 32-bit addressing.

As a result, the Internet Engineering Task Force (IETF) developed a new IP addressing scheme called **Internet Protocol version 6 (IPv6)** that is slowly replacing IPv4. IPv6 extends the 32-bit IP address space to 128 bits, allowing up to 2^{128} addresses! That should hold us for the foreseeable future! This number—close to 3.4×10^{38} addresses—is something like all the grains of sand on Earth or 1/8 of all the molecules in the atmosphere.

Although they achieve the same function—enabling computers on IP networks to send packets to each other—IPv6 and IPv4 differ a lot when it comes to implementation. This section provides you with a quick overview to get you up to speed with IPv6 and show you how it differs from IPv4.

If you really want to know how many IP addresses IPv6 provides, here's your number: 340,282,366,920,938,463,463,374, 607,431,768,211,456.

For those who don't play with hex regularly, one hexadecimal character (for example, *F*) represents 4 bits, so four hexadecimal characters make a 16-bit group. For some reason, the IPv6 developers didn't provide a name for the "group of four hexadecimal characters," so many techs and writers have taken to calling them fields or "hextets" to distinguish them from IPv4 "octets."

IPv4 addresses use 32 bits, and IPv6 addresses use 128 bits. Be sure you can identify their address length differences and address conventions.

IPv6 Address Notation

The familiar 32-bit IPv4 addresses are written as 197.169.94.82, using four octets. The 128-bit IPv6 addresses are written like this:

2001:0000:0000:3210:0800:200C:00CF:1234

IPv6 uses a colon as a separator, instead of the period used in IPv4's dotted-decimal format. Each "group" is a hexadecimal number between 0000 and FFFF called, unofficially, a *field* or *hextet*.

A complete IPv6 address always has eight groups of four hexadecimal characters. If this sounds like you're going to type in really long IP addresses, don't worry, IPv6 offers a number of ways to shorten the address in written form.

First, leading zeros can be dropped from any group, so 00CF becomes CF and 0000 becomes 0. Let's rewrite the previous IPv6 address using this shortening method:

2001:0:0:3210:800:200C:CF:1234

Second, you can remove one or more consecutive groups of all zeros, leaving the two colons together. For example, using the :: rule, you can write the IPv6 address

2001:0:0:3210:800:200C:CF:1234

as

2001::3210:800:200C:CF:1234

You can remove any number of consecutive groups of zeros to leave a double colon, but you can only use this trick *once* in an IPv6 address.

Take a look at this IPv6 address:

FEDC:0000:0000:0000:00CF:0000:BA98:1234

Using the double-colon rule, you can reduce four groups of zeros; three of them follow the FEDC and the fourth comes after 00CF. Because of the "only use once" stipulation, the best and shortest option is to convert the address to

FEDC::CF:0:BA98:1234

You may not use a second :: to represent the fourth groups of zeros—only one :: is allowed per address! This rule exists for a good reason. If more than one :: was used, how could you tell how many groups of zeros were in each group? Answer: you couldn't.

Here's an example of a very special IPv6 address that takes full advantage of the double-colon rule, the IPv6 loopback address:

::1

The unspecified address (all zeros) can never be used, and neither can an address that contains all ones (in binary) or all *F*s (in hex notation).

Without using the double-colon nomenclature, this IPv6 address would look like this:

0000:0000:0000:0000:0000:0000:0000:0001

IPv6 still uses subnets, but you won't find a place to type in 255s anywhere. IPv6 uses the "/*x*" *Classless Inter-Domain Routing* (*CIDR*) nomenclature, where the /*x* refers to the number of bits in the subnet mask, just like in IPv4. Here's how to write an IP address and subnet for a typical IPv6 host:

FEDC::CF:0:BA98:1234/64

Where Do IPv6 Addresses Come From?

Every computer running IPv6 will always have at least a link-local address.

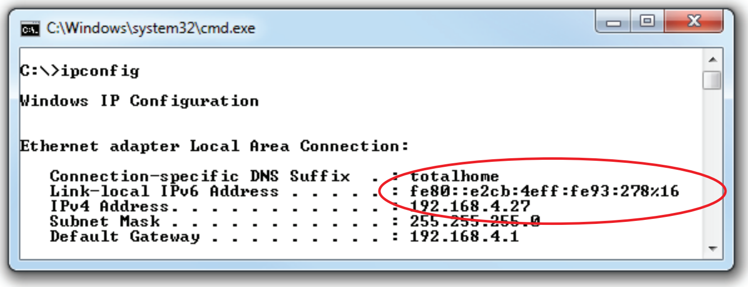
With IPv4, IP addresses come from one of two places: either you type in the IP address yourself (*static IP addressing*) or you use DHCP (also called *dynamic IP addressing*). With IPv6, addressing works very differently. Instead of one IP address, you can have up to three IP addresses on a single network card.

If you want to force Windows to use the MAC address, just go to a command prompt and type this:

```
netsh interface ipv6
set global randomize
identifiers= disabled
```

When a computer running IPv6 first boots up, it gives itself a *link-local address*, IPv6's equivalent to IPv4's APIPA address. Although an APIPA address can indicate a loss of network connectivity or a problem with the DHCP server, computers running IPv6 always have a link-local address. The first 64 bits of a link-local address are always FE80::. That means every address always begins with FE80:0000:0000:0000. If your operating system supports IPv6 and IPv6 is enabled, you can see this address. Figure 22.47 shows the link-local address for a typical system running the ipconfig utility.

The folks who designed IPv6 gave operating system makers a choice on how to make the last 64 bits of an IPv6 address. The first method uses a random value—and this is the way Windows does it. When you activate a NIC, Windows simply makes a random value for the last 64 bits of the IPv6 address. Once created, this unique 64-bit value will never change.



