

# Remote Connectivity

The Network+ Certification exam expects you to know how to

- 1.6 Identify the purpose, features, and functions of the following network components: CSU/DSU (Channel Service Unit/Data Service Unit), NICs, ISDN adapters, modems
- 2.14 Identify the basic characteristics (for example, speed, capacity, media) of the following WAN technologies: packet switching, circuit switching, ISDN, FDDI, T1/E1/J1, T3/E3/J3, OCx (Optical Carrier), X.25
- 2.15 Identify the basic characteristics of the following Internet access technologies: xDSL (Digital Subscriber Line), broadband cable (cable modem), POTS/PSTN (Plain Old Telephone Service/Public Switched Telephone Network), satellite
- 2.16 Define the function of the following remote access protocols and services: RAS (Remote Access Service), PPP (Point-to-Point Protocol), SLIP (Serial Line Internet Protocol), PPPoE (Point-to-Point Protocol over Ethernet), PPTP (Point-to-Point Tunneling Protocol), VPN (Virtual Private Network)
- 2.17 Identify the following security protocols and describe their purpose and function: L2TP
- 2.18 Identify authentication protocols (for example: CHAP—Challenge Handshake Authentication Protocol, MS-CHAP—Microsoft Challenge Handshake Authentication Protocol, PAP—Password Authentication Protocol, RADIUS—Remote Authentication Dial-In User Service, Kerberos, and EAP—Extensible Authentication Protocol)
- 3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks)
- 3.9 Identify the main characteristics and purpose of extranets and intranets
- 4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (for example: file services, print services, authentication failure, protocol configuration, physical connectivity, and SOHO—Small Office/Home Office—router)

To achieve these goals, you must be able to

- Describe the different types of SOHO connections such as dial-up, ADSL, and cable modems
- Describe the different types of higher-capacity connections such as T1/T3, OC-1/OC-3, Frame Relay, and ATM, commonly used for WAN connectivity
- Explain how to set up and use clients and servers for remote access
- Troubleshoot basic remote access problems

Long before the Internet came into popular use, network users and developers desired to take a single system or group of systems and connect them to another network. Connecting individual computers and LANs into other individual computers and LANs gives us the ability to share more resources and to communicate more readily among more computers. Making these interconnections is a challenge, requiring specialized long-distance media, hardware that can convert data from one format to another, unique security functions, and software that understands how to make interconnected systems work together. This chapter begins by inspecting the many remote connection media options, from good old telephone lines to advanced fiber-optic carriers, and even satellites. There are so many ways to make remote connections that this section is broken into two parts. The first part, “SOHO LAN Connections,” deals with the types of remote connections more commonly seen in small offices and the home. This includes dial-up, DSL, and cable modems. The next section, “WAN Connections,” goes into the big pipes—the high-capacity, dedicated connections more commonly seen in the corporate environment.

Once you’ve seen the transmission options, the chapter goes into the types of remote connection you can make. It’s easy to think everything connects to the Internet, but there are a number of situations that have nothing to do with the Internet. What if a person wants to connect his or her laptop to the home office’s network in Texas from a café in Paris? (And who wouldn’t?) At the end of that section, we’ll look at some of the more common problems that take place with remote connectivity and learn how to deal with these problems.

## Test Specific

### SOHO LAN Connections

For many years the only viable connection available to small office and home office (SOHO) users was your telephone via the classic dial-up connection. Dial-up is still the most popular way to get a single computer connected to another network, but today you have a number of excellent options that provide high-speed connectivity at low prices. All of these methods enable you to connect a local area network (LAN) to the Internet through a single PC. Let’s look at these options, starting with the oldest and most well-known, your telephone line.

#### Telephone Options

There are many different types of telephone lines available, but all the choices break down into two groups: dedicated and dial-up. *Dedicated telephone lines* are always off the hook (that is, they never hang up on each other). A true dedicated line does not have a phone number. In essence, the telephone company creates a permanent, hard-wired connection between the two locations, rendering a phone number superfluous. *Dial-up lines*, by contrast, have phone numbers; they must dial each other up to make a connection. When they’re finished communicating, they hang up. Telephone companies hate it, but many

locations use dial-up lines in a dedicated manner. If a dial-up connection is made and the two ends never disconnect, you have basically the same function as a dedicated line. But it is still a dial-up connection, even if the two sides rarely disconnect. Two technologies make up the overwhelming majority of dial-up connections—PSTN and ISDN.

## Public Switched Telephone Network

The oldest, slowest, and most common phone connection is the *Public Switched Telephone Network (PSTN)*. PSTN is also known as *Plain Old Telephone Service* (seriously!—you see it all the time with the acronym *POTS*). PSTN is just a regular phone line, the same line that runs into everybody's home telephone jacks from the central office of your local exchange carrier (LEC—the telephone company that provides local connections).

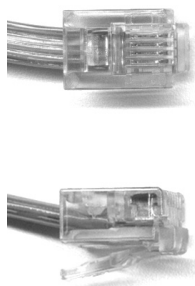
Because PSTN was designed long before computers were common, it was designed to work with only one type of data: sound. Here's how it works. The telephone's microphone takes the sound of your voice and translates it into an electrical analog waveform. The telephone then sends that signal through the PSTN line to the phone on the other end of the connection. That phone translates the signal into sound on the other end using its speaker. The important word here is *analog*. The telephone microphone converts the sounds into electrical waveforms that cycle 2400 times a second. An individual cycle is known as a *baud*. The number of bauds per second is called the *baud rate*. Pretty much all phone companies' PSTN lines have a baud rate of 2400. PSTN uses a connector called RJ-11. It's the classic connector you see on all telephones (see Figure 16-1).

When you connect your modem to a phone jack, the line then runs to a special box known as the *network interface (NI)* or *demarc* (short for demarcation point). The term "network interface" is more commonly used to describe the small box on the side of your home that accepts the incoming lines from the telephone company, and then splits them to the different wall outlets. *Demarc* is more commonly used to describe large connections used in businesses. The terms are interchangeable and always describe the interface between the lines the telephone company is responsible for and the lines for which you are responsible.

Computers, as you know, don't speak analog—only digital (ones and zeros) will do. In addition, the digital signal goes in and out of your computer in eight bits at a time. To connect over phone lines, they need a device that converts the 8-bit wide digital signals from the computer into serial (1-bit wide) digital data, and then convert (modulate) the data into analog waveforms that can travel across PSTN lines. This same device must de-

**Figure 16-1**

RJ-11 connectors  
(top and side  
views)



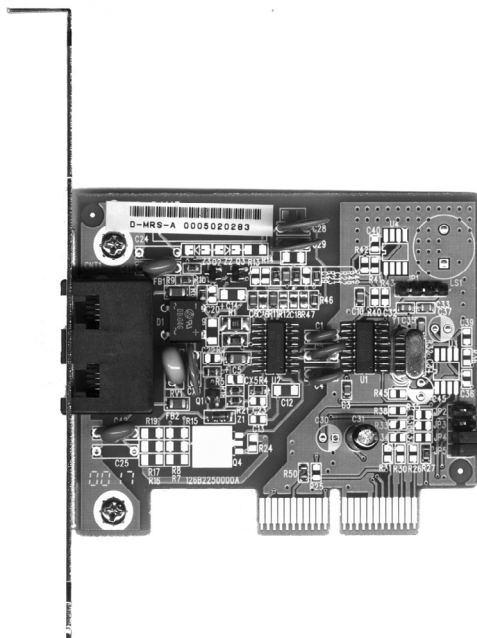
modulate the analog signals from the PSTN wall jack into 8-bit wide sets of ones and zeros the computer can understand. The device that converts the analog data to digital and back is called a *MOdulator DEModulator (modem)*. There are two types of modems seen in the PC world: internal and external. Internal modems are two devices: a UART (Universal Asynchronous Receiver/Transmitter) and a modem. The UART takes the 8-bit wide digital data and converts it into bit-wide digital data and hands it to the modem for conversion to analog data. The process is reversed for incoming data. External modems do not have a UART and instead connect to a serial port or a USB port. These ports have built-in UART functions (see Figure 16-2).

### Baud vs. Bits per Second

Modems utilize phone lines to transmit data, not just voice, at various speeds. These speeds cause a world of confusion and problems for computer people. This is where a little bit of knowledge becomes dangerous. Standard modems you can buy for your home computer normally transmit data at speeds up to 56 Kbps. That's 56 kilobits per second, *not* 56 kilo-baud! Many people confuse the terms *baud* and *bits per second*. This confusion arises because the baud rate and bps are the same for modems until the data transfer rate surpasses 2400 baud.

A PSTN phone line takes analog samples of sound 2400 times a second. This standard was determined a long time ago as an acceptable rate for sending voice traffic over phone lines. Although 2400-baud analog signals are in fact fine for voice communication, they are a big problem for computers trying to send data as computers only work

**Figure 16-2**  
Typical internal  
modem



with digital signals. The job of the modem is to take the digital signals it receives from the computer and send them out over the phone line in an analog form, using the baud cycles from the phone system. The earliest modems—often erroneously called 300-baud modems—used four analog bauds just to send one bit of data. As you should already have realized, they weren't 300-baud modems at all—they were 300 *bps* modems; however, the name baud kind of stuck for describing modem speeds.

As technology progressed, modems became faster and faster. To get past the 2,400 baud limit, modems would modulate the 2,400 baud signal twice in each cycle, thereby transmitting 4,800 bits per second. To get 9,600 bps, the modem would modulate the signal four times per cycle. All PSTN modem speeds are always a multiple of 2,400. Look at the following classic modem speeds:

- $2,400 \text{ baud/sec} \times 1 \text{ bit/baud} = 2,400 \text{ bps}$
- $2,400 \times 2 = 4,800 \text{ bps}$
- $2,400 \times 4 = 9,600 \text{ bps}$
- $2,400 \times 6 = 14,400 \text{ bps}$
- $2,400 \times 8 = 19,200 \text{ bps}$
- $2,400 \times 12 = 28,800 \text{ bps}$
- $2,400 \times 24 = 57,600 \text{ bps (56 Kbps)}$

So, if someone comes up to you and asks, "Is that a 56K baud modem?" you can look them straight in the eye and say, "No, it's a 2,400-baud modem. But its bits per second rate is 57,600!" You'll be technically correct, but soon you will have no friends.

## V Standards

For two modems to communicate with each other at their fastest rate, they must modulate signals in the same fashion. The two modems must also negotiate with, or *query*, each other to determine the fastest speed they share. The modem manufacturers themselves originally standardized these processes as a set of proprietary protocols. The downside to these protocols was that unless you had two modems from the same manufacturer, modems often would not work together. In response, a European standards body called the CCITT established standards for modems. These standards, known generically as the V standards, define the speeds at which modems can modulate. The most common of these speed standards are as follows:

- |                      |                   |
|----------------------|-------------------|
| • V.22 1,200 bps     | • V.34 28,000 bps |
| • V.22bis 2,400 bps  | • V.90 57,600 bps |
| • V.32 9,600 bps     | • V.92 57,600 bps |
| • V.32bis 14,400 bps |                   |

The current modem standard now on the market is the *V.92 standard*. V.92 has the same download speed as the V.90, but upstream rates increase to as much as 48 Kbps. If your modem is having trouble getting 56 Kbps rates with V.90 in your area, you will not notice an improvement. V.92 also offers a Quick Connect feature, which implements faster handshaking to cut connection delays. Finally, the V.92 standard offers a Modem On Hold feature, which enables the modem to stay connected while you take an incoming call-waiting call or even initiate an outgoing voice call. This feature only works if the V.92 server modem is configured to enable it.



**TIP** Know your V standards!

In addition to speed standards, the CCITT, now known simply as ITU, has established standards controlling how modems compress data and perform error checking when they communicate. These standards are as follows:

- V.42 Error Checking
- V.42bis Data Compression
- V.44 Data Compression
- MNP5 Both error checking and data compression

The beauty of these standards is that you don't need to do anything special to enjoy their benefits. If you want 56 Kbps data transfers, for example, you simply need to ensure that the modems in the local system and the remote system both support the V.90 standard. Assuming you have good line quality, the connections will run at or at least close to 56 Kbps.

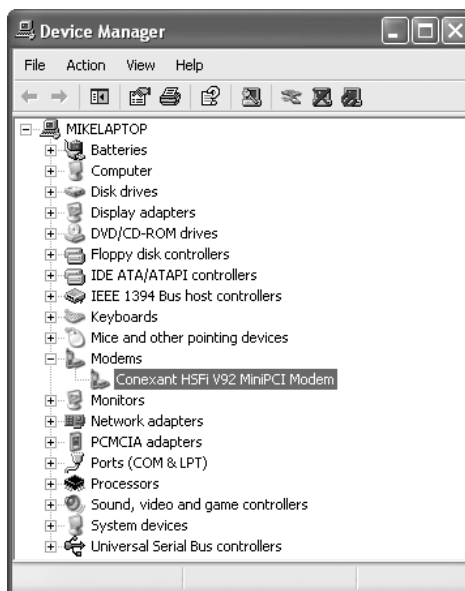


**TIP** Some people get confused by the concept of port speed vs. modem speed. All versions of Windows give you the opportunity to set the port speed. *Port speed* is the speed at which the data travels between the serial port (really the UART) and the modem, not between the local and remote modems (that's the modem speed). As a rule, always set the port speed to the highest setting available (this should be 115,200 bps, assuming your UART is a 16500 or better).