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : totalhome
   Link-local IPv6 Address . . . . . : fe80::e2cb:4eff:fe93:278%16
   IPv4 Address. . . . . . . . . . . : 192.168.4.27
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.4.1
```

• **Figure 22.47** Link-local address in ipconfig

The alternative method to create the IPv6 address uses the MAC address of the network card (called the *Extended Unique Identifier, 64-bit*, or *EUI-64*). Be warned! The CompTIA A+ exams are Windows-centric, and Windows does not use this second method by default. Even though Windows does not currently use this method by default, understanding this is critical to understanding IPv6.

A router solicitation message uses the address FF02::2. This address is read only by other computers running IPv6 in the network. This type of address is different from a broadcast address and is called a *multicast address*. In IPv6, there is no broadcast, only multicast!

IPv6 Subnet Masks

IPv6 subnets function the same as IPv4 subnets, but you need to know two new rules:

- The last 64 bits of an IPv6 address are generated randomly or using the MAC address, leaving a maximum of 64 bits for the network ID. Therefore, no subnet is ever longer than /64.
- The IANA passes out /32 subnets to big ISPs and end users who need large allotments. ISPs and others may pass out /48 and /64 subnets to end users.

Therefore, the vast majority of IPv6 subnets are between /48 and /64.

Subnet masks are just as important in IPv6 networks as they are in IPv4 networks. Unlike with IPv4 networks, however, all IPv6 networks with computers have a /64 subnet mask, so you'll rarely if ever need to make any changes manually.

Most Windows Vista and Windows 7 machines have three IPv6 addresses: one link local address and two global addresses. One global address stays the same, while the second is a temporary address used to make it harder for your system to be tracked by IP address.

Global Addresses

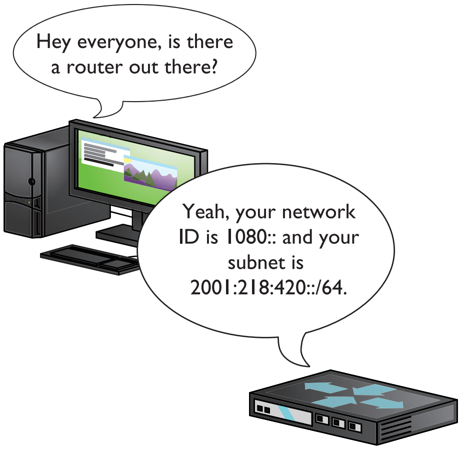
To get on the Internet, a system needs a second IPv6 address called a *global address*. The most common way to get a global address is to request it from the default gateway router, which must be configured to pass out global IPv6 addresses. When you plug a computer into a network, it sends out a very special packet called a *router solicitation* (*RS*) message, looking for a router (see Figure 22.48). The router hears this message and responds with a *router advertisement* (*RA*). This RA tells the computer its network ID and subnet (together called the *prefix*) and DNS server (if configured).

At the moment, IANA only passes out global addresses that begin with the number 2 (for example, 2001::, 2002::, and so on). As demand increases, this will certainly change, but for now, knowing a global address when you see one is easy.

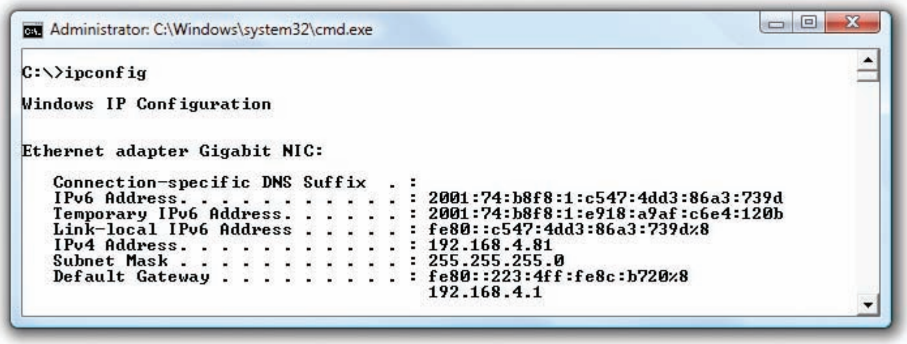
Once the computer gets a prefix, it generates the rest of the address just like with the link-local address. The computer ends up with a legitimate, 128-bit public IPv6 address as well as a link-local address. Figure 22.49 shows the IPv6 information in Windows 7.

Let's look at this process in detail with an example:

1. An IPv6-capable computer boots up. As it boots, it sends out a router solicitation message (FF02::2).
2. An IPv6-configured router hears the request and then sends to the computer a router advertisement containing the prefix and DNS. In this example, let's say it is 2001:470:ABCD:1/64.
3. The computer takes the prefix and adds the EUI-64 or a random value to the end of the prefix. If the MAC address is 00-0C-29-53-45-CA, then the address is 20C:29FF:FE53:45CA.
4. Putting the prefix with the last half of the address, you get the global address: 2001:470:ABCD:1:20C:29FF:FE53:45CA.


Hey everyone, is there a router out there?
Yeah, your network ID is 1080:: and your subnet is 2001:218:420::/64.

• Figure 22.48 Getting a global address



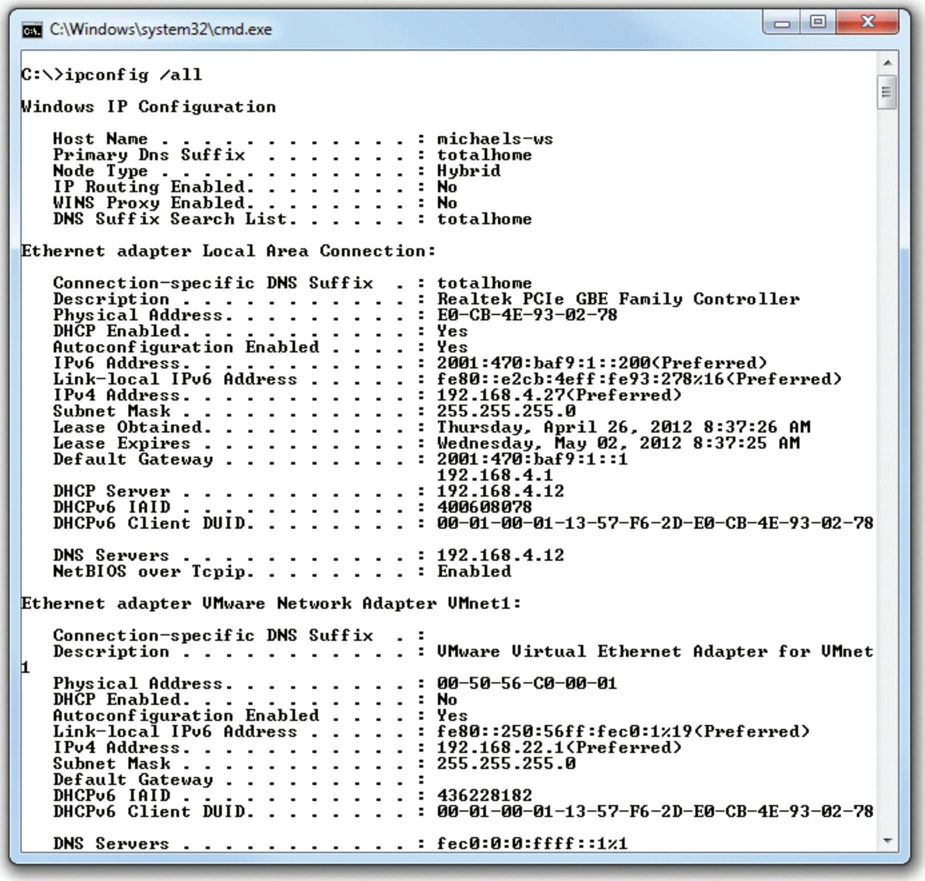
```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Gigabit NIC:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:74:b8f8:1:c547:4dd3:86a3:739d
   Temporary IPv6 Address. . . . . . : 2001:74:b8f8:1:e918:a9af:c6e4:120b
   Link-local IPv6 Address . . . . . : fe80::c547:4dd3:86a3:739d%8
   IPv4 Address. . . . . . . . . . . : 192.168.4.81
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::223:4ff:fe8c:b720%8
                                       192.168.4.1
```

• Figure 22.49 Windows system with a global IPv6 address

A global address is a true Internet address. If another computer is running IPv6 and also has a global address, it can access your system unless you have some form of firewall.

The addition of IPv6 makes programs such as ipconfig fairly complex. Take a look at Figure 22.50. With multiple NICs and both IPv4 and IPv6, the output is vast—too big to even put on a single screen.

Computers using IPv6 need a *global* address to access the Internet.



```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : michaels-ws
   Primary Dns Suffix  . . . . . . . : totalhome
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : totalhome

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : totalhome
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : E0-CB-4E-93-02-78
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:470:baf9:1::200(Preferred)
   Link-local IPv6 Address . . . . . : fe80::e2cb:4eff:fe93:278%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.4.27(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, April 26, 2012 8:37:26 AM
   Lease Expires . . . . . . . . . . : Wednesday, May 02, 2012 8:37:25 AM
   Default Gateway . . . . . . . . . : 2001:470:baf9:1::1
                                       192.168.4.1
   DHCP Server . . . . . . . . . . . : 192.168.4.12
   DHCPv6 IAID . . . . . . . . . . . : 400608078
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-57-F6-2D-E0-CB-4E-93-02-78

   DNS Servers . . . . . . . . . . . : 192.168.4.12
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::250:56ff:fec0:1%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.22.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 436228182
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-57-F6-2D-E0-CB-4E-93-02-78