## Installing a PSTN Connection

Installing a PSTN connection in a Windows computer is a two-step process. First you install a modem, and then you create a connection. Installing a modem in a Windows system is virtually automatic. Modem technologies haven't changed much in the last few years, so any Windows 98 SE client or later almost certainly has a driver you need built into the operating system. Even though Windows probably has a functional driver, you should still use the driver supplied with the modem to take advantage of extra features such as faxing or answering machine functions. Like any newly installed device, a quick trip to Device Manager to confirm that Windows sees the device is always a good idea (Figure 16-3).

**Figure 16-3**  
Properly working  
modem in Device  
Manager



Once a modem has been installed you can then begin to create connections (and the upcoming “Using Remote Access” section shows you how to make these connections). But before a connection can be made, we have one more issue to deal with. How does one modem know where one packet ends and another begins? Sure, the V standards will get the data from one modem to another, but how do the modems know how to send an IP packet on a serial line in such a way that it makes it intact to the other side? The answer to this issue lies in two Data-Link layer protocols for dial-up connections called SLIP and PPP.

## SLIP

*Serial Line Internet Protocol (SLIP)* was the network community’s first effort to make a Data Link protocol for telephony, and it shows. About the only thing good you can say about SLIP is that it worked—barely. SLIP had a number of major limitations. First, it only supported TCP/IP. If you had a NetBEUI or IPX network, you were out of luck. Second, SLIP could not use DHCP, so any system that used SLIP required a static IP address. This wasn’t too much of an issue in the early days of the Internet, but as the Internet became more popular, no Internet provider wanted an IP address tied up when you weren’t online. As if this were not enough, SLIP provided no error checking and instead relied on the hardware making the connection to do any error correction. SLIP also did not natively support compression, which meant that there was no way to streamline your network protocol. There were later versions, such as CSLIP (or Compressed SLIP), which supported a little bit of compression, but it did not fit the bill. Perhaps worst of all (at least from a security standpoint), SLIP transmitted all authentication passwords as clear text. That’s right; there was no encryption on the password. To make matters even more interesting, you usually had to create a script to log on to a server using SLIP. So aside from no security, no support for protocols other than TCP/IP, no compression, no compatibility with DHCP, and a pain-in-the-rear login system, SLIP was not such a bad protocol.



SLIP continues to be supported by most remote access programs, primarily as a backward-compatibility option. But time and technology have moved away from SLIP and into the brighter, better days of PPP.

## PPP

SLIP's many shortcomings motivated the creation of an improved Data Link protocol called *Point-to-Point Protocol (PPP)*. PPP addressed all of the shortcomings of SLIP, and has totally replaced SLIP in all but the oldest connections. Although PPP has many powerful features, two stand out. PPP supports IPX and NetBEUI as well as IP, and it supports dynamic IP addresses. All remote access software comes with the PPP protocol, so PPP is the one to use!

How do you choose your dial-up protocol? Windows uses a handy tool called Dial-up Networking that enables you to create connections for your modem to dial. Go to the Modems Control Panel applet in Windows 9x or the Network Connections in Windows XP. (Note that Windows 2000 calls the section the Network and Dial-up Connections.) A single modem might have multiple connections (my laptop has about ten that I use in different towns) so each connection manifests itself as a separate icon. It's here where you set up the number to dial, the dial-up protocol, any special dialing properties, account numbers, and passwords. You'll see dial-up networking in detail in the "Remote Access Options" section later in this chapter.

## ISDN

There are many pieces to a PSTN telephone connection. First, there's the phone line that runs from your phone out to a network interface box (the little box on the side of your house), and into a central switch. The *central switch* is the device that interconnects multiple individual local connections into the larger telephone network. A central switch will connect to long-distance carriers via high-capacity *trunk lines* and will also connect to other nearby central switches. Central switches are usually rather large and require their own building, called, obviously enough, a central office (CO). Metropolitan areas have a large number of central offices. Houston, Texas, for example, has nearly 100 offices in the general metro area. Before 1970, the entire phone system was analog, but phone companies upgraded their trunk lines to digital systems during the late 1970s and 1980s. Nowadays, the entire telephone system, with the exception of the line from your phone to the central office, is digital.

During this upgrade period, customers continued to demand higher throughput from their phone lines. The old PSTN was not expected to produce more than 28.8 Kbps (56K modems, which were a *big* surprise to the phone companies, didn't appear until 1995). Needless to say, the phone companies were motivated to come up with a way to generate higher capacities. Their answer was fairly straightforward: make the entire phone system digital. By adding special equipment at the central office and the user's location, phone companies can achieve a throughput of up to 64 Kbps per line (see the following) over the same copper wires already used by PSTN lines. This process of sending telephone transmission across fully digital lines end-to-end is called *Integrated Services Digital Network (ISDN)* service.





**NOTE** ISDN also supports voice, but requires special ISDN telephones.

ISDN service consists of two types of channels: Bearer or B channels and Delta or D channels. *B channels* carry data and voice information at 64 Kbps, while *D channels* carry setup and configuration information, as well as data, at 16 Kbps. Most providers of ISDN let the user choose either one or two B channels. The more common setup is two B/one D, usually called a *Basic Rate Interface (BRI)* setup. A BRI setup uses only one physical line, but each B channel sends 64 Kbps, doubling the throughput total to 128 Kbps. Far less common but still available in some areas is ISDN PRI. ISDN PRI only provides a single B channel for a total throughput of 64 Kbps. ISDN connects much faster than PSTN, eliminating that long, annoying, modem mating call you get with PSTN. The monthly cost per B channel is slightly more than a PSTN line, and there is usually a fairly steep initial cost for the installation and equipment. The other limitation is that not everyone can get ISDN. You usually need to be within about 18,000 feet of a central office to use ISDN.



**NOTE** ISDN uses only PPP, not SLIP!

The physical connections for ISDN bear some similarity to PSTN modems. An ISDN wall socket is usually something that looks like a standard RJ-45 network jack. This line runs to your demarc. In home installations most telephone companies will install a second demarc separate from your PSTN demarc. The most common interface for your computer is a device called a *terminal adapter (TA)*. TAs look like regular modems, and like modems, come in external and internal variants. You can even get TAs that also function as hubs, enabling your system to support a direct LAN connection (see Figure 16-4).



**TIP** A single channel is often referred to as a DS0 channel.

When you install an ISDN TA, you must configure the other ISDN telephone number you want to call and a special number called the Service Profile ID (SPID). Your Internet service provider (ISP) provides the telephone number and the telephone company gives you the SPID. (In many cases the telephone company is also the ISP.) Figure 16-5 shows a typical installation screen for an internal ISDN TA. Note that each channel has a phone number in this case. Once installed an external ISDN TA looks like another modem in Device Manager.

**Figure 16-4**

An ISDN terminal adapter with hub



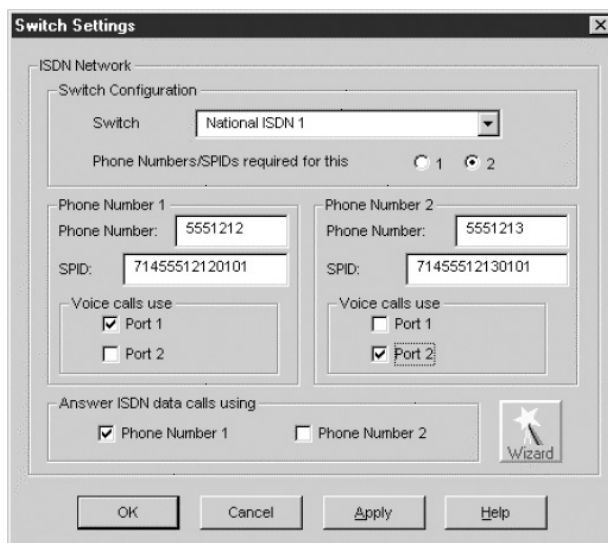
ISDN continues to soldier on in today's networking world, but has for the most part been replaced by faster and cheaper methods such as DSL and cable modems. Nevertheless, every major telephone company still provides ISDN. ISDN is often the only option for users in locations where other high-speed connection options don't exist.

## DSL

*Digital Subscriber Line (DSL)* is a fully digital, dedicated (no phone number) connection provided by a number of telephone companies. DSL represented the next great leap forward past ISDN for telephone lines. A DSL connection manifests as just another PSTN connection, using the same RJ11 jack as any regular phone line. DSL comes in two versions, *Symmetric DSL (SDSL)* and *Asymmetric DSL (ADSL)*. SDSL lines provide the same upload and download speeds, making them excellent for those who send as much data as they receive, although SDSL is relatively expensive. ADSL uses different upload and

**Figure 16-5**

ISDN TA configuration screen



download speeds. ADSL download speeds are much faster than the upload speeds. Most SOHO users are primarily concerned with fast *downloads* for things like web pages, and can tolerate slower upload speeds. ADSL is always much cheaper than SDSL.



**NOTE** These speeds are just for Houston, Texas! Your local providers may offer different speed options.

## SDSL

SDSL provides equal upload and download speed and in theory provides speeds up to 9 Mbps, although the vast majority of ISPs provide packages ranging from 192 Kbps to 1.5 Mbps. A recent tour of some major DSL providers in the author's home town, Houston, Texas, revealed the following SDSL speed options:

- 192 Kbps
- 384 Kbps
- 768 Kbps
- 1.1 Mbps
- 1.5 Mbps

As you might imagine, the pricing for the faster services was higher than the lower packages!

## ADSL

ADSL provides a theoretical maximum download speeds up to 9 Mbps and upload speeds up to 1 Mbps over PSTN lines. However, all ADSL suppliers "throttle" their ADSL speeds and provide different levels of service. Real-world ADSL download speeds vary from 384 Kbps to 3 Mbps and upload speeds go from as low as 64 Kbps to around 384 Kbps. Touring the same DSL providers in Houston, Texas, I found the following speed options:

- 384 Kbps Down/128 Kbps Up
- 1.5 Mbps Down/128 Kbps Up
- 1.5 Mbps Down/384 Kbps Up

## DSL Features

The only real difference between ADSL and SDSL is speed. Everything else—equipment and distance limits—is the same.

One nice aspect of DSL is that you don't have to run new phone lines. The same DSL line you use for data can simultaneously transmit your voice calls. The only downside to DSL is that you can't use it unless your ISP specifically supports DSL. Many ISPs currently support DSL, so most customers have a wide array of choices.

Both versions of DSL have the same central office-to-end-user distance restrictions as ISDN—around 18,000 feet from your demarc to the central office. At the central office your DSL provider has a device called a DSL Access Multiplexer (DSLAM) that connects multiple customers to the Internet.



**NOTE** No DSL provider guarantees any particular transmission speed and will only provide service as a “best efforts” contract—a nice way to say that DSL lines are notorious for substantial variations in throughput. This is true, even of ISPs that lease the lines from the same telephone service.

## Installing DSL

DSL operates using your pre-existing telephone lines (assuming they are up to spec). This is wonderful, but also presents a technical challenge. For DSL and your run-of-the-mill POTS line to coexist, you need to filter out the DSL signal on the POTS line. A DSL line has three information channels: a high-speed downstream channel, a medium-speed duplex channel, and a POTS channel. Segregating the two DSL channels from the POTS channel guarantees that your POTS line will continue to operate even if the DSL fails. This is accomplished by inserting a filter on each POTS line, or a splitter mechanism that allows all three channels to flow to the DSL modem, but sends only the POTS channel down the POTS line. The DSL company should provide you with a few POTS filters for your telephones. If you need more, most computer/electronics stores stock DSL POTS filters.

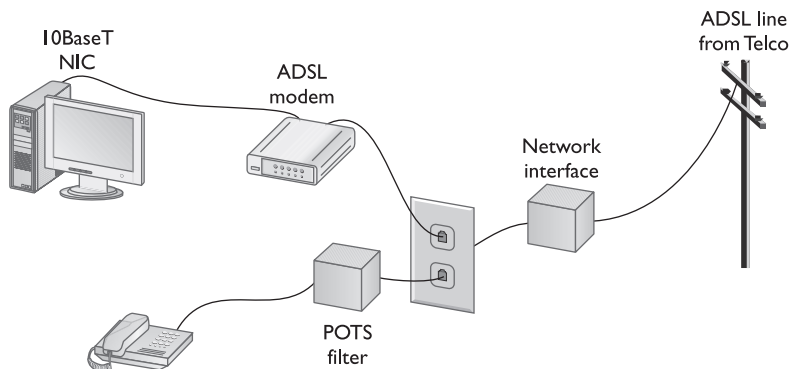


**TIP** If you install a telephone onto a line in your home with DSL and you forget to add a filter, don't panic. You won't destroy anything, although you won't get a dial tone either! Just insert a DSL POTS filter and the telephone will work.

The most common DSL installation consists of a *DSL modem* connected to a telephone wall jack, and to a standard NIC in your computer (see Figure 16-6). A DSL modem is not an actual modem—it's more like an ISDN terminal adapter—but the term stuck, and even the manufacturers of the devices now call them DSL modems.