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
```

• Figure 22.50 The ipconfig command with IPv6 and IPv4

Installing and Configuring a Wired Network

Halfway through the chapter and we're finally getting to the good stuff: installing and configuring a network! To have network connectivity, you need to have three things in place:

- **NIC** The physical hardware that connects the computer system to the network media
- **Protocol** The language that the computer systems use to communicate
- **Network client** The interface that allows the computer system to speak to the protocol

If you want to share resources on your PC with other network users, you also need to enable Microsoft's File and Printer Sharing. Plus, of course, you need to connect the PC to the network switch via some sort of cable (preferably CAT 6 with Gigabit Ethernet cranking through the wires, but that's just me!). When you install a NIC, by default Windows installs upon setup the TCP/IP protocol, the Client for Microsoft Networks, and File and Printer Sharing for Microsoft Networks.

Installing a NIC

The NIC is your computer system's link to the network, and installing one is the first step required to connect to a network. NICs are manufactured to operate on specific media and network types, such as 1000BaseT Ethernet. Follow the manufacturer's instructions for installation. If your NIC is of recent vintage, it will be detected, installed, and configured automatically by Windows. You might need a driver disc or a driver download from the manufacturer's Web site.

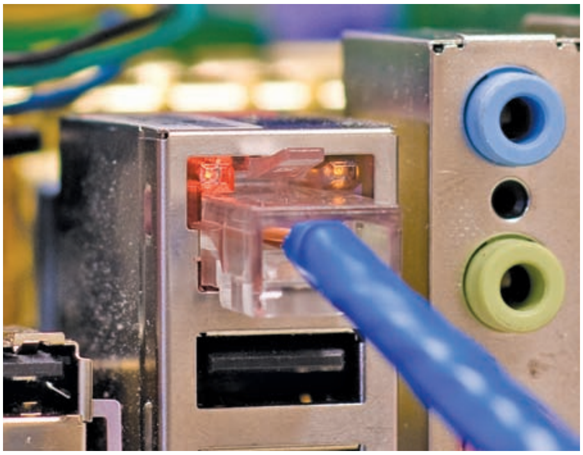
The Add Hardware Wizard in Windows XP automates installation of non–plug-and-play devices or plug-and-play devices that were not detected correctly. Start the wizard by clicking Start | Control Panel and then double-clicking the icon for the Add Hardware applet. Click the Next button to select the hardware task you wish to perform, and follow the prompts to complete the wizard. If, for some reason, Windows Vista or Windows 7 doesn't automatically detect a new NIC after you turn the PC back on, go to Start | Control Panel | Add Hardware in Windows Vista or Start | Devices and Printers and click on *Add a device* in Windows 7 to install it.

Duplex and Half-Duplex

All modern NICs can run in **full-duplex** mode, meaning they can send and receive data at the same time. The vast majority of NICs and switches use a feature called *auto-sensing* to accommodate very old devices that might attach to the network and need to run in half-duplex mode. Half-duplex means that the device can send and receive, but not at the same time. An obvious example of a half-duplex device is the walkie-talkies you played with as a kid that required you to press and hold the orange button to transmit—at which time you couldn't hear anything. Half-duplex devices are exceedingly rare in modern computers, but you need to understand this option. Some NICs just can't handle full-duplex communication when you connect them directly to another NIC by using a crossover cable—that is, no switch. Dropping both NICs down from full-duplex or auto-sensing can sometimes enable these odd NICs to communicate.

Link Lights

NICs made today have some type of light-emitting diode (LED) *status indicator* that gives information about the state of the NIC's link to whatever is on the other end of the connection. Even though you know the lights are actually LEDs, get used to calling them **link lights**, because that's the term all network techs use. NICs can have between one and four different link lights, and the LEDs can be any color. These lights give you clues about what's happening with the link and are one of the first items to check whenever you think a system is disconnected from the network (see Figure 22.51).

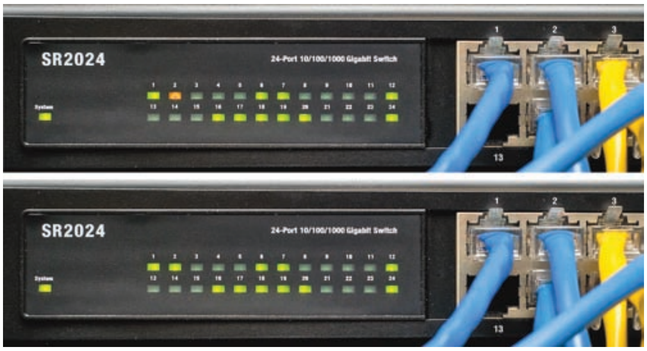


• Figure 22.51 Mmmm, pretty lights!

Switches also have link lights, enabling you to check the connectivity at both ends of the cable. If a PC can't access a network, always check the link lights first. Multispeed devices usually have a link light that tells you the speed of the connection. In Figure 22.52, the light for port 2 on the top photo is orange, for example, signifying that the other end of the cable is plugged into either a 10BaseT or 100BaseT NIC. The same port connected to a Gigabit NIC—that's the lower picture—displays a green LED.

A properly functioning link light is steady on when the NIC is connected to another device. No flickering, no on and off, just on. A link light that is off or flickering shows a connection problem.

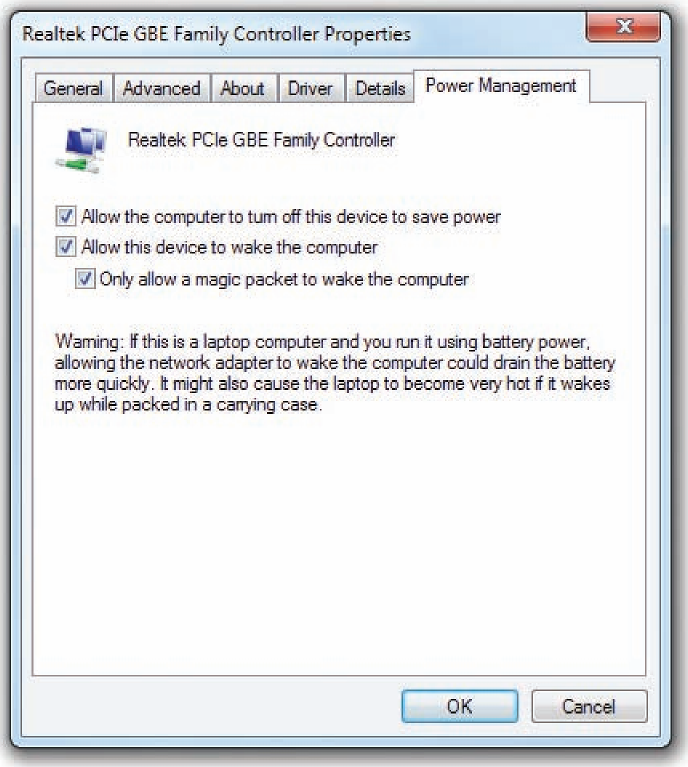
Another light is the **activity light**. This little guy turns on when the card detects network traffic, so it makes an intermittent flickering when operating properly. The activity light is a lifesaver for detecting problems, because in the real world, the connection light sometimes lies to you. If the connection light says the connection is good, the next step is to try to copy a file or do something else to create network traffic. If the activity light does not flicker, you have a problem.


SR2024
24-Port 10/100/1000 Gigabit Switch
SR2024
24-Port 10/100/1000 Gigabit Switch

• Figure 22.52 Multispeed lights

Though no real standard exists for NIC LEDs, the CompTIA A+ exams will test you on some more-or-less *de facto* LED meanings. You should know that a solid green light means connectivity, a flashing green light means intermittent connectivity, no green light means no connectivity, and a flashing amber light means there are collisions on the network (which is sometimes okay). Also, know that the first things you should check when having connectivity issues are the NIC's LEDs.

No standard governs how NIC manufacturers use their lights; as a result, LEDs in NICs come in an amazing array of colors and layouts. When you encounter a NIC with a number of LEDs, take a moment to try to figure out what each one means. Although different NICs have different ways of arranging and using their LEDs, the functions are always the same: link, activity, and speed.


Realtek PCIe GBE Family Controller Properties

Realtek PCIe GBE Family Controller

☑ Allow the computer to turn off this device to save power

☑ Allow this device to wake the computer

☑ Only allow a magic packet to wake the computer

Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.

• Figure 22.53 Wake-on-LAN settings on the Power Management tab

Wake-on-LAN

A popular feature of most NICs is the ability to turn on or wake up a powered-down or sleeping PC. You'll learn more about power management in Chapter 26, but for now, know that *Wake-on-LAN* is handy when you want to wake up one or multiple computers that you aren't physically near. To wake up a PC with Wake-on-LAN, you'll need to use a second PC to send either a special pattern or a *magic packet* (a broadcast packet that essentially repeats the destination MAC address many times).

A powered-down or sleeping PC knows to look for this special pattern or packet, at least after configured to do so. In Windows XP, go to the Control Panel and open Network Connections. In Windows Vista/7, go to the Control Panel and open Network and Sharing Center. Click *Manage network connections* (Vista) or *Change adapter settings* (7) on the left. For all versions of Windows, right-click on the adapter and select Properties. Click the Configure button in the Properties dialog box and then select the Power Management tab (see Figure 22.53). To enable Wake-on-LAN, make sure the checkbox next to *Allow this device to wake the computer* is checked. Optionally, you can select *Only allow a magic packet to wake the computer*, which will instruct the NIC to ignore everything but magic packets.

Wake-on-LAN is very convenient, but it has one nasty downside. As noted in the Properties dialog box, Wake-on-LAN can wake up or turn on laptops using wireless connections, even when they aren't plugged in or are inside a carrying case. Don't let your laptop's battery die or overheat—unless you know that you'll need it, turn off Wake-on-LAN on your laptop.

Your BIOS might also have settings for controlling Wake-on-LAN functions. Check your CMOS System Configuration tool to find out.

Configuring a Network Client

To establish network connectivity, you need a network client installed and configured properly. Let's look at Microsoft's client.

Installed as part of the OS installation, the Client for Microsoft Networks rarely needs configuration, and, in fact, few configuration options are available. To start it in Windows Vista/7, click Start, right-click Network, and select Properties. Then click *Manage network connections* (Vista) or *Change* *adapter settings* (7) on the left. In Windows XP, click Start, right-click My Network Places, and select Properties.

In all versions of Windows, the next step is to double-click the Local Area Connection icon, click the Properties button, and highlight Client for Microsoft Networks. In Windows XP/Vista, click the Properties button. Windows 7 disables this option. Note, however, that there's not much to do here. Unless told to do something by a network administrator, just leave this alone.

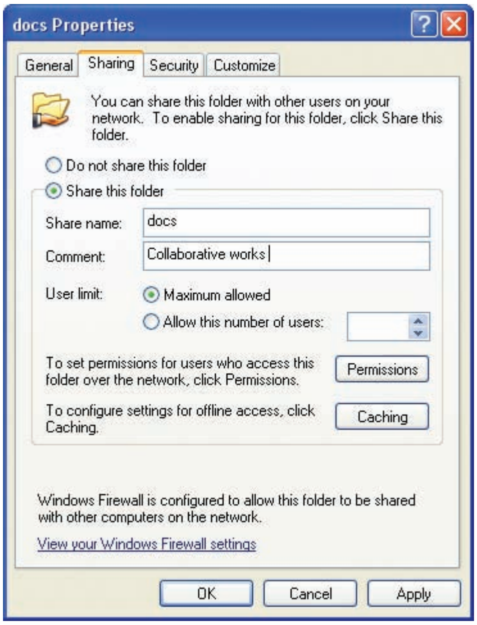
Sharing and Security

Windows systems can share all kinds of **resources**: files, folders, entire drives, printers, faxes, Internet connections, and much more. Conveniently for you, the scope of the CompTIA A+ certification exams is limited to folders, printers, and Internet connections. You'll see how to share folders and printers now; Internet connection sharing is discussed in Chapter 24.

Sharing Drives and Folders

All versions of Windows share drives and folders in basically the same manner. Right-click any drive or folder and choose Properties. Select the Sharing tab (see Figure 22.54). In Windows Vista/7, click the Advanced Sharing button. Select *Share this folder*, add something in the Comment or User limit fields if you wish (they're not required), and click Permissions (see Figure 22.55).

Hey! Doesn't NTFS have all those wild permissions such as Read, Execute, Take Ownership, and all that? Yes, it does, but NTFS permissions and network permissions are totally separate beasties. Microsoft wanted Windows to support many different file systems (NTFS, FAT16, FAT32), old and



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: docs

Comment: Collaborative works

User limit: ● Maximum allowed

○ Allow this number of users:

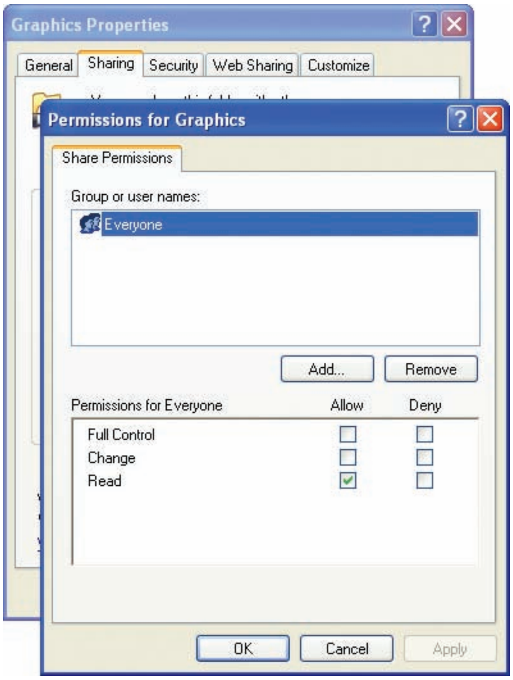
To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

Windows Firewall is configured to allow this folder to be shared with other computers on the network.

View your Windows Firewall settings

• **Figure 22.54** Windows XP Sharing tab on NTFS volume



Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

• **Figure 22.55** Network permissions

new. Network permissions are Microsoft's way of enabling you to administer file sharing on any type of partition supported by Windows, no matter how ancient. Sure, your options will be pretty limited if you are working with an older file system, but you *can* do it.

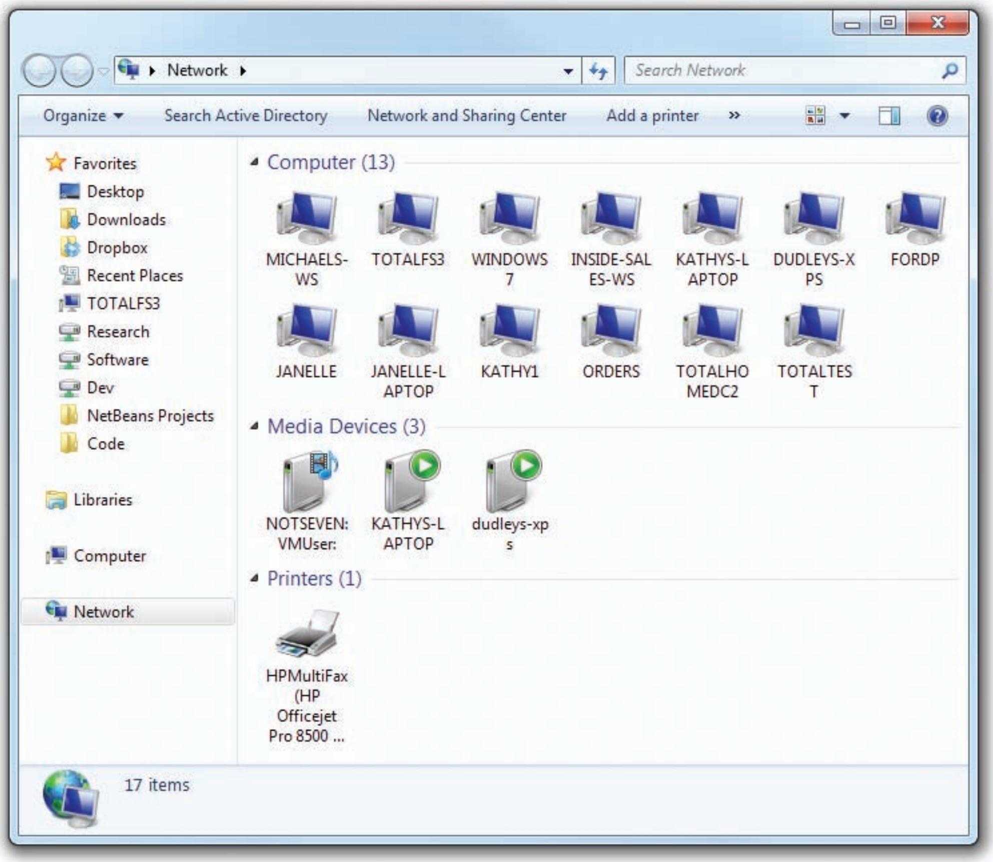
If you share a folder on an NTFS drive, as you normally do these days, you must set *both* the network permissions and the NTFS permissions to let others access your shared resources. Some good news: This is actually no big deal! Just set the network permissions to give everyone full control, and then use the NTFS permissions to exercise more precise control over *who* accesses the shared resources and *how* they access them. Open the Security tab to set the NTFS permissions.

Windows offers two types of sharing: share-level and NTFS permissions.

Accessing Shared Drives/Directories

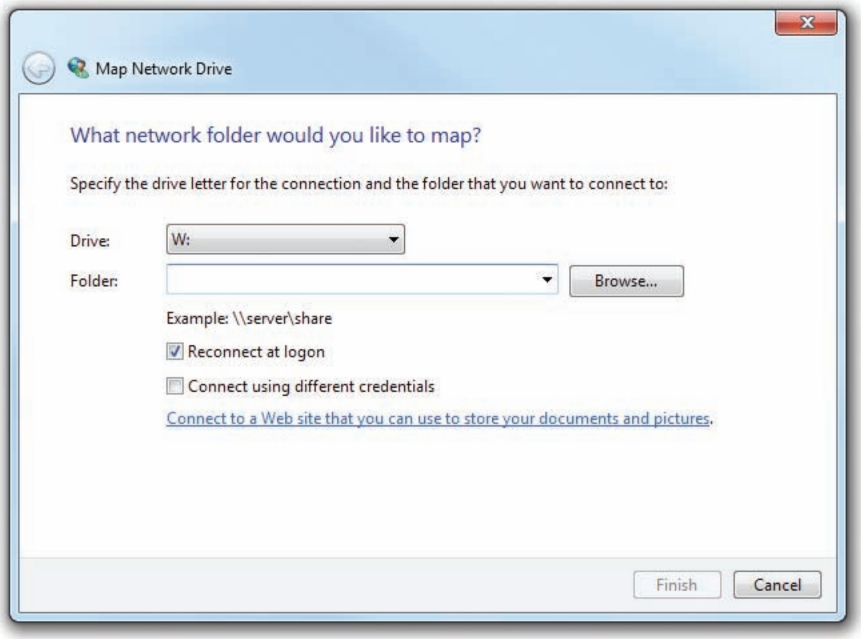
Once you have set up a drive or directory to be shared, the final step is to access that shared drive or directory from another machine. Windows XP uses My Network Places and Windows Vista and Windows 7 use Network, although you'll need to do a little clicking to get to the shared resources (see Figure 22.56).

You can also map network resources to a local resource name. For example, the FREDC share can be mapped to be a local hard drive such as E: or F:. From within any Explorer window (such as My Documents or Documents),



• Figure 22.56 Shared resources in Network choose Tools | Map Network Drive to open the Map Network Drive dialog box (see Figure 22.57). In Windows Vista/7, you might need to press the ALT key once to see the menu bar. Click the Browse button to check out the neighborhood and find a shared drive (see Figure 22.58).

Windows 2000 had the handy Add Network Place icon in My Network Places to add network locations you frequently access without using up drive letters. Windows XP removed the icon but added the menu option in its context bar on the left. Windows Vista and Windows 7 have removed it altogether but have added the ability to add links to network locations to your Favorites in Windows Explorer. Simply drag the network share, or


Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: W:

Folder:

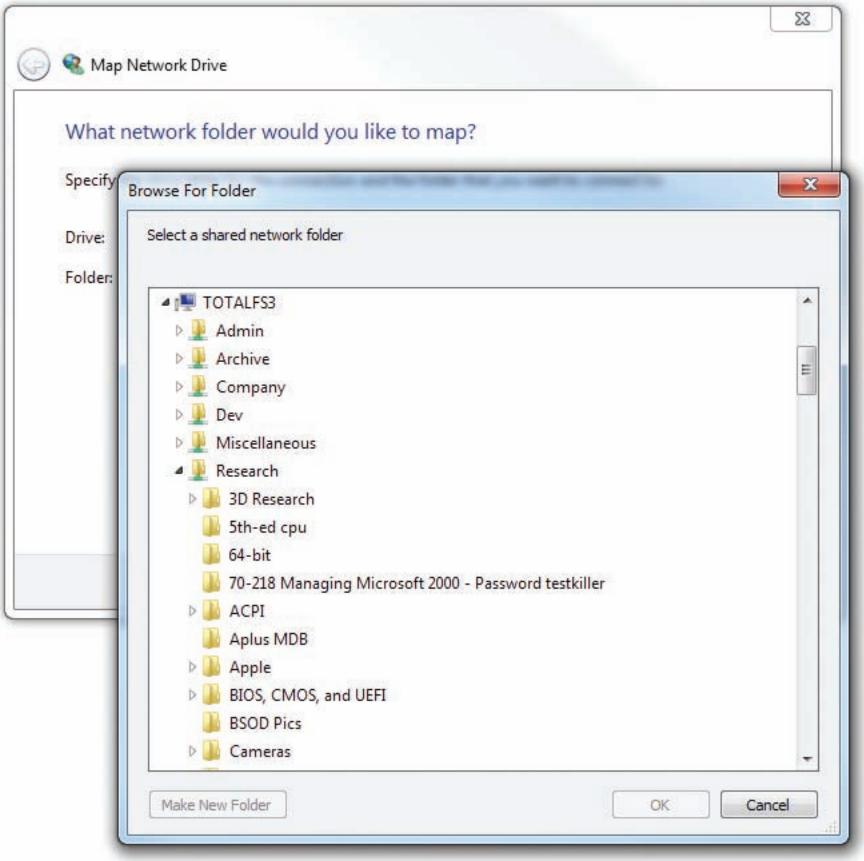
Example: \\server\share

☑ Reconnect at logon

☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

• **Figure 22.57** Map Network Drive dialog box in Windows 7


Map Network Drive

What network folder would you like to map?

Specify

Drive:

Folder:

Browse For Folder

Select a shared network folder

- TOTALFS3
  - Admin
  - Archive
  - Company
  - Dev
  - Miscellaneous
  - Research
    - 3D Research
    - 5th-ed cpu
    - 64-bit
    - 70-218 Managing Microsoft 2000 - Password testkiller
    - ACPI
    - Aplus MDB
    - Apple
    - BIOS, CMOS, and UEFI
    - BSOD Pics
    - Cameras

• **Figure 22.58** Browsing for shared folders any folder for that matter, to the Favorites list in the Navigation pane on the left. Figure 22.59 shows how it looks on a Windows 7 system.

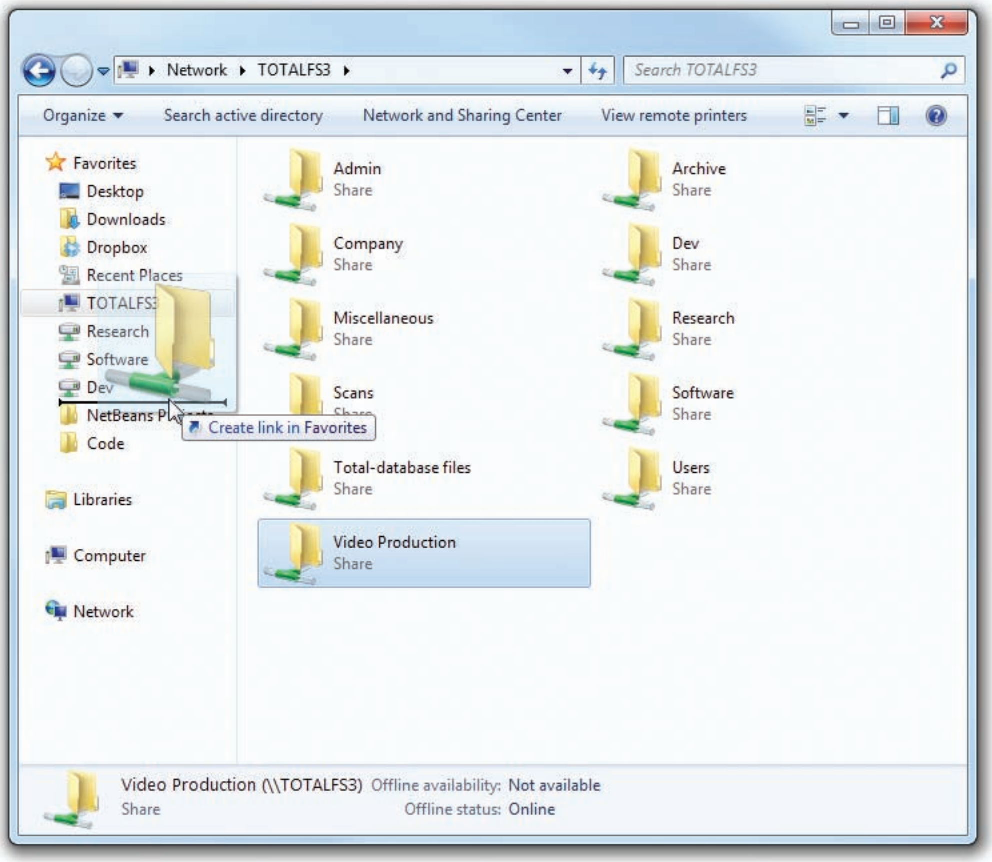
Mapping shared network drives is a common practice, as it makes a remote network share look like just another drive on the local system. The only downside to drive mapping stems from the fact that users tend to forget they are on a network. A classic example is the user who always accesses a particular folder or file on the network and then suddenly gets a “file not found” error when the workstation is disconnected from the network. Instead of recognizing this as a network error, the user often imagines the problem is a missing or corrupted file.

All shared resources should show up in My Network Places/Network. If a shared resource fails to show up, make sure you check the basics first: Is File and Printer Sharing activated? Is the device shared? Don’t let silly errors fool you!

UNC

All computers that share must have a network name, and all of the resources they share must also have network names. Any resource on a network can be described by combining the name of the resource being shared and the name of the system sharing it. If a machine called SERVER1 is sharing its C: drive as FREDC, for example, the complete name would look like this:

```
\\SERVER1\FREDC
```



Video Production (\\TOTALFS3) Offline availability: Not available
Share Offline status: Online

• **Figure 22.59** Adding a network location to the Windows 7 Navigation pane

This is called the **universal naming convention (UNC)**. The UNC is distinguished by its use of double backslashes in front of the sharing system's name and a single backslash in front of the shared resource's name. A UNC name can also point directly to a specific file or folder:

```
\\SERVER1\FREDC\INSTALL-FILES\SETUP.EXE
```

In this example, INSTALL-FILES is a subdirectory in the shared folder FREDC (which may or may not be called FREDC on the server), and SETUP .EXE is a specific file.

net

Windows enables you to view a network quickly from the command line through the **net command**. This works great when you plug into a network for the first time and, naturally, don't know the names of the other computers on that network. To see the many options that net offers, type **net** at a command prompt and press ENTER. The view and use options offer excellent network tools.

You can think of net view as the command-line version of My Network Places/Network. When run, net view returns a list of Windows computers on the network:

```
C:\Users\Mike>net view
Server Name            Remark
--------------------------------------------------
\\SABERTOOTH
\\UBERBOX
\\SERVER1


The command completed successfully.


C:\Users\Mike>
```

Once you know the names of the computers, you type **net view** followed by the computer name. The net view command will show any shares on that machine and whether they are mapped drives:

```
C:\>net view server1
Shared resources at SERVER1
Share name  Type  Used as  Comment
-------------------------------------------------------------
FREDC       Disk
Research    Disk  W:
The command completed successfully.
```

The net use command is a command-line method for mapping network shares. For example, if you wanted to map the Research share shown in the previous example to the X: drive, you simply type

```
C:\>net use x: \\server1\research
```

This will map drive X: to the Research share on the SERVER1 computer.

nbtstat

The nbtstat command is an old command-line utility that goes back to before Windows. It stands for NetBIOS over TCP/IP Statistics. Even though NetBIOS is long gone, it's still a great tool for learning anything "Windowsy" you want to know about your network, such as "What other workgroups or domains are on this network?" It's also is a great tool to answer the question, "Who am I connected to right now?" Try running **nbtstat –s** to see all your connections:

```
C:\>nbtstat -s
Local Area Connection:
Node IpAddress: [192.168.15.102] Scope Id: []
                    NetBIOS Connection Table
    Local Name        State    In/Out  Remote Host       Input Output
    ----------------------------------------------------------------
    UBERBOX   <00>  Connected   Out    SABERTOOTH  <20>    1KB  769B
    UBERBOX   <00>  Connected   Out    AARONV      <20>   760B  606B
    UBERBOX   <00>  Connected   Out    AARONV      <20>   950B  695B
    UBERBOX   <00>  Connected   Out    THEATER     <20>   620B  659B
    UBERBOX         Connected   In     SABERTOOTH  <00>  649KB  791KB
C:\>
```

Note that nbtstat –s shows every connection, even if two computers have multiple connections. You can also use nbtstat with the –c command for a more abbreviated list:

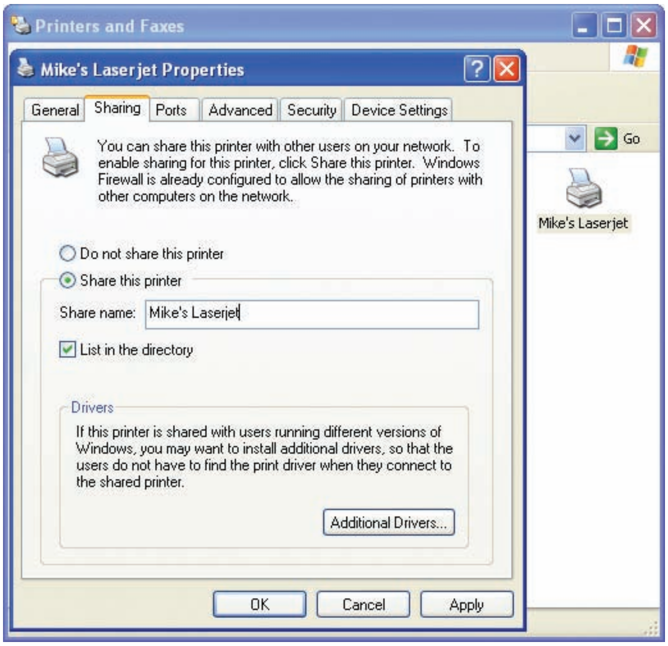
```
C:\>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.15.102] Scope Id: []