**Figure 16-6**

An ADSL modem connected to a PC and Telco





**NOTE** The one potentially costly aspect of ADSL service is the ISP link. Many ISPs add a significant surcharge to use ADSL. Before you choose ADSL, make sure that your ISP provides ADSL links at a reasonable price. Most telephone companies bundle ISP services with their ADSL service for a low cost.

Many offices use DSL. In my office we use a special DSL line (we use a digital phone system so the DSL must be separate) that runs directly into our equipment room (Figure 16-7).

This DSL line runs into our DSL modem via a standard phone line with RJ-11 connectors. The DSL modem connects to our gateway router with a CAT 5e patch cable, which in turn connects to the company's hub. Figure 16-8 shows an ADSL modem and a router, giving an idea of the configuration in our office.

Home users often connect the DSL modem directly to their PC's NIC. Either way, there is nothing to do in terms of installing DSL equipment on an individual system—just make sure you have a NIC that works with your DSL modem (almost all do). The person who installs your DSL will test the DSL line, install the DSL modem, connect it to your system, and verify that it all works. The one issue you may run into with DSL is something called *PPP over Ethernet (PPPoE)*.

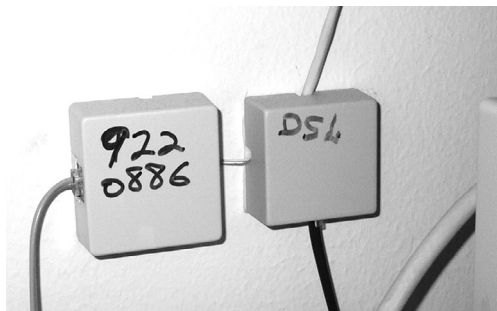
The first generation of DSL providers used *bridged connection*—once the DSL line was running it was the same as if you snapped an Ethernet cable into your NIC—you were on the network. Those were good days for DSL. You just plugged your DSL modem into your NIC and, assuming your IP settings were whatever the DSL folks told you to use, you were running.

The DSL providers didn't like that too much. There was no control—no way to monitor who was using the DSL modem. As a result, the DSL folks started to use PPPoE, a protocol that was originally designed to encapsulate PPP frames into Ethernet frames. The DSL people adopted it to make stronger controls over your DSL connection. In particular, you could no longer simply connect, you now had to logon with an account and a password to make the DSL connection. PPPoE is now predominant on DSL. If you get a DSL line, you must add software to your PC to enable you to logon to your DSL network. If you have Windows XP, you have built in support. Many SOHO routers come with built in PPPoE support, enabling you to enter your user name and password into the router itself.

While most DSL providers will gladly configure a single system for DSL, no DSL provider will configure a gateway router for free—some DSL companies even try to prevent more than one machine from using a single DSL connection. Many companies sell SOHO routers with all the necessary DSL support—including PPPoE.

**Figure 16-7**

DSL line into  
equipment room



**Figure 16-8**  
DSL connection  
with router



## Cable Modems

The big competition for ADSL comes from the cable companies. Almost every house in America has a coax cable running into it for cable TV. In a moment of genius, the cable industry realized if they could put the Home Shopping Network and the History Channel into every home, why not provide Internet access? The entire infrastructure of the cabling industry had to undergo some major changes to deal with issues like bidirectional communication, but most cities in the United States now provide cable modem service. Cable modems are well on their way to becoming as common as cable TV boxes, or at least such is the dream of the cable companies.



**NOTE** DSL and cable modem are collectively called *broadband* connections.

The single most impressive aspect of cable modems is their phenomenal top speeds. These speeds vary from cable company to cable company, but most advertise speeds in the (are you sitting down?) *10 to 27 megabits per second* range! Okay, now that you've heard this exciting news, don't get too excited, because there is a catch: You have to *share* that massive throughput with all of your neighbors who also have cable modems. The problem: as more people in the neighborhood connect, the throughput of any individual modem drops. How significant is this drop? Some early installations showed that the throughput of a heavily used cable line can drop to *under 100 Kbps*! The cable modem providers are aware of this and now do a good job of keeping any single neighborhood from getting too many systems and causing these terrible drops in service. Today most cable modems provide a throughput speed of 1 to 3 Mbps downloading and 500 Kbps uploading, though some service providers limit upstream access speeds to 256 Kbps or less.



**NOTE** Unlike DSL, most cable companies do provide a guaranteed minimum speed.

A cable modem installation consists of a cable modem connected to a cable outlet. The cable modem gets its own cable outlet, separate from the one that goes to the television. It's the same cable line, just split from the main line as if you were adding a second cable outlet for another television. As with ADSL, cable modems connect to PCs using a standard NIC (see Figure 16-9).

It's hard to tell a cable modem from a DSL modem! The only difference, other than the fact that one will have "cable modem" printed on it while the other will say "DSL modem" is that the cable modem has a coax and an RJ-45 connector while the DSL modem has an RJ-11 and an RJ-45 connector.

Cable modems have proven themselves to be reliable and fast and have surpassed DSL as the broadband connection of choice in homes. Cable companies are also aggressively marketing to business customers with high-speed packages, making cable a viable option for businesses.

## Satellite

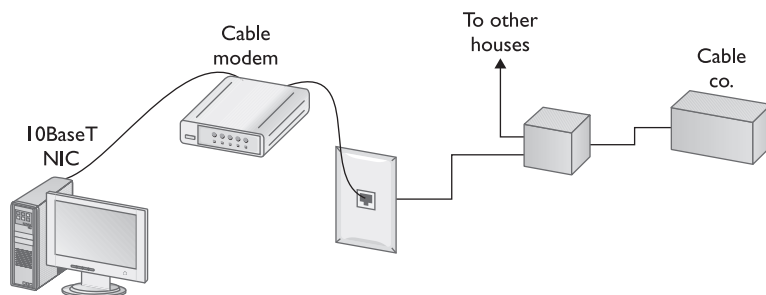
Living in the countryside may have its charms, but it makes it tough to get high-speed Internet access. For those too far away to get anything else, satellite may be your only option. Satellite access comes in two types: one-way and two-way. *One-way* means that you download from satellite but you must use a PSTN connection for uploads. *Two-way* means the satellite service handles both the uploading and downloading.

Satellite isn't as fast as DSL or cable modems, but it's still faster than PSTN. Both one-way and two-way satellite connections provide around 500 Kbps download and 50 Kbps upload. Satellite requires a small satellite antenna, identical to the ones used for satellite television. This antenna connects to a satellite modem, which in turn connects to your PC or your network (Figure 16-10).



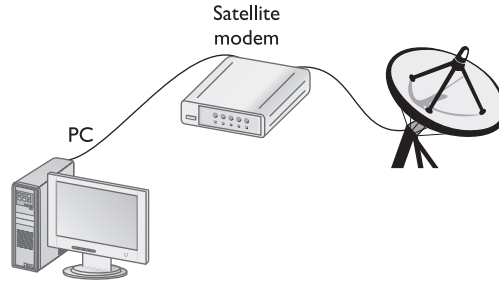
**TIP** Neither cable modems nor satellite use PPP, PPPoE, or anything else that begins with three Ps.

**Figure 16-9**  
A typical cable  
modem  
configuration





**Figure 16-10**  
Satellite setup



## Which Connection?

With so many connection options for homes and small offices, making a decision is often a challenge. Your first question is availability: which services are available in your area? The second question is how much bandwidth do you need? This is a question of great argument. Most services will be more than glad to increase service levels if you find a certain level is too slow. I usually advise clients to start with a relatively slow level, and then increase if necessary. After all, it's hard to go slower once you've tasted the higher speeds, but relatively painless to go faster!

## WAN Connections

A *wide area network (WAN)* is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more LANs connected together over a distance. Computers in a WAN often connect through a public network, such as the telephone system. They can also connect through leased lines or satellites. The largest WAN in existence is—can you guess?—the Internet.

As I hope you realize by now, mystical packet gnomes do not magically whisk information from one LAN to another. Packets travel over a variety of connection media. Because a large quantity of information needs to travel between LANs in a speedy and reliable fashion, WAN backbone connections are faster and *far* more expensive than any SOHO connection. You're not going to find a typical home user connecting her computer to an ATM or a T3 connection (we'll discuss these in a moment); those are for businesses and universities that have many computers connecting to other LANs across the globe.

WAN connections come with a rather hairy hodgepodge of terms, so it's best to think about WAN connections using the OSI seven-layer model. All WAN connections are digital and use some form of data packets, so there's a strong analogy between WAN connections and LAN connections. All WAN connections consist of three distinct parts: the physical link, the signal method, and the switching protocol. The *physical link* works at the Physical layer of OSI, and is simply the cabling and the connections, as well as the equipment on each end of the link that sends and reads the signal. The *signal method* is roughly the Data Link layer and deals with how the signals propagate across the WAN connection. The *switching protocol* is the framing method and also works at the Data Link layer, defining the ways each WAN device is addressed and defines the packets used.

We can break all WAN connections in two groups: copper carriers and fiber carriers. Both copper and fiber have their own unique physical links and signal methods but share the same switching protocols. Let's look at copper and fiber connections, and then see the switching protocols they share.

## Copper Carriers: T1 and T3

Taking an analog voice signal and moving it across hundreds or thousands of miles has always been a challenge for the telephone industry. One way to make voice transmission easier is to convert it from analog to digital. Digital signals are easier to create, can accept more degradation over distance than analog, and allow for the idea of packetizing the information to allow multiple conversations to take place over the same line at the same time. Digitizing voice for long-distance communication can be traced back to the 1930s, but it wasn't until the introduction of the T1 technology that we saw widespread use of digital voice communication across the United States.

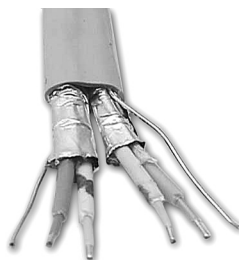
T1 has several meanings. First, it refers to a high-speed digital networking technology called a T1 connection. Second, the term *T1 line* refers to the specific, shielded, two-pair cabling that connects the two ends of a T1 connection (Figure 16-11). Two wires are for sending data and two wires for receiving data. At either end of a T1 line you'll find an unassuming box called a Channel Service Unit/Digital Service Unit (CSU/DSU). The CSU/DSU has a second connection that goes from the phone company (where the boxes reside) to a customer's equipment (usually a router). A T1 connection is point-to-point—you cannot have more than two CSU/DSUs on a single T1 line.

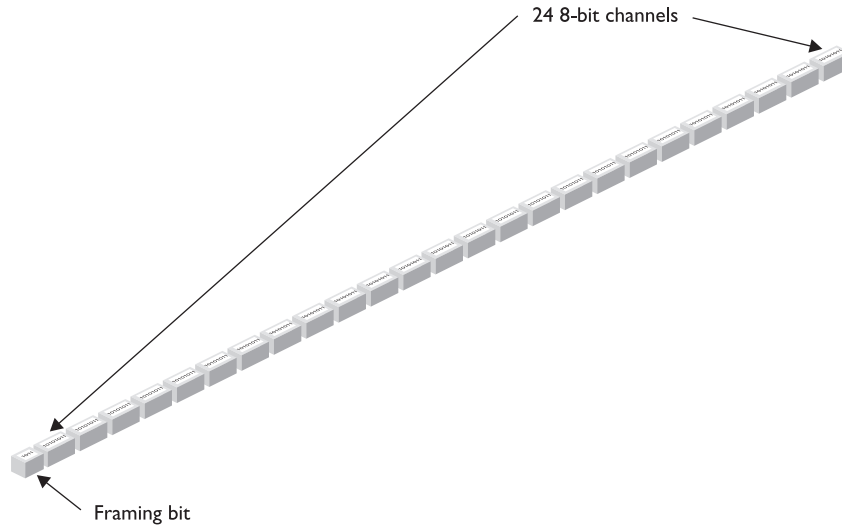
T1 uses a special signaling method called DS1. *DS1* uses a relatively primitive frame—the frame doesn't need to be complex because with point to point there's no addressing necessary. Further, error checking is handled at higher layers, not at the Physical layer, which means the frame does not need the added complexity.

Each DS1 frame has 25 pieces: a framing bit and 24 data channels. Each data channel can hold 8 bits of data; the framing bit and data channels combine to make 193 bits per DS1 frame. These frames are transmitted 8000 times/sec, making a total throughput of 1.544 Mbps (Figure 16-12). DS1 defines, therefore, a data transfer speed of 1.544 Mbps, split into 24 64-Kbps *channels*. Each channel can carry a separate signal, or channels can be configured (with the right CSU) to work together. This process of having frames that carry a bit of every channel in every frame sent on a regular interval is called *time division multiplexing*.

**Figure 16-11**

T1 cable





**Figure 16-12** DS1 frame



**TIP** If you're handy with math in your head or with a calculator, you might immediately question the accuracy of the numbers involved in describing T1 speeds. After all,  $193 \text{ bits} \times 8,000 \text{ seconds} = 1,544,000 \text{ bits per second}$ , or 1.544 million bits per second. You normally wouldn't use the abbreviation Mbps for *million* bits per second, right? Sadly, that's exactly the case here. When reading the signaling speeds regarding T1 and other WAN technologies (such as SONET, discussed in the following), think "millions" and "billions" of bits per second when you see Mbps and Gbps!