                   NetBIOS Remote Cache Name Table
        Name            Type       Host Address    Life [sec]
    ------------------------------------------------------------
    AARONV       <20>  UNIQUE      192.168.15.100      327
    SABERTOOTH   <20>  UNIQUE      192.168.15.101      485
    THEATER      <20>  UNIQUE      192.168.15.201      380
C:\>
```

To learn about accessing shared printers in Windows, check out Chapter 28 for more information.

Sharing Printers

Sharing printers in Windows follows the same process as sharing drives and folders. Assuming that the system has printer sharing services loaded, in Windows XP and Vista go to the Printers folder in the Control Panel or Start menu and right-click the printer you wish to share. Select Sharing, and then click *Share this printer* and give it a name (see Figure 22.60). In Windows 7, choose Start | Devices and Printers, right-click on the printer you wish to share, select Printer properties, and then select the Sharing tab. From here it's just like XP and Vista—click *Share this printer* and you're done.

One of the most pleasant aspects of configuring a system for networking under all versions of Microsoft Windows is the amazing amount of the process that is automated. For example, if Windows detects a NIC in a system, it automatically installs the NIC driver, a network protocol (TCP/IP), and Client for Microsoft Networks. So if you want to share a resource, everything you need is automatically installed. Note that although File and Printer Sharing is also automatically installed, you still must activate it by clicking the appropriate checkbox in the Local Area Connection Properties dialog box.


Printers and Faxes

Mike's Laserjet Properties

General | Sharing | Ports | Advanced | Security | Device Settings

You can share this printer with other users on your network. To enable sharing for this printer, click Share this printer. Windows Firewall is already configured to allow the sharing of printers with other computers on the network.

○ Do not share this printer

● Share this printer

Share name: Mike's Laserjet

☑ List in the directory

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Additional Drivers...

OK | Cancel | Apply

• Figure 22.60 Giving a name to a shared printer on Windows XP

Troubleshooting Networks

Once you go beyond a single PC and enter the realm of networked computers, your troubleshooting skills need to take a giant leap up in quality. The secret to finding the right answer to networking problems on the CompTIA A+ exams is to remember that the exams only ask about the skills to get a single computer back on the network. Granted, this might mean you'll need to check a switch or verify another system's connectivity, but in general, always focus your network troubleshooting answers on getting a single system up and running.

The troubleshooting issues discussed here apply only to a LAN, and do not cover issues related to troubleshooting Internet access. We'll cover Internet troubleshooting in Chapter 24, using the knowledge you've gained in this chapter and adding even more tools.

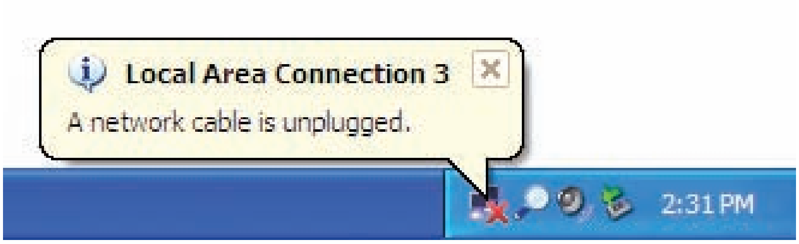
CompTIA likes to ask questions that deal with "no connectivity" or "intermittent connectivity." There are two ways to look at connectivity issues and CompTIA A+ exam objectives don't specify which type is covered on the exams. The first type of connectivity issue (and probably the one CompTIA means) is when your computer loses physical connectivity. The second type is when you're on the network and can't access a particular resource (you can access other resources, just not the one you want right now). Let's consider both.

Repairing Physical Cabling

"The network's down!" is one of the most terrifying phrases a network tech will ever hear. Networks fail for many reasons, and the first thing to know is that good-quality, professionally installed cabling rarely goes bad, but when it does, you need to know what to do. Let's take a moment now to discuss what to do when you think you've got a problem with your physical network.

Symptoms

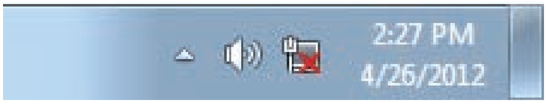
Losing physical connectivity is pretty obvious in Windows. Windows XP gives you a nice pop-up message warning you that you have lost a



Local Area Connection 3

A network cable is unplugged.

• Figure 22.61 Windows XP pop-up message and red X error icon



• Figure 22.62 Windows 7 red X error icon

connection, along with a red X over the network icon (see Figure 22.61). Windows Vista and Windows 7 aren't quite as obvious, displaying only the red X over the network icon in the system tray to show you're not connected (see Figure 22.62).

If you encounter this problem, first check the obvious: Is the cable unplugged at your system? At the wall outlet? Then go for the less obvious: Is the NIC disabled in Device Manager? If these checks don't solve the problem, take a peek on the other side of the cable. If you're not connected to a running switch, you're going to get the disconnect errors.

Intermittent connectivity is often the same issue but typically is harder to figure out. Either way, read the next section to see how to get serious about testing for these pesky connectivity problems.

Diagnosing Physical Problems

Look for errors that point to physical disconnection. A key clue that the computer may have a physical problem is that a user gets a "No server is found" error, or tries to use the operating system's network explorer utility (like Network in Windows 7) and doesn't see any systems besides his or her own.

Multiple systems failing to access the network often points to hardware problems. This is where knowledge of your network cabling helps. If all the systems connected to one switch suddenly no longer see the network, but all the other systems in your network still function, you not only have a probable hardware problem, but also have a suspect—the switch.

Check the Lights

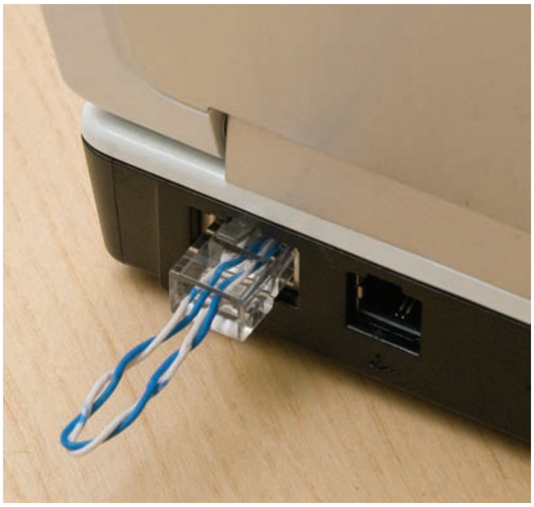
If you suspect a hardware problem, first check the link lights on the NIC and switch. If they're not lit, you know the cable isn't connected somewhere. If you're not physically at the system in question (if you're on a tech call, for example), you can have the user check his or her connection status through the link lights or through software.

If the problem system clearly cannot connect, eliminate the possibility of a failed switch or other larger problem by checking to make sure other people can access the network, and that other systems can access the shared resource (server) that the problem system can't see. Inspect the cable running from the back of the PC to the outlet. Finally, if you can, plug the system into a known good outlet and see if it works. A veteran network tech keeps a long patch cable for just this purpose. If you get connectivity with the second outlet, you should begin to suspect the structured cable running from the first outlet to the switch. Assuming the cable is installed properly and has been working correctly before this event, a simple continuity test will confirm your suspicion in most cases.

Check the NIC

Be warned that a bad NIC can also generate a "can't see the network" problem. Use the utility provided by the OS to verify that the NIC works. If you've got a NIC with diagnostic software, run it—this software will check the NIC's circuitry. The NIC's female connector is a common failure point, so NICs that come with diagnostic software often include a special test called a **loopback test**. A loopback test sends data out of the NIC and checks to see if it comes back. Some NICs perform only an internal loopback, which tests the circuitry that sends and receives, but not the actual connecting pins. A true external loopback requires a **loopback plug** inserted into the NIC's port (see Figure 22.63). If a NIC is bad, replace it.

Onboard NICs on laptops are especially notorious for breaking due to frequent plugging and unplugging. On some laptops, the NICs are easy to replace; others require a motherboard replacement.



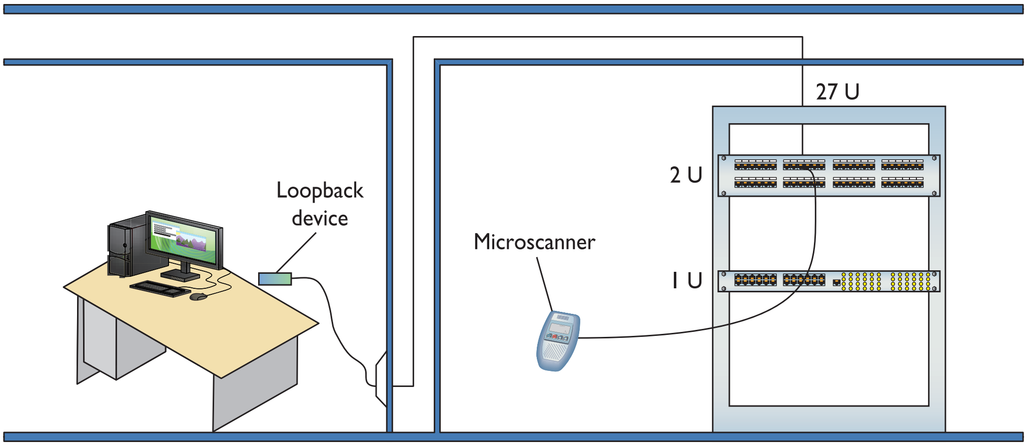
• Figure 22.63 Loopback plug

Cable Testing

The vast majority of network disconnection problems occur at the work area. If you've tested those connections, though, and the work area seems fine, it's time to consider deeper issues.

With the right equipment, diagnosing a bad horizontal cabling run is easy. Anyone with a network should own a midrange time-domain reflectometer (TDR) tester such as the Fluke MicroScanner. A TDR measures impedance in network cabling. If the tester measures any impedance, something is wrong with the cable. With a little practice, you can easily determine not only whether a cable is disconnected but also where the disconnection takes place. Sometimes patience is required, especially if you've failed to label your cable runs, but you will find the problem.

When you're testing a cable run, always include the patch cables as you test. This means unplugging the patch cable from the PC, attaching a tester, and then going to the telecommunications room. Here you'll want to unplug the patch cable from the switch and plug the tester into that patch cable, making a complete test, as shown in Figure 22.64.



• Figure 22.64 Cable tester in action

Testing in this manner gives you a complete test from the switch to the system. In general, a broken cable must be replaced. A bad patch cable is an easy fix, but what happens if the horizontal cable is to blame? In these cases, I get on the phone and call my local installer. If a cable is bad in one spot, the risk of it being bad in another is simply too great to try anything other than total replacement.

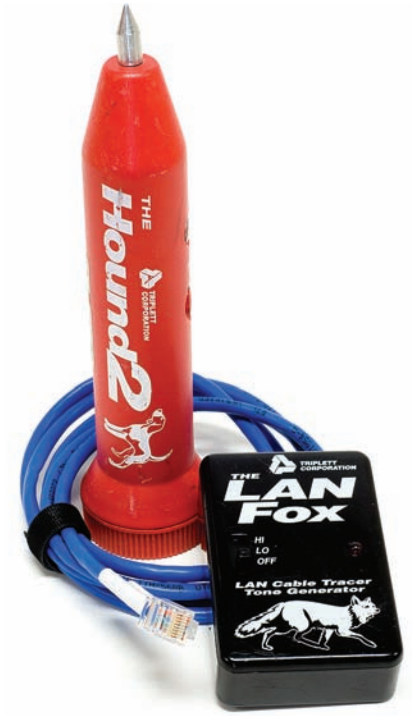
Toners

It would be nice to say that all cable installations are perfect and that over the years they won't tend to grow into horrific piles of spaghetti-like, unlabeled cables. In the real world, though, you might eventually find yourself having to locate or *trace* cables. Even in the best-planned networks, labels fall off ports and outlets, mystery cables appear behind walls, new cable runs are added, and mistakes are made counting rows and columns on patch panels. Sooner or later, most network techs will have to be able to pick out one particular cable or port from a stack.

When the time comes to trace cables, network techs turn to a device called a toner for help. **Toner** is the generic term for two separate devices that are used together: a tone generator and a tone probe. The **tone generator** connects to the cable using alligator clips, tiny hooks, or a network jack, and it sends an electrical signal along the wire at a certain frequency. The **tone probe** emits a sound when it is placed near a cable connected to the tone generator. These two devices are often referred to by the brand-name Fox and Hound, a popular model of toner made by the Triplett Corporation (see Figure 22.65).

You'll see a tone probe referred to on the CompTIA A+ exam as a *toner probe*.

To trace a cable, connect the tone generator to the known end of the cable in question, and then position the tone probe next to the other end of each of the cables that might be the right one. The tone probe makes a sound when it's placed next to the right cable. Some toners have one tone probe that works with multiple tone generators. Each generator emits a separate frequency, and the probe sounds a different tone for each one. Even good toners are relatively inexpensive ($75); although inexpensive toners can cost less than $25, they don't tend to work well, so spending a little more is worthwhile. Just keep in mind that if you have to support a network, you'd do best to own a decent toner.



• Figure 22.65

Fixing Common Problems

Let's go back and look at the second possible meaning for a loss in connectivity. It's very common to try to connect to a shared resource and either fail or find that a shared resource you've used time and again has suddenly disappeared.

Failing to Connect to a New Resource

When you can't connect to a resource on the first try, it often points to a configuration issue. In most cases, a quick double-check of the sharing system will reveal one of the following problems (and call for the associated solution).

- You don't have the right share name? Go check at the serving system.
- You don't have the required user name/password? Ask someone who might have this knowledge, or double-check that your account has access.
- You don't have permission to use/access/connect to the shared resource? Make sure you have the correct permissions.
- You're not on the right homegroup/domain/workgroup? Check your system and the sharing system to verify which workgroup/domain name to use. On a homegroup, make sure you've used the proper password.
- The folder or printer isn't shared? Share it!
- The folder or printer doesn't exist? Make sure the serving system still hosts the folder you want. Install the network printer if you haven't yet.

Failing to Connect to a Previously Used Resource

If you suddenly can't connect to a resource that you've used many times before, go with the easy answers first:

- Verify that you are not already connected by using **nbtstat –s**.
- Check that you can see the resource using My Network Places/Network or **net view**.
- Check that the serving system is on.
- Check that the computer is physically connected to the serving system.

Chapter 22 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about networking.

Install and troubleshoot structured cabling

- Fiber optic Ethernet transmits light instead of electricity, achieving much greater maximum distances than other forms of Ethernet. Most fiber networks use LEDs to send light signals and use multimode fiber optic cabling. Networks that use laser light use single-mode fiber optic cabling. Laser light and single-mode cabling are used most often for very long-distance connections.
- Most fiber optic cables use one of two connectors: the square SC type or the round ST type.
- Early versions of Ethernet ran on coaxial cable instead of UTP. Coax cable consists of a center cable, or core, surrounded by insulation, covered by a shield of braided cable. Coaxial cables are rated using an RG name, with the two most popular standards being RG-6 and RG-59.
- The two common coaxial cable connectors are the BNC twist connector and the F-type screw connector.
- Hubs connected older Ethernet networks. They repeat data to every connected port.
- Switches have replaced hubs as the modern interconnection point for Ethernet networks. They create point-to-point connections between two computers.
- A bridge enables two devices with different connector types, such as UTP and fiber optic, to connect and communicate with one another.
- A network attached storage (NAS) device is a simple box that supports one or more hard drives for sharing data across a network. These are often self-configuring. A NAS is a type of network appliance.
- A router connects multiple LANs together. By definition, a router must have at least two connections: one into the network, and one out to another network.
- Structured cabling refers to a set of standards for installing wired networks, including the type of cables to be used, where to place them, how to connect them, and so on. The idea is to create a safe and reliable cabling infrastructure. Structured cabling requires three ingredients: a telecommunications room, horizontal cabling, and a work area.
- All UTP cables use either solid core or stranded core. Each wire in solid core UTP uses a single solid wire. With stranded core, each wire is actually a bundle of tiny wire strands. Each of these cable types has its benefits and downsides.
- A patch panel is a box with a row of female connectors (or ports) in the front and permanent connections in the back, where you connect your horizontal cables. Most patch panels use a 110 block.

Explain the basics of TCP/IP

- TCP/IP is the primary protocol of most modern networks, including the Internet. For a PC to access the Internet, it must have TCP/IP loaded and configured properly.
- Any network address must provide two pieces of information: it must uniquely identify the machine and it must locate that machine within the larger network. In a TCP/IP network, the IP address identifies the PC and the network on which it resides.
- Part of every IP address identifies the network (the network ID), and another part identifies the local computer (the host ID, or host) on the network. The subnet mask is a value that a NIC uses to distinguish which part of the IP address identifies the network ID and which part of the address identifies the host.
- IP addresses are divided into class licenses that correspond with the potential size of the network: Class A, Class B, and Class C. Class A licenses were intended for huge companies and organizations, such as major multinational corporations, universities, and governmental agencies. Class B licenses were assigned to medium-size companies, and Class C licenses were designated for smaller LANs.

- When you want to be positive that the data moving between two systems gets there in good order, use a connection-oriented application. If it's not a big deal for data to miss a bit or two, then connectionless is the way to go. The connection-oriented protocol used with TCP/IP is called the Transmission Control Protocol (TCP). The connectionless one is called the User Datagram Protocol (UDP).
- TCP/IP provides sharing functions called services. Well-known TCP/IP services include HTTP, the language of the World Wide Web, Telnet, and ping.
- TCP/IP requires that several settings are properly configured before you can connect to a network. A network administrator should configure these for you. These settings include your IP address, default gateway, DNS settings, and DHCP settings.
- Windows includes several tools for testing and managing TCP/IP, including ping, ipconfig, nslookup, and tracert.
- By default, TCP/IP is configured to receive an IP address automatically from a DHCP server on the network (and automatically assign a corresponding subnet mask).
- Windows supports a feature called Automatic Private IP Addressing (APIPA) that automatically assigns an IP address to the system when the client cannot obtain an IP address automatically.
- IPv6 extends the 32-bit IP address space to 128 bits, allowing up to 2^{128} (that's close to 3.4×10^{38}) addresses. The familiar 32-bit IPv4 addresses are written as 197.169.94.82, using four octets. The 128-bit IPv6 addresses are written like this: 2001:0000:0000:3210:0800:200C:00CF:1234. A complete IPv6 address always has eight groups of four hexadecimal characters.
- You may have up to three IPv6 addresses on your PC at one time: a link-local address and two global addresses.

Install and configure wired networks

- When you install a NIC, by default, Windows installs upon setup the TCP/IP protocol (configured for DHCP), the Client for Microsoft Networks, and File and Printer Sharing for Microsoft Networks.
- To establish network connectivity, you need a network client installed and configured properly. The Client for Microsoft Networks is installed as part of the OS installation.
- All versions of Windows share drives and folders in basically the same manner. Right-click any drive or folder, choose Properties, and then select the Sharing tab. In Windows Vista/7 click the Advanced Sharing button. Click the *Share this folder* radio button and type a share name.
- When sharing a folder on an NTFS drive, you must set the network permissions to give everyone full control, and then use the NTFS permissions (on the Security tab) to exercise more precise control over who accesses the shared resources and how they access them.
- Network resources can be mapped to a local resource name. This can be done from Windows Explorer or by right-clicking a share in My Network Places/Network and choosing Map Network Drive.
- All computers that share must have a share name, and all the resources they share must also have names. Any resource on a network can be described by combining the name of the resource being shared and the name of the system sharing it. The complete UNC name of the FREDC share on SERVER1, for example, would be \\SERVER1 \FREDC.