An analogy I like to use in class for T1 technology is that of a conveyor belt in a milk-bottling factory. At regular intervals, big crates with 24 bottles come rolling down the belt. When they reach the filling machine, the bottles get filled with milk and the crate keeps rolling down to the other end where two machines take over: the labeling and sorting machines. The labeling machine plucks out the bottles and applies a label to each, appropriate to the contents. The sorting machine sorts the bottles into cases of each type.

This is pretty simple if the filling machine uses only one type of milk. All 24 bottles fill with whole milk; all are labeled as whole milk; and all go into the case marked "Whole Milk." Once enough bottles come in with the milk, the case gets completed, and you have a product.

That's pretty much how an Ethernet packet works, right? The whole packet is used for a single set of data, and then multiple packets get put together at the end to make your data transfer complete.

The cool thing about the DS1 frame, though, is that you don't have to use the whole frame for a single set of data. With the right CSU/DSU at either end, you can specify which channels go with a specific thread of data. Sloshing back into the analogy . . . the milk company produces four types of milk: whole milk, lowfat milk, chocolate milk, and strawberry milk. The strawberry milk is seasonal; the whole milk sells the most, followed by chocolate, and then lowfat.

To accommodate the different products, the factory master designates channels 1–10 for whole milk, 11–18 for chocolate milk, 19–22 for lowfat milk, and 23–24 for strawberry. Now the labeling and sorting machines are going to have to work for a living! When a crate reaches the filling machine, the bottles get filled with the various types of milk, and then the crate trundles on down the belt. The labeling machine knows the numbering system, so it labels bottles 1–10 as whole milk, 11–18 as chocolate, and so on. The sorting machine also knows the system and has four cases at hand, one for each product. As the bottles arrive, it places them into the appropriate cases. Now notice that the cases will fill at different rates of speed. It'll take a while for the strawberry case to fill, especially compared to the whole milk, because only two channels in each crate carry strawberry.

What happens if the cows temporarily stop producing chocolate milk? Will the whole factory need to be reordered so the filling machine's eight chocolate dispensers can dispense some other kind of milk? The answer at this factory is no. The crates continue to roll down the conveyor belt at regular intervals. The filling machine fills the bottles in channels 1–10 with whole milk, leaves the bottles in channels 11–18 empty, and puts lowfat and strawberry in channels 19–22 and 23–24, respectively.

DS1 and T1 work the same way! The frame just keeps jetting down the line, even if some of the channels contain no data. The CSU/DSU at the other end collects the data streams and keeps them separate. To paraphrase the immortal words of Professor Egon, "Never cross the streams." Otherwise you'd lose data!

To bring the milk bottling factory analogy completely into the realm of networking and T1 connections, keep in mind that there would be two conveyor belts running in opposite directions. Milk flows in; milk flows out. You can both send and receive on T1 connections.

A T1 line is a dedicated phone connection that you lease, usually on a monthly basis, from the telephone company. It has no telephone number and it's always connected. An entire T1 bundle can be expensive, so many telephone companies let you buy just some of these individual channels. This is known as *fractional T1 access*.



**NOTE** Each 64K channel in a DS1 signal is called a DS0. ISDN B lines are DS0 channels.

A T3 line is a dedicated telephone connection supporting a data rate of about 43 Mbps. A T3 line consists of 672 individual channels, each of which supports 64 Kbps. T3 lines (sometimes referred to as DS3 lines) are used mainly by ISPs connecting to the Internet backbone, and by the backbone itself.

Similar to the North American T1 line, *E1* is the European format for digital transmission. An E1 line carries signals at 2 Mbps (32 channels at 64 Kbps), compared to the T1's 1.544 Mbps (24 channels at 64 Kbps). Both E1 and T1 lines may be interconnected for international use. There are also E3 lines, which are similar to T3 lines, with a bandwidth of 45 Mbps. Japan also has its own digital transmission formats: J-1 is identical to T1 in every way with the exception of a few signaling differences, while J-3 provides 480 channels with a throughput of 32 Mbps.

A CSU/DSU, as mentioned earlier, connects a leased T1 or T3 line from the telephone company to a customer's equipment. A CSU/DSU has (at least) two connectors, one that goes to the T1/T3 line running out of your demarc/NJ and another connection that goes to your router. It performs line encoding and conditioning functions, and often has a loopback function for testing. Although CSU/DSUs look a lot like modems, they are not modems, because they don't modulate/demodulate. All they do is interface between a T1 or T3 line and a router. Many newer routers have CSU/DSUs built into them. Figure 16-13 shows the back of a Cisco router with two T1 interfaces. Two interfaces on one router is quite common, the dual links providing redundancy if one link goes down.

The CSU part of a CSU/DSU is designed to protect the T1 or T3 line and the user equipment from lightning strikes and other types of electrical interference. It also stores statistics and has capabilities for loopback testing. The DSU part supplies timing to each user port, taking the incoming user data signals and converting the input signal into the specified line code, and then framing the format for transmission over the provided line.

## Fiber Carriers: SONET/SDH and OC

In the early 1980s, fiber-optic cabling became the primary tool for long distance communication all over the world, but the major telephone carriers had four different, virtually incompatible transmission standards—not a good thing. In an incredible moment of corporate cooperation, in 1987, all of the primary fiber-optic carriers decided to drop their own standards and move to a new international standard called *Synchronous Optical Network (SONET)* in the United States and *Synchronous Digital Hierarchy (SDH)* in Europe.

**Figure 16-13**

Cisco router with two WAN connections  
(photo courtesy of Cisco Corp.)





**NOTE** Students often wonder why two separate names exist for the same technology. In reality, SONET and SDH vary a little in their signaling and frame type, but routers and other magic boxes on the Internet handle the interoperability between the standards. The American National Standards Institute (ANSI) publishes the standard as SONET; the International Telecommunications Union (ITU) publishes the standard as SDH, but includes SONET signaling. For simplicity sake and because SONET is the more common term in the United States, this book uses SONET as the generic term for this technology.

SONET is the primary standard for connecting fiber-optic transmission systems. There is a high level of comparison of SONET to network standards like Ethernet or Token Ring because SONET defines interface standards at the Physical and Data Link layers of the OSI seven-layer model. The physical aspect of SONET is partially covered by the Optical Carrier standards, but it also defines a ring-based topology that most SONET adopters now use. SONET does not require a ring, but a SONET ring has extra survivability in case of line loss. As a result, most of the big, long-distance optical pipes for the world's telecommunications networks are SONET rings.



**TIP** SONET is one of the most important standards for making all of our WAN interconnections—and it's also the least likely standard you'll ever see because it's hidden away from all but the biggest networks.

The real beauty of SONET lies in its multiplexing capabilities. A single SONET ring can combine multiple DS1, DS3, even European E1 signals and package them into one big SONET frame for transmission down the line. Clearly, for SONET to handle such large data rates it needs high-capacity fiber optics—and that's where the optical carrier standards come into play!

The *Optical Carrier (OC)* specification is used to denote the optical data carrying capacity (in Mbps) of fiber-optic cables in networks conforming to the SONET standard. The OC standard is an escalating series of speeds, designed to meet the needs of medium-to-large corporations. SONET establishes OCs from 51.8 Mbps (OC-1) to 13.2 Gbps (OC-256).

SONET uses the *Synchronous Transport Signal (STS)* signal method. The STS consists of two parts: the STS *payload* (which carries data), and the STS *overhead* (which carries the signaling and protocol information). When we talk about STS, we add a number to the end of "STS" to designate the speed of the signal. For example, STS-1 is the 51.85 Mbps signal that runs on an OC-1 line. STS-3 runs at 155.52 Mbps on OC-3 lines, and so on.

Table 16-1 describes the most common optical carriers.

## Packet Switching

All of these impressive connections that start with Ts and Os are powerful, but they are not in and of themselves a complete WAN solution. These WAN connections make up the entire mesh of long-range connections we call the Internet, but these same connec-

**Table 16-1**  
Optical Carriers

SONET Optical Level	Line Speed	Signal Method
OC-1	51.85 Mbps	STS-1
OC-3	155.52 Mbps	STS-3
OC-12	622.08 Mbps	STS-12
OC-24	1.244 Gbps	STS-24
OC-48	2.488 Gbps	STS-48
OC-192	9.955 Gbps	STS-192
OC-256	13.22 Gbps	STS-256
OC-768	39.82 Gbps	STS-768

tions also carry voice and other types of data as well as TCP/IP packets. All of these connections are point to point, so we need to add another level of devices to enable us to connect multiple T1s, T3s, or OC connections together to make that mesh. That's where packet switching comes into play.

Around the same time the ARPANET folks came up with the idea of routers, the telephone industry was moving from an analog system to a digital one where long-distance (and later, local) conversations were moved using packets of data. Packets, as you know from what you've learned about networking, need some form of addressing scheme to get from one location to another. The telephone industry came up with its own types of packets that run on ISDN, T1/T3, and OC lines to get data from one CO to another. These packet-switching protocols are functionally identical to routable network protocols such as IPX/SPX and TCP/IP. One of these packet-switching protocols—ATM—started as a high-speed LAN protocol but is not used by the telephone industry.

## X.25

X.25 Packet Switched networks enable remote devices to communicate with each other across high-speed digital links without the expense of individual leased lines. X.25 encompasses the first three layers of the OSI seven-layer architecture, and gives you a virtual high-quality digital network at low cost. It is inexpensive because you share the infrastructure with other people who use the service. In most parts of the world, users pay for X.25 by way of a fixed monthly connection fee combined with a charge for the amount of data passed through the X.25 connection.

X.25 is considerably slower than the other WAN communications discussed here, but it's still out there. The big reason, aside from its continued large presence in Europe, is that X.25 is used by Automatic Teller Machines (ATMs) in the United States. So, oddly enough, X.25 is used with ATM, just not the ATM you're about to learn about! X.25 has been around since the mid-1970s, so it's thoroughly debugged and stable. You literally never encounter data errors on modern X.25 networks.

## Frame Relay

*Frame Relay* is an extremely efficient data-transmission technique used to send digital information such as voice, data, LAN, and WAN traffic quickly and cost-efficiently to many destinations from one port. It is especially effective for the off-again/on-again traffic typ-



ical of most LAN applications. Frame Relay switches packets end-to-end much faster than X.25, but without any guarantee of data integrity at all. The network delivers the frames whether the CRC check matches or not. You can't even count on it to deliver all the frames, because it will discard frames whenever there is network congestion. In practice, however, a Frame Relay network delivers data quite reliably. Unlike the analog communication lines that were originally used for X.25, the modern digital lines that use Frame relay have very low error rates.

Frame Relay is extremely popular. If you decide to go with a T1 line in the United States, what you're getting is a T1 line running Frame Relay, although some companies are now moving away from Frame Relay and moving toward ATM as their packet-switching solution.

## ATM

Most people think an ATM is an automatic teller machine, and so it is, but not in this case. ATM is short for *Asynchronous Transfer Mode*. ATM was originally designed as a high-speed LAN networking technology. While ATM only saw limited success in the LAN world, ATM has become extremely popular in the WAN world. Most of the SONET rings that move voice and data all over the world use ATM for packet switching. ATM integrates voice, video, and data on one connection, using short and fixed-length packets called *cells* to transfer information. Every cell sent with the same source and destination travels over the same route, giving ATM the potential to remove the performance bottlenecks that exist in today's LANs and WANs. The key problem ATM addresses is that data and audio/video transmissions have different transfer requirements. Data can tolerate a delay in transfer, but not signal loss. Audio and video transmissions, on the other hand, can tolerate signal loss but not delay. Because ATM transfers information in cells of one set size (53 bytes long), it is scalable and can handle both types of transfers well. ATM transfer speeds range from 155.52 to 622.08 Mbps and beyond.

## Using Remote Access

Because most businesses are no longer limited to a simple little shop like you would find in a Dickens novel, there is a great need for people to be able to access files and resources over a great distance. Enter remote access. *Remote access* uses WAN and LAN connections to enable a computer user to log on to a network from the other side of a city, a state, or even the globe. As people travel, information has to remain accessible. Remote access enables users to dial into a server at the business location and log in to the network as if they were in the same building as the company. The only problem with remote access is that there are so many ways to do it! The four most common forms of remote access are as follows:

- **Dial-up to the Internet** Using a dial-up connection to connect to your ISP
- **Private dial-up** Using a dial-up connection to connect to your private network
- **Virtual private network** Using an Internet connection to connect to a private network
- **Dedicated connection** Using a non-dial-up connection to another private network or the Internet

In this section we look at configuring these four types of connections in a Windows environment. After seeing how to configure these types of remote connections, we move into observing some security issues common to every type of remote connections. Last, we'll see how to use Windows Internet Connection Sharing with any of these remote access options to enable a network of computers to use a single connection for remote access.



**NOTE** *Extranet* is one of those terms that you'll see more in books than in the day-to-day workings of networks and network techs. So, what is an extranet? Whenever you allow authorized remote users to access some part of your private network, you have created an extranet.