- The nbtstat command shows you information about your network, including the workgroups or domains on the network.
- Windows provides the net utility to help you explore and diagnose a Windows network. One of the more popular options is net view, which lists other Windows systems on the network. Another popular option is the net use command to map a remote share as a network drive.
- To share a printer in Windows, open the Printers folder in the Control Panel or Start menu and right-click the printer you wish to share. Select Sharing, and then click *Share this printer* and give it a name.

Troubleshoot wired networks

- Look for errors that point to physical disconnection. A key clue that you may have a physical problem is that a user gets a "No server is found" error, or tries to use the operating system's network explorer utility (like Network in Windows 7) and doesn't see any systems besides his or her own.

- If you suspect a hardware problem, first check the link lights on the NIC and switch. If they're not lit, you know the cable isn't connected somewhere. If you're not physically at the system in question (if you're on a tech call, for example), you can have the user check his or her connection status through the link lights or through software.
- Be warned that a bad NIC can also generate a "can't see the network" problem. Use the utility provided by your OS to verify that the NIC works. If you've got a NIC with diagnostic software, run it—this software will check the NIC's circuitry.
- A loopback test sends data out of the NIC and checks to see if it comes back. Some NICs perform only an internal loopback, which tests the circuitry that sends and receives, but not the actual connecting pins. A true external loopback requires a loopback plug inserted into the NIC's port.
- A TDR measures impedance in network cabling. If the tester measures any impedance, something is wrong with the cable.
- When you're testing a cable run, always include the patch cables as you test. This means unplugging the patch cable from the PC, attaching a tester, and then going to the telecommunications room.
- When the time comes to trace cables, network techs turn to a device called a toner for help. The tone generator connects to the cable using alligator clips, tiny hooks, or a network jack, and it sends an electrical signal along the wire at a certain frequency. The tone probe emits a sound when it is placed near a cable connected to the tone generator. These two devices are often referred to by the brand-name Fox and Hound, a popular model of toner.

Key Terms

110 block *(831)*
activity light *(851)*
Automatic Private IP Addressing (APIPA) *(838)*
bridge *(826)*
coaxial cable *(824)*
crossover cable *(823)*
Dynamic Host Configuration Protocol (DHCP) *(841)*
equipment rack *(830)*
fiber optic cable *(823)*
full-duplex *(850)*
horizontal cabling *(828)*
Internet Protocol version 4 (IPv4) *(846)*
Internet Protocol version 6 (IPv6) *(846)*
IP address *(836)*
ipconfig *(842)*
link lights *(851)*
loopback plug *(861)*
loopback test *(861)*
net command *(857)*
nslookup *(842)*
patch cable *(832)*
patch panel *(831)*
ping *(840)*
punchdown tool *(831)*
resources *(853)*
run *(828)*
solid core *(829)*
static IP address *(841)*
stranded core *(829)*
structured cabling *(827)*
subnet mask *(836)*
switch *(825)*
TCP/IP services *(840)*
telecommunications room *(828)*
tone generator *(862)*
tone probe *(862)*
toner *(862)*
tracert *(843)*
Transmission Control Protocol/Internet Protocol (TCP/IP) *(835)*
U *(830)*
universal naming convention (UNC) *(856)*
work area *(828)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. HTTP and Telnet are both examples of special sharing functions called ______________.
2. The command-line utility called ______________ enables one machine to check whether it can communicate with another machine.
3. A center cable surrounded by insulation and covered with a shield of braided cable is called ______________.
4. A computer on a(n) ______________ network gets a 32-bit address.
5. A computer on a(n) ______________ network gets a 128-bit address.
6. The set of standards established by the TIA/EIA regarding network cabling is called ______________.
7. ______________ uses light, instead of electricity, to transmit data.
8. You can use a(n) ______________ to connect two different types of network media, such as coaxial and UTP.
9. When troubleshooting a NIC, you'll need to crawl behind your computer and look for the ______________, which should be on or blinking.
10. To test a possibly broken Ethernet port, plug in a(n) ______________.

Multiple-Choice Quiz

1. Everything worked fine on your 1000BaseT network yesterday, but today no one can connect to the server. The server seems to be in good running order. Which of the following is the most likely problem?
   - **A.** Someone changed all of the passwords for server access.
   - **B.** A switch is malfunctioning.
   - **C.** Someone's T connector has come loose on the bus.
   - **D.** The server's cable is wired as TIA/EIA 568A and all of the others are wired as TIA/EIA 568B.
2. Simon's system can't contact a DHCP server to obtain an IP address automatically, but he can still communicate with other systems on his subnet. What feature of Windows makes this possible?
   - **A.** Subnet masking
   - **B.** Default gateway
   - **C.** APIPA
   - **D.** Client for Microsoft Networks
3. Which of the following is the correct net syntax for discovering which network shares on a particular server are mapped on your computer?
   - **A.** net view \\fileserver
   - **B.** net \\fileserver
   - **C.** net map \\fileserver
   - **D.** net share \\fileserver
4. A small device that enables you to test a NIC's circuitry is called?
   - **A.** Loopback plug
   - **B.** Port tester
   - **C.** Multimeter
   - **D.** Integrated network and logic probe
5. What is the term used to describe where the network hardware and patch panels are kept?
   - **A.** Drop room
   - **B.** Telecommunications room
   - **C.** Routing room
   - **D.** Telecloset room

6. You are down under your desk organizing some wires when you notice that the activity light on your NIC is blinking erratically. Is there a problem?

   A. Yes, the activity light should be on steadily when the computer is running.

   B. Yes, the activity light should be blinking steadily, not randomly.

   C. No, the light blinks when there is network traffic.

   D. No, the light blinks to show bus activity.

7. What is a common symptom of a bad network cable?

   A. Rapidly blinking link lights

   B. No link lights

   C. Solid on link lights

   D. Steady blinking link lights

8. What command-line utility would you run to show a list of network computers?

   A. net send

   B. show net_servers

   C. net use

   D. net view

9. When connecting a cable run onto a patch panel, which tool should you use?

   A. 110-punchdown tool

   B. Crimper

   C. TDR

   D. Tone generator

10. What is the structured cabling name for the end user's office space where network computers are set up?

   A. Backbone

   B. Building entrance

   C. Cable drop

   D. Work area

11. You are trying to locate which patch cable in the main switch traces back to a particular computer. Which tool should you use?

   A. Tone probe

   B. Cable tester

   C. Punchdown tool

   D. Butt set

12. Which of the following describes an IPv4 address? (Select three.)

   A. Uses decimal, not hexadecimal numbers

   B. Uses periods, not colons, as separators

   C. Uses four octets

   D. Uses eight sets of characters

13. Which of the following are fiber connector types? (Select three.)

   A. LC

   B. LS

   C. MT-RJ

   D. ST

14. What benefit does full-duplex offer?

   A. It enables NICs to send and receive signals at the same time.

   B. It enables NICs to send data twice as fast.

   C. It enables NICs to receive data twice as fast.

   D. It enables a switch to connect to both coaxial and fiber optic cables.

15. What do most techs call a toner or tone generator?

   A. TDR

   B. UTP

   C. UDP

   D. Fox and Hound

Essay Quiz

1. You are a tech for a small company and you get a call from Jessica, who cannot access the network anymore from her workstation. What techniques would you use to help troubleshoot her system and get her back working?
2. There are different classifications of IP addresses and different ways to assign them. Write a short essay on the difference between Class A, B, and C addresses, and how to choose either static or dynamic addressing.
3. Which types of computer network cable connections are you familiar with already? Write a short paragraph describing your experience.
4. Prepare a list of questions you would ask a large organization's network administrator regarding cabling, connections, hubs, switches, and even routers.

Lab Projects

• Lab Project 22.1

This chapter described how Windows automatically generates an IP address if there is no DHCP server. Experiment with this idea. If you have a network of Windows PCs that you can play with, make sure there is no DHCP server on the network. Use ipconfig and see what your IP address is, and try sharing it and pinging other systems. Try to share resources and access shared resources on other machines in the lab.

• Lab Project 22.2

The PC is not the only device that can connect to an Ethernet network. Do an Internet search or make a run to your local computer store and create a list of network devices. What did you find? How would they be used?

• Lab Project 22.3

Nearly every hardware manufacturer wants you to upgrade to their latest networking gear and they keep adding new features to entice you. Do a search through the bigger companies' product lists and compare the Linksys, Netgear, Microsoft, and D-Link devices:

www.linksys.com

www.netgear.com

www.microsoft.com

www.dlink.com

• Lab Project 22.4

The Internet is a big, sprawling place with big routers that move packets from place to place around the world. Using the tracert command, see how many hops it takes to get to various Web sites around the world.