## Dial-up to the Internet

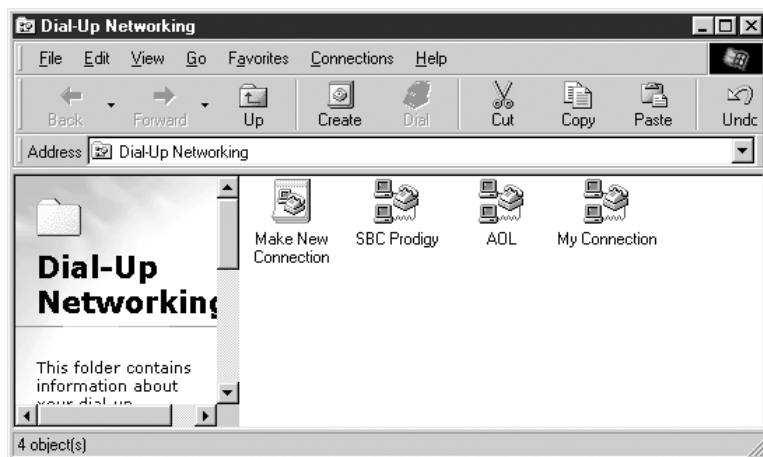
Dialing up to the Internet is the oldest, cheapest, and the most common way for home and small office users to connect to the Internet. Dial-up requires you to have some method to create a connection to your ISP. This connection needs information to work. At the very least, you'll need:

- The telephone number to dial
- The modem to use (you might have more than one!)
- User name and password (provided to you by the ISP)
- Type of connection (PPP or SLIP)
- IP information (provided to you by the ISP)

Also keep in mind that you might have more than one dial-up connection. Your operating system needs a way to create and store multiple connections for you to choose from depending on which dial-up connection you want to make at a given moment.

Every version of Microsoft Windows since Windows 95 comes with some tool to help you set up your dial-up connections. This tool has had many names. It's called *Dial-Up Networking* (DUN) in Windows NT and 9x (Figure 16-14) and treats dial-up connections

**Figure 16-14**  
DUN in  
Windows 98



separately from other network connections. Windows 2000 calls it Network and Dial-up Connections; Windows XP calls it Network Connections, combining dial-up connections into the same dialog box as your other network connections (Figure 16-15). Whatever the name, this tool is what you use to create dial-up connections.



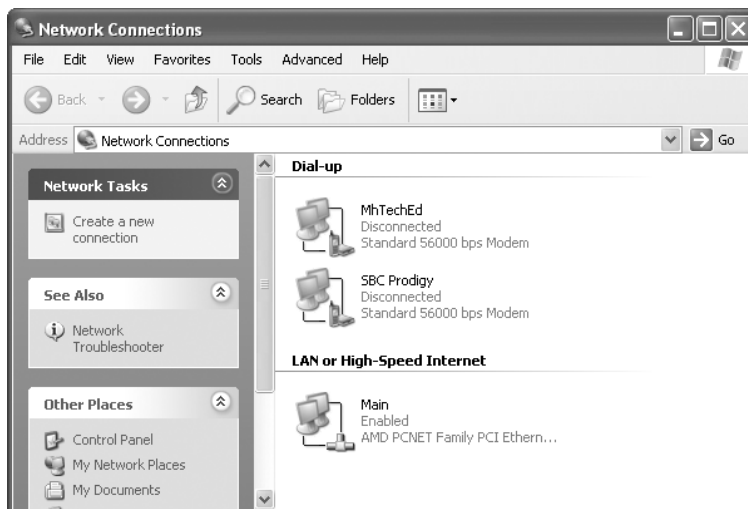
**TIP** Two issues to remember. First, even though all of these programs have different names, they are accessed the same way: Start | Programs | Accessories | Communications | <name of program>. Second, make sure you are comfortable with the different names for the different versions of Windows.

All these tools have a Make New Connection (or *Create a new connection* option in Windows XP) icon that starts a utility (a *wizard* in Microsoft parlance) to help you make the connections you need. Every version of Windows has a slightly different wizard. Even though these wizards may each have their own look, they all do the same thing—make new connections. Figure 16-16 shows the Windows 98 wizard in action. Note that it only configures dial-up connections. If you want to make any other type of connection, you need to head over to the Network Neighborhood Properties dialog box.

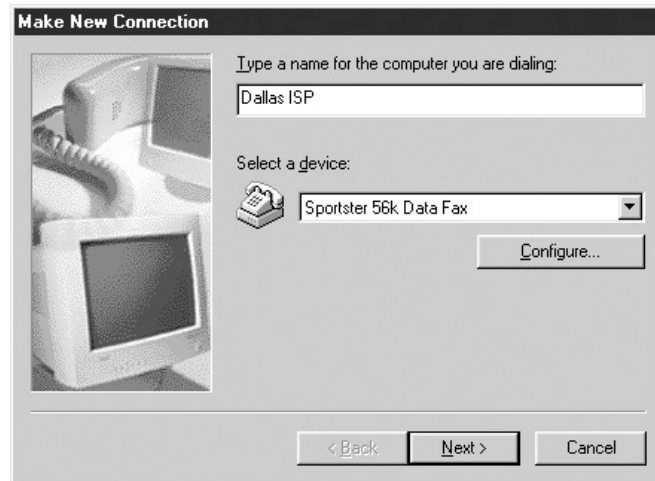
The New Connection Wizard in Windows XP (Figure 16-17) is for more than just dial-up connections. This one wizard handles every type of remote connection you might want to make, not just dial-up connections. We'll see this wizard again as we move into other remote connection options.

Each Windows dial-up wizard has a different look and feel, but we can watch the creation of two dial-up connections—one in Windows 98 and one in Windows XP—to get a pretty good grasp of the scope of how to do this. Let's start with Windows 98.

**Figure 16-15**  
Network  
Connections in  
Windows XP  
Professional



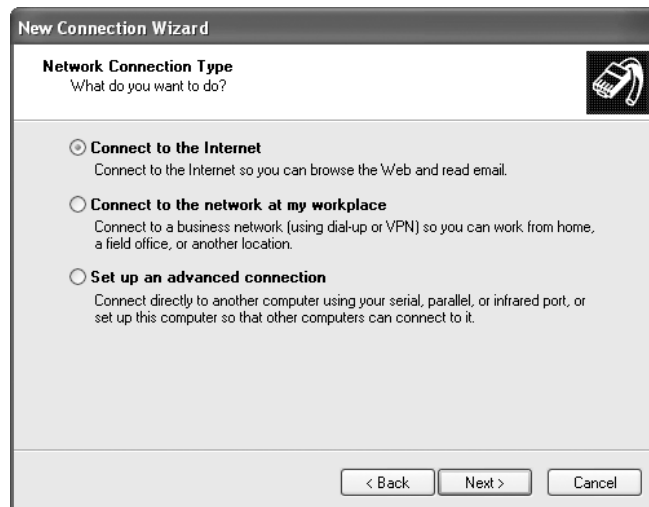
**Figure 16-16**  
Windows 98  
DUN Wizard in  
action



## Dial-up in Windows 98


Creating a dial-up connection in Windows 98 is simple—possibly too simple as you often need to go back into a connection after it's created by the wizard to add information. The previous Figure 16-16 just showed you the first screen in the DUN wizard in Windows 98, asking for a name for the connection and the modem to use. Always give your connections a good descriptive name so you can tell them apart. Clicking the Next button (Figure 16-18) brings you to the second and last screen (other than the Finish screen) of the wizard where it prompts you for a phone number and country code (for those who like to make expensive remote connections)!

**Figure 16-17**  
Windows XP  
Professional New  
Connection  
Wizard in action



**Figure 16-18**

Prompting for  
telephone  
number



**Make New Connection**

Type the phone number for the computer you want to call:

Area code:  Telephone number:

Country code:

< Back Next > Cancel

That's pretty much it for the Windows 98 DUN wizard. So where is the SLIP/PPP selection? Where do you enter the user name and password? Where do you enter IP information? This is where the age of the old Windows 98 wizard shows—you need to go to other places to complete the process. The user name and password are saved the first time you dial the connection. Figure 16-19 shows the Connect To dialog box when you select a connection the first time. Here you enter the user name, password, and dialing location—we'll discuss dialing locations in a moment. You can also change the phone number here.

To make other changes to a dial-up connection's settings in Windows 98, you'll need to head to the connections' Properties dialog box. To change a connection's properties, just alternate-click the connection and select Properties to see a dialog box like the one shown in Figure 16-20. The General tab enables you to make changes to the phone number and the modem you want to use as well as other settings.

**Figure 16-19**

Connect To  
dialog box



**Connect To**

Dallas ISP

User name:

Password:

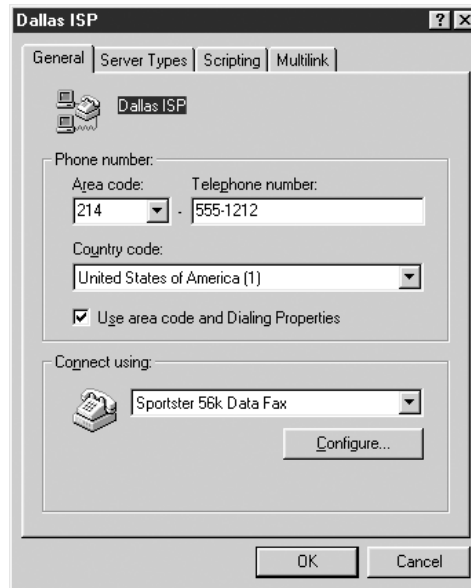
☒ Save password

Phone number:

Dialing from:  [Dial Properties...](#)

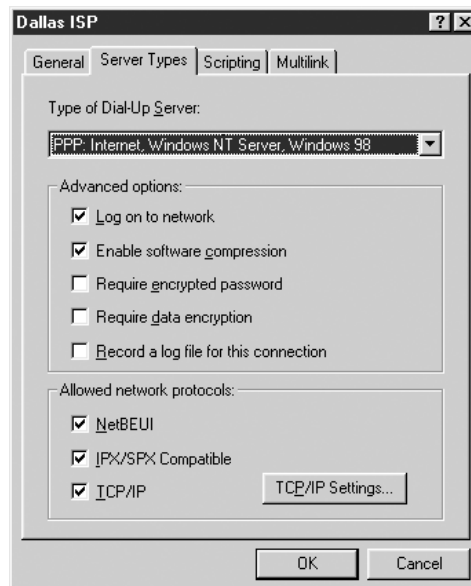
Connect Cancel

**Figure 16-20**  
Connection  
Properties  
General tab



The most heavily visited tab in this dialog box is the Server Types tab (Figure 16-21). If you're having a problem with a Windows 98 dial-up connection, this is probably your first place to check. This is where you select the type of connection: PPP, SLIP, and other types; but given that Windows 98 defaults to PPP, you're usually in good shape.

**Figure 16-21**  
Connection  
Properties Server  
Types tab



How you need to set up the Advanced options differs for every ISP, although the defaults of *log on to network* and *Enable software compression* work for most ISPs. The *Allowed network protocols* section defines what protocols to load for this connection. By default, Windows 98 loads NetBEUI, IPS/SPX, and TCP/IP. This is not good because running NetBEUI in particular will expose your system to hacking. Be sure to turn off NetBEUI and IPX/SPX! Your connection is set up for DHCP by default, but if you needed to configure TCP/IP settings like the IP address or DNS server, you click on the TCP/IP Settings button.



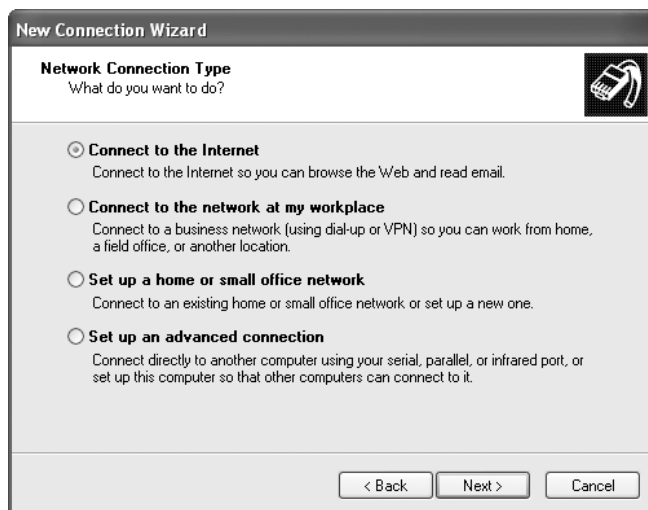
**NOTE** The Scripting and Multilink tabs are rarely used. The Scripting tab runs script files to support older connections and the Multilink tab enables two modems to work together as one connection. Multilink requires ISP support and few ISPs offer this option.

Once you've made these settings, you're ready to start dialing. Keep in mind that your best source for information on configuring a dial-up connection (and this is true for all versions of Windows) is your ISP. Every ISP has good-to-superb support to show you how to configure these settings properly. Let's do this again, but this time use Windows XP Professional.

## Windows XP Dial-up

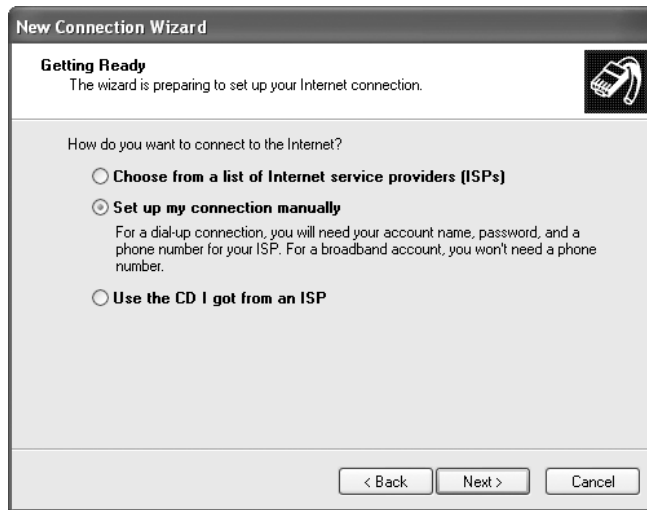
The Windows XP New Connection Wizard shows how Microsoft has matured the dial-up process. You'll find more screens and more questions, reflecting more robust and sophisticated dial-up connections. This is an intelligent wizard that can change based on how you're connected to the network (domain vs. workgroup) and other settings. Way back in Figure 16-17 you saw the first screen of XP's New Connection Wizard. Note that it has three settings. Now look at Figure 16-22—it has a fourth setting called *Set up a home or small office network*. The computer in Figure 16-17 is part of a domain so the wizard assumes you don't want to set up a home or small office network—a pretty safe assumption!

**Figure 16-22**  
New Connection  
Wizard in  
Windows XP





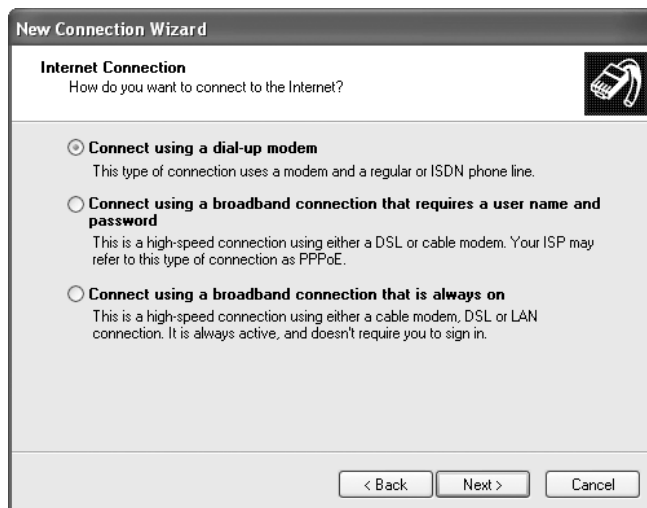
**Figure 16-23**  
Selecting a manual  
connection setup



Either way, you're going to configure a dial-up connection to the Internet, so just select the *Connect to the Internet* radio button and click Next to see Figure 16-23. Given that most people who connect to the Internet aren't astute like us, Microsoft gives the user the choice for more automated setups for common ISPs, either built into Windows (can you say MSN?) or via CDs provided by the ISP. Because we *are* astute techs, select *Set up my connection manually* (Figure 16-24), click Next, and choose how you want to connect to the Internet.

Ah ha! While the obvious choice is *Connect using a dial-up modem*, as Figure 16-24 shows, note the other choices—these will be handy when you configure a dedicated connection later.

**Figure 16-24**  
Connection type



The next two screens are simple. Just click Next and the wizard prompts for the name of the ISP; click Next again and it prompts for the phone number. The screen after that (Figure 16-25) asks for the user account and password. It also has three check boxes. The first enables anyone on this computer to use the same user account and password—this is handy when multiple people use the same dial-up connection to access the Internet. The second check box defines this as the default Internet connection. My laptop has an 802.11 NIC that I use as my default, so I turn this off. The third and last check box turns on Internet Connection Firewall (ICF)—Windows XP’s built-in protection software for computers connecting to the Internet. Chapter 17, “Protecting Your Network,” covers ICF and other firewalls in some detail.

When you click Next the wizard is done (after a few Finish dialog boxes) and a new connection shows up in Network Connections. If any settings for this connection need adjusting, you go into the connection properties, just as you did in Windows 98. Figure 16-26 shows the Properties dialog box for a dial-up connection to MHTechEd.

The Properties dialog box for a dial-up connection in Windows XP is similar to the one in Windows 98, but adds a number of extras. The General tab enables you to change telephone numbers, modem, and something called Dialing Rules. Dialing Rules are the same thing as dialing locations in Windows 98 and we’ll discuss them in the next section. The Options tab provides general options like *Display progress while connecting* or the number of times to redial. The Security tab determines how to log on—how you set this varies among ISPs. (Log on is covered in more detail in the “Private Dial-up” section later in this chapter.) The Networking tab is where you go to set SLIP/PPP and edit TCP/IP settings. The Advanced tab is covered in the next chapter.

As you can see, configuring a dial-up connection isn’t difficult in any version of Windows. The only real challenge is remembering what you need to configure—usually your ISP has the answer for you—and getting comfortable with the differences in wizards.

Both of the dial-up connection installations you just saw required a dialing location (Windows 98) or a Dialing Rule (Windows XP). Let’s see what that’s all about.

**Figure 16-25**  
Internet Account  
Information

**New Connection Wizard**

**Internet Account Information**

You will need an account name and password to sign in to your Internet account.

Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: mikemeyers21

Password: .....

Confirm password: .....

☒ Use this account name and password when anyone connects to the Internet from this computer

☐ Make this the default Internet connection

☐ Turn on Internet Connection Firewall for this connection

< Back    Next >    Cancel

**Figure 16-26**

Dial-up  
connection  
Properties  
dialog box



## Dialing Rules

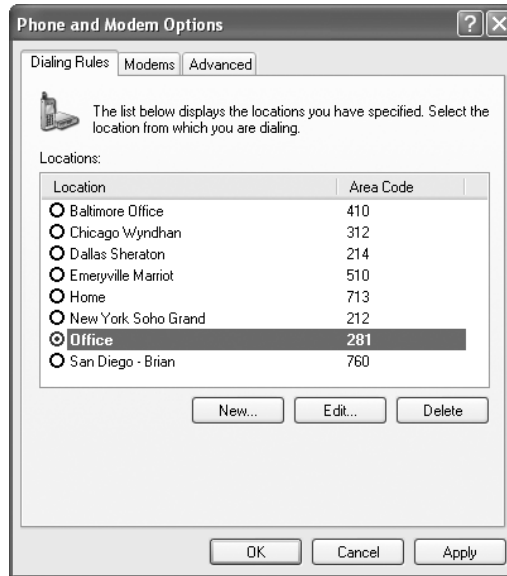
A dialing location/Dialing Rules (we'll use the term "Dialing Rules") is the set of rules that tells the modem how to dial from your current location. Do you need to dial a 9 first to get a dial tone? Do you need to use area codes to make a local call? Do you need to disable call waiting? Do you want to use a calling card? That's where the Dialing Rules are important. Every version of Windows has a Control Panel applet to help you configure these options. In Windows 98 and NT the applet is called Telephony. In Windows 2000 and XP the applet is called Phone and Modem Options. Whatever the name, this applet gives you the ability to configure your modem to dial from any location. Dialing Rules aren't terribly helpful to a computer that stays in one place, but are important for a computer that dials from different places (like my laptop). Figure 16-27 shows the Dialing Rules property sheet for my Windows XP laptop—I travel a lot!

To set up a particular location, select it and click on the Edit button. Figure 16-28 shows the Edit Location dialog box for my Office location. Note the options for local and long distance calls, as well as call waiting. The Area Code Rules tab enables me to select which area codes are local and which are long distance—in Houston we must dial the area code for local calls and long distance calls, so the computer needs to know which area codes are for local calls. The Calling Card tab enables me to enter my calling card information if I want to use one for this location.

## Private Dial-up

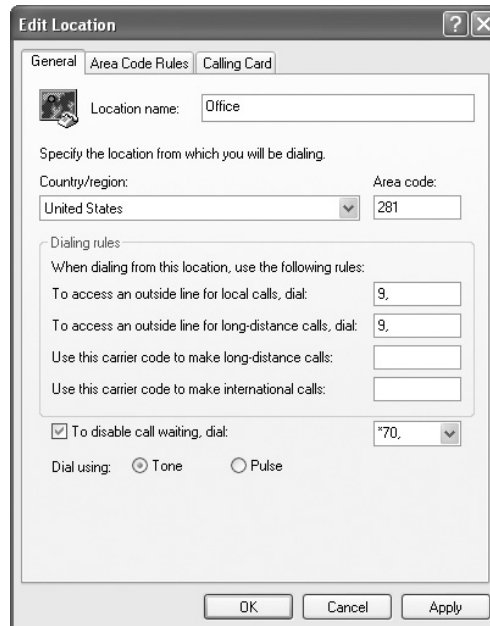
A private dial-up connection connects a remote system to a private network via a dial-up connection. Private dial-up requires two systems. One system acts as a *remote access server* (RAS). The other system is the client running DUN (or whatever your version of Windows calls your connection tool).

**Figure 16-27**  
Dialing Rules in  
Windows XP



In Windows a RAS is a server dedicated to handling users who are not directly connected to a LAN but who need to access file and print services on the LAN from a remote location. For example, when a user dials into a network from home using an analog modem or an ISDN connection, she is dialing into a RAS. Once the user is authenticated, she can access shared drives and printers as if her computer were physically connected to the office LAN.

**Figure 16-28**  
Edit Location  
dialog box in  
Windows XP



You must set up a server system in your LAN as a RAS server. That system becomes your RAS server, accepting incoming calls and handling password authentication. Because TCP/IP is the dominant (and best) remote connection protocol, you must ensure that your remote access server is using the TCP/IP protocol for its network communications. Many remote servers have separate sets of permissions for dial-in users and local users. You must also configure the server to set the dial-in user's rights and permissions. Configuring a RAS system is outside the scope of this book but it is important for you to properly configure a Windows system to act as a RAS client!



**TIP** *Remote access server* is a catchall phrase. It refers to both the hardware component (servers built to handle the unique stresses of a large number of clients calling in) and the software component of a remote access solution.

Most techs call RAS “razz,” rather than use the initials, “R-A-S.” This creates a seemingly redundant phrase used to describe a system running RAS: “RAS server.” This helps distinguish servers from clients and makes geeks happier.

Creating the client side of a private dial-up connection is identical to setting up a dial-up connection to the Internet. All versions of Windows provide a wizard (Figures 16-29, 16-30) that prompts for the name of the connection, the telephone number, and so forth and creates a new dial-up connection. This new connection resides in the same folder as your other dial-up connections. The only difference is that instead of having an ISP tell you what IP settings, account name, and password to use, the person who sets up the RAS server tells you this information. The one area that gets interesting in a private dial-up compared to dialing up to an ISP is how the remote user authenticates to the RAS.

**Figure 16-29**  
Windows XP  
New Connection  
Wizard prompting  
for connection



**Figure 16-30**  
Windows XP  
New Connection  
Wizard prompting  
for connection  
type



## Authentication

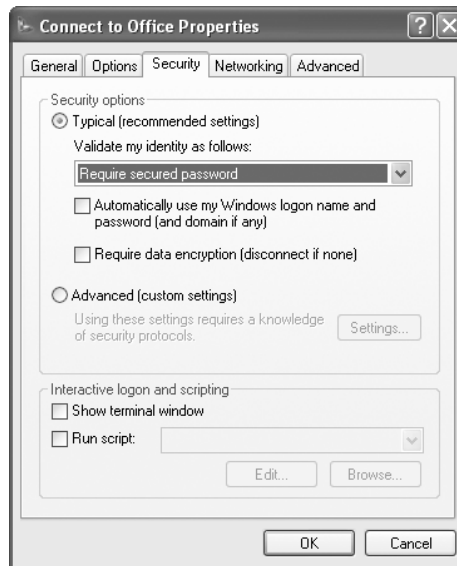
When a computer logs into a server in a LAN, the user name and password must travel along the wires of the network to the serving system. In early networks, this data was transmitted “in the clear.” The user name and password were transmitted on the wires in plain text, what most network techs refer to as *clear text*. Over the years, NOS makers came up with methods to encrypt the user name and password to prevent hackers from intercepting this important information. Because NOS makers control software development of both their client and their server software, for the most part they created their own proprietary encryption protocols.

In today’s increasingly interconnected and diverse networking environment, there is a motivation to enable different network operating systems to authenticate any client system from any other NOS. Modern network operating systems use standardized authentication protocols based on encryption methods like MIT’s Kerberos, enabling multiple brands of servers to authenticate multiple brands of clients. These LAN encryptions are usually transparent and work quite nicely even in mixed networks.

The need for good authentication was especially critical in dial-up environments. Given that any modem configured to accept incoming calls was effectively open to the public, the powers that be developed a blanket protocol called Remote Authentication Dial-In User Service (RADIUS). A RADIUS server keeps track of all authorized dial-in users and their passwords, effectively locking out any unauthorized remote access attempts. Unfortunately, RADIUS doesn’t include specifics for *how* to do this, leaving the details to various vendors who have created their own access tools over the years.

Today there are so many different remote access tools—based on UNIX/Linux, NetWare, and Windows serving programs—that most remote access systems and clients have to support a variety of different authentication protocols. All Windows clients come with good support for all of the common authentication protocols. Let’s take a look at a Windows XP connection, learn about some of the most common authentication protocols, and see where to configure them.

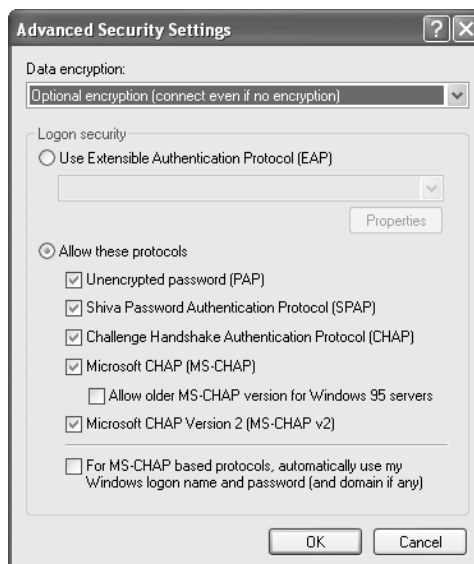
**Figure 16-31**  
Security tab in  
Windows XP



In the “Dial-up to the Internet” section earlier in this chapter, you saw the Properties dialog box for a Windows XP dial-up connection. Let’s go back to the Properties dialog box, this time concentrating on the Security tab. The Security tab is the primary tool used to configure authentication for private dial-up clients (Figure 16-31).

The Security options area is where you configure an authentication protocol. To see them, select the Advanced radio button, and then click the Settings button to display the authentication protocols Windows supports. Figure 16-32 shows the Advanced Security Settings dialog box.

**Figure 16-32**  
Authentication  
protocols available  
in Windows XP





Here is a quick list of the more common authentication protocols and their uses.

- **PAP** Password Authentication Protocol (PAP) is the oldest and most basic form of authentication. It's also the least safe, because it sends all passwords in clear text. No NOS uses PAP for a client system's login, but almost all network operating systems that provide remote access service will support PAP.
- **SPAP** Shiva is the brand name for a family of popular remote access servers. The Shiva Password Authentication Protocol is a unique encrypted protocol used to enable Windows clients to connect to these servers.
- **CHAP** Challenge Handshake Authentication Protocol (CHAP) is the most common remote access protocol. CHAP has the serving system challenge the remote client, which must provide an encrypted password.
- **MS-CHAP** MS-CHAP is Microsoft's variation of the CHAP protocol. It uses a slightly more advanced encryption protocol. MS-CHAP V2 is yet another improvement on MS-CHAP.
- **EAP** All the previous protocols use encryptions generated by either the server, the client, or both. While this is good encryption, there is nothing unique about the encryption to identify the system that created it. That's where the Extensible Authentication Protocol (EAP) shines. EAP uses a special device—like a smart card—or special, unique data called certificates to create the encryption and to identify the source of the encryption.

Note in Figure 16-32 that multiple protocols are checked. This enables the client dial-up connection to try a number of authentication protocols until it finds one that the RAS server system will accept. In the real world, the person who sets up the RAS server will tell you which authentication to use and you then turn off all of the other protocols.

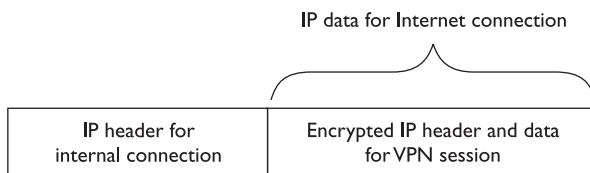
## Data Encryption

Encryption methods don't stop at the authentication level. There are a number of ways to encrypt network *data* as well. The choice of encryption method is dictated to a large degree by the method used by the communicating systems to connect. Many networks consist of multiple networks linked together by some sort of private connection, usually some kind of telephone line like ISDN or T1. Microsoft's encryption method of choice for this type of network is called *IPSec* (derived from IP security). IPSec provides transparent encryption between the server and the client.

## VPNs

Many networks forego the idea of using private long-distance lines to connect a client to a RAS and instead use the Internet itself as a way to connect LANs both to individual systems and to each other. The obvious danger with this is the complete exposure of all network data to the Internet. This has led to the development of encryption methods designed to protect data moving between systems. A network employing encryption to use the Internet as if it were a private network is referred to as a *virtual private network (VPN)*.

**Figure 16-33**  
VPN packet



A VPN connection consists of two items: a regular connection to the Internet (dial-up or dedicated) and an encrypted IP session that runs within the Internet connection. The regular Internet connection uses the IP address allocated to it from the ISP. The encrypted connection uses IP addresses of the private network. Figure 16-33 diagrams a typical VPN packet between a LAN and a remote client.

You can make a VPN through dedicated hardware or through a software solution. Figure 16-34 shows a Linksys VPN router. This VPN router connects to another identical router at another location to make a VPN connection. Hardware solutions are attractive in that they are fast and there is little or nothing to do at the actual client—the VPN is just your Internet connection. Hardware VPN solutions are a popular method to connect a desktop client to a private LAN or to connect two LANs.

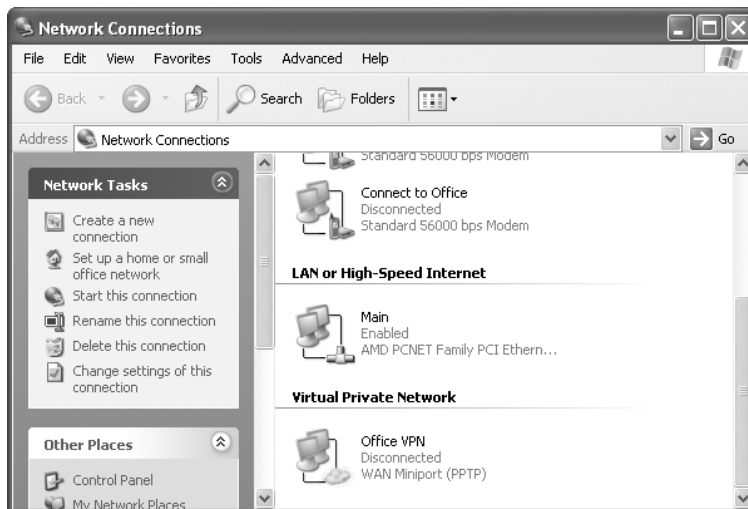
Software VPNs have one big advantage—there is no hardware for the clients to haul around, making it the obvious choice for laptop users who want to connect to a home or office LAN. A software VPN solution manifests on the client as a separate remote connection, as shown in Figure 16-35. Windows 9x had no real support for VPNs, requiring you to use special software. Windows 2000/2003 and XP have excellent wizards to help you configure a VPN client. Creating a VPN client requires that you have the IP address of the device on your private LAN that can accept your VPN request and create a VPN connection.

If you look closely at Figure 16-35 you'll see the term "PPTP." *Point-to-Point Tunneling Protocol (PPTP)* is the Microsoft VPN encryption protocol. Cisco uses its own VPN encryption protocol called *Layer 2 Tunneling Protocol (L2TP)*. Microsoft went proprietary with Windows NT—you couldn't find a place to choose between these two protocols and had to use PPTP. Later versions of Windows use both PPTP and L2TP.

**Figure 16-34**  
A Linksys VPN  
router



**Figure 16-35**  
VPN connection  
in Windows XP

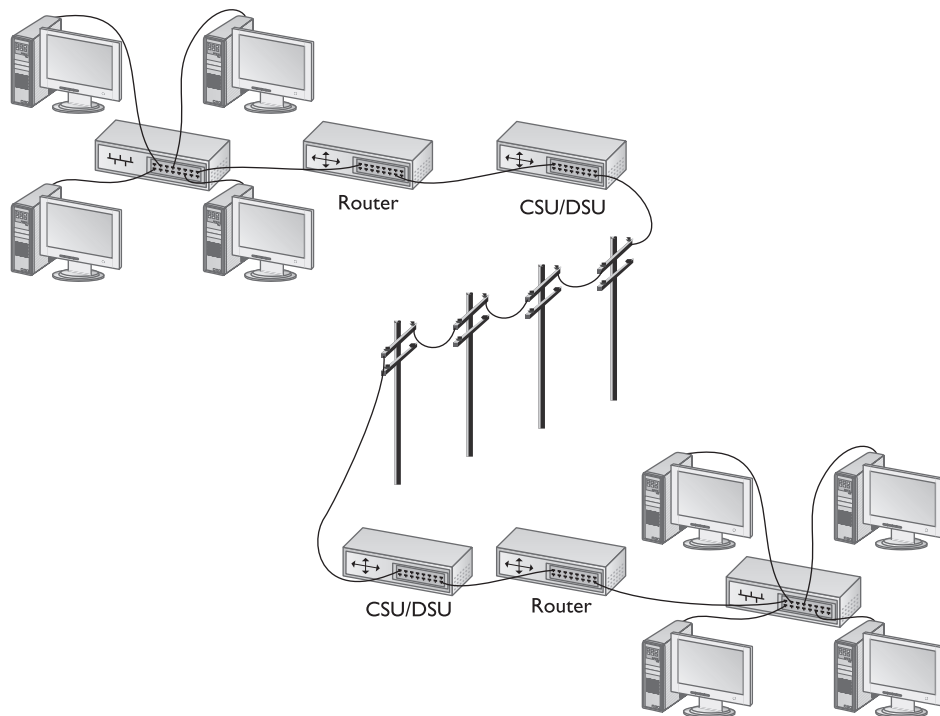


## Dedicated Connection

*Dedicated connections* are remote connections that never disconnect. Dedicated connections can be broken into two groups: dedicated private connections between two locations and dedicated connections to the Internet. Dedicated private connections manifest themselves as two locations interconnected by a (usually high-speed) connection such as a T1 line (Figure 16-36).

Each end of the T1 line goes into a router (after going through a CSU/DSU, of course!). Note that this connection does not use the Internet in any way—it is not a VPN connection! Dedicated connections of this type are expensive and are only used by organizations that need the high bandwidth these connections provide. These connections are invisible to the individual computers on each network. There is no special remote connection configuration of the individual systems, although there may be some configuration of DHCP, DNS, and WINS servers to insure that the network runs optimally.

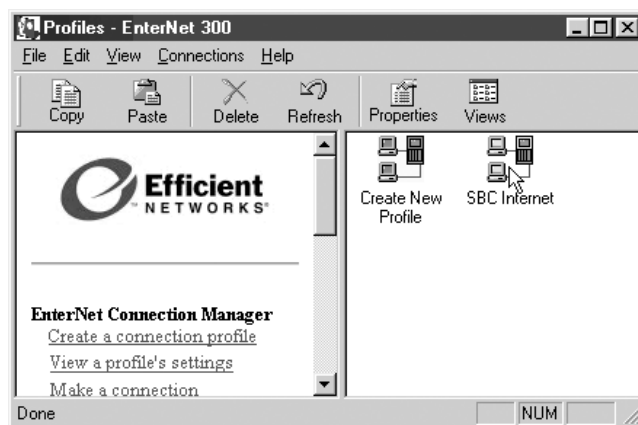
Dedicated connections to the Internet are common today. Cable modems and DSL have made dedicated connections to the Internet inexpensive and very popular. In most cases there is nothing to configure in these dedicated connections but many cable and DSL providers give you a CD-ROM disc that installs testing software, PPPoE login support, and little extras such as e-mail clients and software firewalls (consult Chapter 17, "Protecting Your Network," for information on software firewalls). Figures 16-37 and 16-38 show an ADSL install program for Windows 98 from my ISP, SBC/Prodigy. This program enables you to connect by entering your PPPoE information for your ADSL connection. Once started, these programs usually stay running in the system tray until your next reboot.



**Figure 16-36** Dedicated private connection

Windows XP is the first version of Windows to come with broadband support wizards. When you run the Windows XP New Connection Wizard and select *Connect to the Internet | Set up my connection manually*, you get the screen shown in Figure 16-39. Note the two broadband options: one for a connection that needs a user name and another for a broadband connection that does not.

**Figure 16-37**  
DSL connections



**Figure 16-38**  
PPPoE  
information



The dialog box is titled "User Name and Password". On the left is a collage of images showing people working at computers. The main area contains three input fields: "Enter the User Name for this Connection" with the text "Your Username@sbcglobal.net", "Enter the Password for this Connection" with masked characters, and "Enter the Password one more time." with masked characters. At the bottom are three buttons: "< Back", "Next >" (which is highlighted with a mouse cursor), and "Cancel".

If you choose to create a connection that the Windows wizard describes as “always on,” the wizard doesn’t do anything other than tell you that your connection should already be working. This makes sense because your cable modem or non-PPPoE DSL simply uses your NIC. If you choose *Connect using a broadband connection that requires a user name and password*, however, then you’ll see a dialog box asking for a connection name followed by the dialog box shown in Figure 16-40, prompting for a user name and password. Once this connection is created it shows up in Network Connections (Figure 16-41).

## Internet Connection Sharing

All of these types of remote connections have shown a single remote system connecting to either the Internet or to a private network. What if you have a small LAN with a dial-up or dedicated remote Internet connection on one system and you want all the other PCs in the LAN to connect to the Internet? That’s the job of Internet Connection Sharing.

**Figure 16-39**  
Internet  
Connection  
options



The dialog box is titled "New Connection Wizard". The first step is "Internet Connection" with the question "How do you want to connect to the Internet?". There is a modem icon in the top right. Three radio button options are listed:
 

- ☐ **Connect using a dial-up modem**  
This type of connection uses a modem and a regular or ISDN phone line.
- ☒ **Connect using a broadband connection that requires a user name and password**  
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.
- ☐ **Connect using a broadband connection that is always on**  
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.

 At the bottom are three buttons: "< Back", "Next >", and "Cancel".

**Figure 16-40**  
New Connection  
Wizard prompting  
for PPPoE  
information



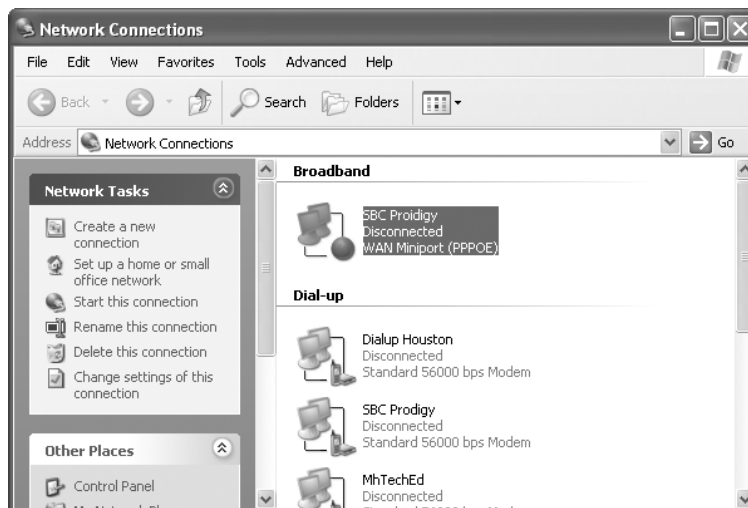
The screenshot shows the 'New Connection Wizard' window with the 'Internet Account Information' tab selected. The window title is 'New Connection Wizard'. Below the title bar, it says 'Internet Account Information' and 'You will need an account name and password to sign in to your Internet account.' There is a small icon of a hand holding a pen. The main area contains instructions: 'Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)' Below this are three text boxes: 'User name:' with 'fakeuser', 'Password:' with six dots, and 'Confirm password:' with six dots. There are three checked checkboxes: 'Use this account name and password when anyone connects to the Internet from this computer', 'Make this the default Internet connection', and 'Turn on Internet Connection Firewall for this connection'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

*Internet Connection Sharing (ICS)* is Microsoft's term to describe the technique of allowing more than one computer to access the Internet simultaneously using a single Internet connection on a single system. When you use ICS, you connect an entire LAN to the Internet using one computer. This connection to the Internet may be via modem, cable modem, ADSL, ISDN, leased line, or T1. In most cases, ICS uses *Network Address Translation (NAT)* to achieve this sharing.



**NOTE** ICS is only for sharing Internet connections. It is not designed to support connecting to another private network.

**Figure 16-41**  
PPPoE  
connection in  
Windows XP



There are many benefits to using ICS. For starters, having only one Internet account reduces costs. ICS also protects your data by putting your computers behind a firewall, and by enabling administrators to control user access to Internet services and resources. If you have multiple computers on a LAN, you can use ICS to allow different computers on the LAN to perform different tasks simultaneously. For example, one person can send and receive e-mail messages, while another person downloads a file, and another person browses the Internet. ICS uses DHCP and DNS to configure TCP/IP information automatically for clients in the LAN. Any IP-attached device can connect to the LAN, including older Windows clients and non-Windows-based clients, without any additional client software.

ICS has the following components:

- **DHCP Allocator** Assigns the IP address, gateway, and name server on the local network.
- **DNS Proxy** Resolves names on behalf of local network clients and forwards queries.
- **Network Address Translation (NAT)** Maps a set of private addresses to a set of public addresses. NAT tracks private-source IP addresses and public-destination IP addresses for outbound data flows. It changes the IP address information and edits the required IP header information dynamically.
- **Auto-dial** Automatically dials connections.
- **Application Programming Interfaces (APIs)** Used by programs for configuration, status, and dial control.

Configuring ICS is simple. You turn on ICS on one system and it works (Figure 16-42). An ICS system must have two connections: an Internet connection via an ISP, and a NIC that connects to the rest of the network. ICS doesn't have to use dial-up. Any computer connected to the ISP via dial-up modem, cable modem, DSL modem, or over even a T1 line can use ICS. The location of ICS varies on different versions of Windows but usually is located under the modem's properties.

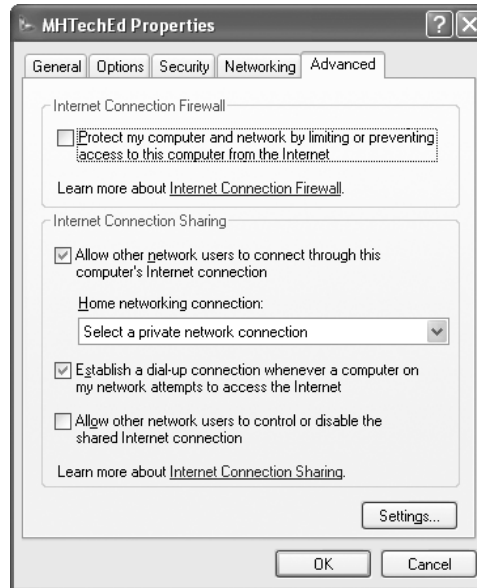
## Troubleshooting Remote Access

Troubleshooting remote access connections might seem at first to be a bit of a challenge, given the different physical connection options as well as the type of remote access you are using. In reality, troubleshooting remote access is usually easy if you first realize that all remote access connections share a number of common areas. Let's see what every remote access connection has in common and see how to use these common issues to troubleshoot.



**NOTE** These remote issues are not in any particular order.

**Figure 16-42**  
ICS in  
Windows XP



## Is the Physical Remote Connection Running?

The physical connection is the signal that runs between your PC and your other connection. These are the telephone lines (PSTN, DSL, T1) or coaxial cables (cable modems) as well as the signal they carry. If a connection works one day but doesn't work the next odds are good nothing has changed on your remote client. If a remote access connection suddenly quits working you need to determine if the physical remote connection is available. The trick is how to do this—and that varies by the type of connection.

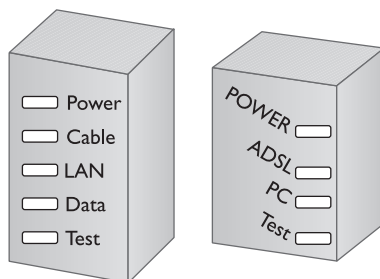
If it's a PSTN line, this simply means to check for a dial tone. Lack of a dial tone usually means the modem is unplugged from the phone jack or a telephone in another room was left off the hook.

Cable and DSL connections are virtually identical in terms of verifying their physical connections—the secret is the LEDs on the cable or DSL modem. Figure 16-43 shows drawings of two sets of LEDs, the left from my cable modem and the right from my DSL modem. There are two LEDs of interest that help determine if the connection is up. The most important is the one that says "Cable" or "ADSL." These LEDs are on when your cable or DSL modem has a connection to whatever device is on the other end to make this connection work. If those LEDs are not on, you don't have a connection.

Most DSL and cable providers go down from time to time—if those LEDs are off, you'll need to try to reset the connection. How this is done varies; some devices have a reset button and some have to be turned off and then turned back on to reset. During the reset the test LED comes on. The test LED flickers and blinks, eventually turning off after the connection is reestablished. The test LED is also used by your cable or DSL provider's telephone support staff if you call in with problems.



**Figure 16-43**  
Cable (left) and  
DSL (right) LEDs



Most cable and DSL tech support people use the term “cycle the modem” when they want you to unplug the modem for 10–30 seconds and plug it back in. You’ll find the need to cycle the modem if you change hardware; for example, if you swap out NICs or add a broadband router to the mix.



**NOTE** Every DSL and cable modem is different. Some have more and some have fewer LEDs than the ones described here.

If the DSL or cable modem fails to work after a reset, your provider will come onsite for diagnostics and repair armed with handy testers with funny names such as a Bit Error Rate (BERT) tester or a SNR (Signal to Noise Ratio) tester. Based on their findings, they will repair internal lines (you pay for this) or external lines (they pay for that) to ensure a good connection.

If you use T1 or other higher-end connections, the CSU/DSU is the place to check for your connection. Every CSU/DSU has an LED that confirms a connection to the far CSU/DSC. If this LED shows no connection, call your local exchange carrier to have them perform a “loopback” or “loop” test of their line. Additionally, all CSU/DSUs have some form of self-test to verify that the connection to the other CSU/DSU is in good order. This self-test is handy for making sure the wire running from the demarc to the CSU/DSU is in good shape. It is common for you to run this program yourself—a good reason to keep the CSU/DSU manual handy!

## Is Your Hardware Running?

Your own hardware is almost always overlooked. Is your modem/NIC working? Do you have a good connection to your cable modem or DSL modem? Is the DSL or cable modem working properly? Take advantage of Device Manager to test internal devices and use any testing programs at your disposal if available for your device. One of the best times to learn about testing programs is at installation. Don’t be afraid to ask the install techs what testing if any they provide. The testing tools vary widely between technologies and providers so ask the people who know best—the install and repair techs.

## Are You Configured?

Improper configuration is the single biggest reason for remote connection failures. Configurations take place at so many levels. Start with hardware configuration. Some devices—cable modems are a great example—have no user configuration. Other devices such as ISDN modems have a number of configurations such as the SPID number. The best idea here is to perform what I call the “mental reinstall:” going through the process of installation to see what configurations come up.

Configuration doesn’t stop with the hardware. Connections have plenty of configurations. Are you running PPP or SLIP? Do you have the right telephone number? Do the dialing rules work properly? What are the TCP/IP settings for this connection? One of the nice aspects to connections is that you can make as many as you want. If I think a connection is improperly configured, I just make another one. Of course I keep the old connection to compare and check!

## Is the Server Awake?

The term “server” here has two meanings. The first meaning has to do with private connections and VPNs. In these cases the connection itself must have some device on the other end to make a connection. If the RAS or VPN server isn’t functioning, you won’t make a connection. There’s only one way to test this—call someone at the other location. If no one’s there you have no way to confirm whether the server is up and running.

The second meaning to the word “server” is more in the vein of Internet connections. All Internet connections need the usual assortment of DNS, DHCP, and other such servers running to connect. Testing TCP/IP on a remote connection is no different than on a LAN. Use the tools and techniques you learned about in Chapter 14, “Going Large with TCP/IP,” to make sure your Internet servers are working.

## Chapter Review

### Questions

1. Which of the following is *not* a Data Link protocol for telephone lines? (Select all that apply.)
  - A. SLIP
  - B. IP
  - C. PPP
  - D. PPTP
2. Which of the following provides the fastest throughput?
  - A. PSTN
  - B. ISDN BRI

- C. ISDN PRI
  - D. POTS
3. The popular Microsoft remote access client is called
- A. RAS
  - B. Dial-Up Networking
  - C. Dial-Up Server
  - D. Microsoft Client for Networks
4. Thor is concerned that e-mail sent from his laptop to the RAS system in his home office could be read by others. What does he need to use?
- A. A password
  - B. Encryption
  - C. A login name
  - D. SMTP
5. BRI ISDN uses
- A. One B channel and 24 D channels
  - B. 24 B channels and one D channel
  - C. One B channel and two D channels
  - D. Two B channels and one D channel
6. The V.90 standard defines a modem speed of
- A. 56 Kbps
  - B. 33.6K baud
  - C. 28.8 Kbps
  - D. 2400 baud
7. Which of the following V standards defines error checking?
- A. V.42
  - B. V.42bis
  - C. V.34
  - D. MNP 8
8. The ISDN equivalent of a modem is called a
- A. Terminal point
  - B. Network interface device
  - C. Terminal adapter
  - D. Network adapter

9. Which of the following are benefits of ISDN over PSTN? (Select all that apply.)
- A. ISDN is more widely available.
  - B. ISDN is faster.
  - C. ISDN connects more quickly.
  - D. ISDN is cheaper.
10. Generally, how close do you need to be to a central office to use ISDN?
- A. 1,800 feet
  - B. 1,800 meters
  - C. 18,000 feet
  - D. 18,000 meters

## Answers

- 1. B, D. SLIP and PPP are Data Link protocols for telephone lines.
- 2. C. ISDN PRI has a throughput of 1.5 Mbps. The next fastest is ISDN BRI at 128 Kbps.
- 3. B. The popular Microsoft remote access client is called Dial-Up Networking. RAS is remote access server software.
- 4. B. Thor needs to use some form of encryption.
- 5. D. BRI ISDN uses two B channels and one D channel.
- 6. A. The V.90 standard defines a 56-Kbps modem speed.
- 7. A. The V.42 standard defines modem error checking.
- 8. C. The ISDN equivalent of a modem is called a terminal adapter.
- 9. B, C. ISDN is faster than PSTN and connects more quickly.
- 10. C. You generally need to be within 18,000 feet of a central office to take advantage of ISDN.